МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

ПЕТРИК ВІТАЛІЙ ВІТАЛІЙОВИЧ

УДК 343.14:004:34.05

ДИСЕРТАЦІЯ
ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ В УКРАЇНІ ТА СВІТІ

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. В. Петрик**

Науковий керівник: **Хахановський Валерій Георгійович,**
доктор юридичних наук, професор

Київ–2026

АНОТАЦІЯ

Петрик В. В. Особливості використання електронних доказів у кримінальному процесі в Україні та світі. – *Кваліфікаційна наукова праця на правах рукопису.*

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

Дисертацію присвячено комплексному дослідженню теоретичних, правових і прикладних аспектів використання електронних доказів у кримінальному провадженні України й інших держав. В умовах цифровізації суспільних відносин інформаційно-комунікаційні технології відіграють подвійну роль у сфері кримінальної юстиції: з одного боку, їх використовують для вчинення та приховування кримінальних правопорушень, з іншого – вони стають незамінним засобом їх виявлення та розслідування, оскільки більшість протиправних дій залишають цифрові сліди. Попри посилення доказового значення електронної інформації, її правовий статус, порядок збирання, фіксації, перевірки й оцінки залишаються недостатньо врегульованими на законодавчому рівні, що зумовлює актуальність дослідження.

Сформульовано авторське функціональне визначення електронного доказу як інформації в електронній формі, що створена, збережена, передана або відображена за допомогою електронних пристроїв, систем чи мереж, містить відомості про обставини, які мають значення для кримінального провадження, і може бути використана як доказ за умови її отримання та перевірки в порядку, передбаченому Кримінальним процесуальним кодексом України. На відміну від наявних доктринальних підходів, визначення ґрунтується на способі існування інформації в електронному середовищі, без оцінних категорій автентичності та цілісності в дефініції, що забезпечує її придатність і для майбутніх форм електронних об’єктів. Обґрунтовано доцільність закріплення електронного доказу як самостійного джерела доказів шляхом доповнення частини 2 статті 84 Кримінального процесуального кодексу України.

Виокремлено та систематизовано специфічні ознаки електронних доказів, що відрізняють їх від традиційних джерел, зокрема це: нематеріальність, динамічність, відтворюваність, залежність від технічних засобів, відсутність жорсткої прив'язки до матеріального носія та наявність метаданих. Обґрунтовано виокремлення метаданих як ознаки із самостійним доказовим значенням, що дають змогу встановлювати час, джерело й історію змін електронного об'єкта.

Запропоновано координатну авторську класифікацію електронних доказів за п'ятьма взаємодоповнюваними критеріями: за способом створення інформації (створені людиною, комп'ютером, комбіновані та створені штучним інтелектом); за процесуальним режимом отримання (безпосередньо вилучені, отримані через тимчасовий доступ, негласні слідчі (розшукові) дії та міжнародне співробітництво); за процесуальним статусом носія (локальні, мережеві, локально-мережеві, транзитні); за рівнем процесуальної верифікованості (самоверифіковані, технічно верифіковані, експертно підтверджені, презумптивно верифіковані); за рівнем втручання в право на повагу до приватного життя. Координатний характер класифікації дає змогу одночасно описати кожен доказ за всіма критеріями та визначити процесуальний маршрут роботи з ним. Окремо розроблено авторську класифікацію листування в месенджерах як виду електронних доказів за вісьмома критеріями (кількістю учасників, рівнем доступу, можливістю розміщення контенту, етапом створення, джерелом походження, форматом, змістово-інформаційною складовою та способом формування відповідей).

Обґрунтовано процесуально-правову концепцію трансформації електронного об'єкта на доказ через чотири послідовні операції: відтворення інформації засобами програмно-апаратного забезпечення; аналіз її атрибутів і метаданих; описове закріплення в процесуальному документі; вилучення або копіювання з гарантією цілісності через хешування та фіксацію ланцюга поводження (chain of custody). Доведено, що порушення цього мінімального стандарту фіксації тягне недопустимість доказу за частиною 1 статті 87 Кримінального процесуального кодексу України. Обґрунтовано доктринальне положення про презумпцію допустимості електронної форми доказу, згідно з яким

електронна форма не є підставою для визнання доказу недопустимим, а підстави недопустимості, пов’язані з порушенням процесуального порядку, доводить сторона, яка оспорює доказ. Достовірність електронного доказу обґрунтовано як динамічну характеристику, яку верифікують на кожному наступному етапі провадження через ланцюг поводження.

Запропоновано доповнити Кримінальний процесуальний кодекс України статтею 99-3 «Особливості оцінки електронних доказів, створених або модифікованих засобами штучного інтелекту», яка передбачає три взаємопов’язані правила: обов’язок учасника провадження розкривати факт використання технологій штучного інтелекту; перерозподіл тягаря доказування автентичності на сторону, що подала доказ, у разі заявлення обґрунтованих сумнівів; недопустимість електронного доказу штучного походження, не розкритого стороною, що його подала. Доцільність такого регулювання підтверджена результатами анкетування, за якими переважна більшість опитаних практичних працівників розцінюють докази, згенеровані штучним інтелектом, як актуальну загрозу.

На підставі порівняльно-правового аналізу правових систем Сполучених Штатів Америки, Канади та Великої Британії, Французької Республіки й Федеративної Республіки Німеччина, а також Китайської Народної Республіки та Республіки Індія, нормативної бази Європейського Союзу виокремлено три моделі регулювання: формалізовану (кодифіковані критерії допустимості та самоавтентифікація за Federal Rules of Evidence), із презумпцією цілісності (Canada Evidence Act) і прагматичну (суддівська дискреція за Police and Criminal Evidence Act). Обґрунтовано комбіновану модель регулювання електронних доказів для України, що поєднує формалізований і прагматичний елементи й наднаціональний каркас транскордонного доступу (механізми European Production Order і European Preservation Order Регламенту (ЄС) 2023/1543). Запропоновано запровадити в Кримінальному процесуальному кодексі України інститут дистанційного проникнення до інформаційних систем на трьох принципах, серед них: обов’язковість попередньої судової санкції; обмеження кола злочинів вичерпним переліком тяжких й особливо тяжких правопорушень; заборона збирання даних

«ядра приватного життя». Обґрунтовано необхідність ратифікації Україною Другого додаткового протоколу до Конвенції про кіберзлочинність і запровадження механізму прямого звернення до іноземних постачальників послуг електронних комунікацій.

Емпіричну базу дослідження становлять результати проведеного автором анкетування 130 працівників прокуратури, матеріали судової практики (опрацьовано понад 300 рішень Єдиного державного реєстру судових рішень і понад 50 рішень судів інших держав), практика Європейського суду з прав людини, а також національне й закордонне законодавство, міжнародні акти у сфері електронних доказів.

Практичне значення одержаних результатів полягає в можливості їх використання в науково-дослідній діяльності, правотворчості (під час удосконалення КПК України), правозастосуванні й освітньому процесі.

Ключові слова: електронний доказ, кримінальний процес, допустимість доказів, штучний інтелект, месенджер, порівняльне правознавство, кримінальне судочинство.

SUMMARY

Petryk V. Peculiarities of the Use of Electronic Evidence in Criminal Proceedings in Ukraine and Worldwide. – *Qualifying scientific work as a manuscript.*

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

The dissertation provides a comprehensive study of the theoretical, legal and applied aspects of the use of electronic evidence in the criminal proceedings of Ukraine and foreign states. Amid the digitalisation of social relations, information and communication technologies have acquired a dual role in the sphere of criminal justice: on the one hand, they are used to commit and conceal criminal offences; on the other, they have become an indispensable means of detecting and investigating such offences, since the overwhelming part of unlawful activity leaves digital traces. Despite the growing evidentiary significance of electronic information, its legal status and the procedure for its collection, recording, verification and evaluation remain insufficiently regulated at the legislative level, which determines the relevance of the study.

The author formulates an original functional definition of electronic evidence as information in electronic form that is created, stored, transmitted or displayed by means of electronic devices, systems or networks, contains data on circumstances relevant to the criminal proceedings, and may be used as evidence provided that it is obtained and verified in the manner prescribed by the Criminal Procedure Code of Ukraine (hereinafter the Criminal Procedure Code of Ukraine). Unlike the existing doctrinal approaches, the definition is built upon the mode of existence of information in the electronic environment, without incorporating the evaluative categories of authenticity and integrity into the definition itself, which ensures its applicability to future forms of electronic objects as well. The expediency of enshrining electronic evidence as an independent source of evidence by supplementing part 2 of Article 84 of the Criminal Procedure Code of Ukraine is substantiated.

Six specific features of electronic evidence that distinguish it from traditional sources are identified and systematised: intangibility, mutability, reproducibility,

dependence on technical means, the absence of a rigid attachment to a material medium, and the presence of metadata. The author substantiates the singling out of metadata as a feature possessing independent evidentiary value, which makes it possible to establish the time, source and history of changes to an electronic object.

An original coordinate (multidimensional) classification of electronic evidence is proposed, based on five mutually complementary criteria: by the method of creating the information (created by a human, by a computer, combined, and created by artificial intelligence); by the procedural regime of obtaining (directly seized, obtained through temporary access, through covert investigative (search) actions, and through international cooperation); by the procedural status of the medium (local, network, local-network, transit); by the level of procedural verifiability (self-verified, technically verified, expert-confirmed, presumptively verified); and by the level of interference with the right to respect for private life. The coordinate nature of the classification makes it possible to describe each item of evidence simultaneously against all the criteria and to determine the procedural route for handling it. Separately, the author develops a classification of messenger correspondence as a type of electronic evidence according to eight criteria (by the number of participants, the level of access, the possibility of posting content, the stage of creation, the source of origin, the format, the substantive-informational component, and the manner of generating replies).

A procedural-legal concept of the transformation of an electronic object into evidence is substantiated through four successive operations: reproduction of the information by means of software and hardware; analysis of its attributes and metadata; descriptive recording in a procedural document; and seizure or copying with a guarantee of integrity through hashing and documentation of the chain of custody. It is proved that a breach of this minimum standard of recording entails the inadmissibility of the evidence under part 1 of Article 87 of the Criminal Procedure Code of Ukraine. A doctrinal proposition on the presumption of admissibility of the electronic form of evidence is substantiated, according to which the electronic form in itself does not constitute a ground for declaring evidence inadmissible, while the grounds for inadmissibility connected with a violation of the procedural order are to be proved by the party that challenges the

evidence. The reliability of electronic evidence is substantiated as a dynamic characteristic that is verified at each subsequent stage of the proceedings through the chain of custody.

It is proposed to supplement the Criminal Procedure Code of Ukraine with Article 99-3 «Peculiarities of the Evaluation of Electronic Evidence Created or Modified by Means of Artificial Intelligence», which provides for three interrelated rules: the obligation of a participant in the proceedings to disclose the fact of using artificial intelligence technologies; the reallocation of the burden of proving authenticity to the party that submitted the evidence where reasonable doubts are raised; and the inadmissibility of artificially originated electronic evidence that has not been disclosed by the party submitting it. The expediency of such regulation is confirmed by the results of a survey, according to which the overwhelming majority of the practitioners surveyed regard evidence generated by artificial intelligence as a pressing threat.

On the basis of a comparative legal analysis of the legal systems of the United States of America, Canada and the United Kingdom, the French Republic and the Federal Republic of Germany, as well as the People's Republic of China and the Republic of India, and of the regulatory framework of the European Union, three models of regulation are identified: a formalised model (codified admissibility criteria and self-authentication under the Federal Rules of Evidence), a model with a presumption of integrity (the Canada Evidence Act), and a pragmatic model (judicial discretion under the Police and Criminal Evidence Act). A combined model for the regulation of electronic evidence in Ukraine is substantiated, which combines formalised and pragmatic elements with a supranational framework for cross-border access (the European Production Order and European Preservation Order mechanisms under Regulation (EU) 2023/1543). The introduction into the Criminal Procedure Code of Ukraine of an institution of remote penetration of information systems is proposed, based on three principles: the mandatory nature of prior judicial authorisation; the limitation of the range of offences to an exhaustive list of grave and especially grave offences; and the prohibition on collecting data belonging to the «core of private life». The need for Ukraine to ratify the Second

Additional Protocol to the Convention on Cybercrime and to introduce a mechanism of direct requests to foreign electronic communications service providers is substantiated.

The empirical basis of the study comprises the results of a survey of 130 prosecutors conducted by the author, materials of judicial practice (more than 300 decisions from the Unified State Register of Court Decisions and more than 50 decisions of courts of foreign states were examined), the case-law of the European Court of Human Rights, as well as national and foreign legislation and international instruments in the field of electronic evidence.

The practical significance of the results obtained lies in the possibility of their use in research activity, in law-making (in the course of improving the Criminal Procedure Code of Ukraine), in law enforcement and in the educational process.

Keywords: electronic evidence, criminal procedure, admissibility of evidence, artificial intelligence, messenger, comparative law, criminal justice.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких відображено основні результати дослідження:

1. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. № 87. С. 119–123. DOI: 10.24144/2307-3322.2025.87.4.17

2. Хахановський В. Г., Петрик В. В. Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект). *Європейський правничий часопис.* 2025. Вип. 8. С. 161–165. DOI: 10.36919/3041-1149(Print).8.2025.161-165

3. Петрик В. В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. *Науковий вісник Ужгородського національного університету. Серія «Право».* № 90, ч. 4. 2025. С. 324–328. DOI: 10.24144/2307-3322.2025.90.4.46

4. Петрик В. В., Ментинська І. Б. Відтворення англомовних назв програмних продуктів у кримінальному процесі: проблеми уніфікування. *Інтернаука*. 2026. № 1 (95). С. 161–168. DOI: 10.25313/2520-2308-2026-1-11840

5. Петрик В. В. Електронні об’єкти, згенеровані штучним інтелектом, як докази у кримінальному провадженні: проблеми правового регулювання в Україні та зарубіжний досвід. *Юридичний науковий електронний журнал.* 2026. № 4. С. 217–222. DOI: 10.32782/2524-0374/2026-4/46

6. Машталяр О. М., Петрик В. В. Персональні дані як електронний доказ у кримінальному процесі. *Юридичний науковий електронний журнал.* 2026. № 5. С. 218–221. DOI: 10.32782/2524-0374/2026-5/49

7. Khakhanovsky V., Petryk V. Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad. *Scientific Journal of the National Academy of Internal Affairs*. 2026. № 31 (2). P. 9–19. DOI: 10.63341/naia-herald/2.2026.09

Наукові праці, у яких засвідчено апробацію матеріалів праці:

1. Петрик В. В. Електронні докази в судочинстві України та зарубіжних країн: поняття, правове регулювання та проблеми використання. Global trends in science and education : матеріали III Міжнар. наук.-практ. конф. (Київ, 7–9 квіт. 2025 р.). Київ, 2025. С. 921–926.

2. Петрик В. В. Поняття та правова природа електронних доказів у кримінальному процесі України. Future of science: innovations and perspectives. Proceedings of the 9th International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2025. Pp. 224–228 .

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 14
ВСТУП 15
РОЗДІЛ 1. ВИЗНАЧЕННЯ, ОЗНАКИ, КЛАСИФІКАЦІЯ ТА ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ 28
1.1. Стан наукових досліджень. Поняття електронних доказів. 28
1.2. Ознаки та класифікація електронних доказів 39
1.3. Правове регулювання електронних доказів у кримінальному процесуальному законодавстві України та міжнародних актах 58
Висновки до розділу 1 63
РОЗДІЛ 2. ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ 65
2.1. Використання електронних доказів у кримінальному процесі. Питання допустимості електронних доказів 65
2.2. Належність, достатність і достовірність електронних доказів 88
2.3. Електронне листування в месенджерах як вид електронних доказів 105
2.4. Об’єкти, створені штучним інтелектом: проблеми оцінки в доказуванні 117
Висновки до розділу 2 130
РОЗДІЛ 3. АНАЛІЗ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ ІНШИХ КРАЇН 133
3.1. Електронні докази в англо-саксонській системі права (США, Канада, Велика Британія) 134
3.2. Електронні докази в романо-германській системі права (Франція, Німеччина, нормативна база ЄС) 144
3.3. Електронні докази в інших правових системах (КНР, Індія) 153
3.4. Порівняльний аналіз зарубіжного досвіду та перспективи вдосконалення правового регулювання електронних доказів у кримінальному процесі України 159
Висновки до розділу 3 165

ВИСНОВКИ..... 168
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 174
ДОДАТКИ..... 199

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВС – Верховний Суд

ГПК – Господарський процесуальний кодекс

ЄДРСР – Єдиний державний реєстр судових рішень

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

КК – Кримінальний кодекс

ККС ВС – Касаційний кримінальний суд у складі Верховного Суду

КПК – Кримінальний процесуальний кодекс

МВС – Міністерство внутрішніх справ

НСРД – негласні слідчі (розшукові) дії

ССЄС – Суд справедливості Європейського Союзу

ЦПК – Цивільний процесуальний кодекс

ШІ – штучний інтелект

CLOUD Act – Clarifying Lawful Overseas Use of Data Act (Закон про роз'яснення законного використання даних, що зберігаються за кордоном)

CPP – Code de procédure pénale (Кримінальний процесуальний кодекс Франції)

EIO – European Investigation Order (Європейський ордер на розслідування)

FRE – Federal Rules of Evidence (Федеральні правила доказування США)

FRCP – Federal Rules of Criminal Procedure (Федеральних правилах кримінального судочинства)

GPS – Global Positioning System (глобальна система позиціонування)

IP – Internet Protocol (міжмережевий протокол)

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission

PACE – Police and Criminal Evidence Act 1984 (Закон про поліцію та кримінальні докази Великої Британії)

ВСТУП

Обґрунтування вибору теми дослідження. Стрімкий розвиток процесів цифровізації суспільства й інформаційно-комунікаційних технологій впливає на всі сфери людського життя. В електронному вигляді формуються дані про все життя людини, а створення штучного інтелекту зумовило революцію у використанні електронних технологій, що можна порівняти з винайденням двигуна або інтернету.

У мережі Інтернет фіксуються події, які за певних обставин можуть утворювати склад кримінального правопорушення. Водночас інформація з мережі Інтернет може слугувати джерелом відомостей про подію правопорушення: підтверджувати факт його вчинення, містити дані про сліди протиправної діяльності, характеризувати заподіяні наслідки.

Актуальність дослідження зумовлена не лише поширенням інформаційно-комунікаційних технологій, а й якісною зміною їхньої ролі у сфері кримінального права та процесу. З одного боку, такі технології дедалі активніше використовують для вчинення та приховування кримінальних правопорушень – від кібершахрайств і збуту заборонених речовин через месенджери до застосування шифрування та засобів штучного інтелекту для маскування слідів протиправної діяльності.

З іншого боку, ті самі технології стають незамінним інструментом виявлення, фіксації та розслідування злочинів, оскільки переважна частина сучасної протиправної діяльності залишає електронні сліди. Ці обставини підвищують значення електронних доказів і потребу в їх належному процесуальному регулюванні.

Слід акцентувати й на тому, що в інформаційних мережах відображаються відомості про юридично та соціально значущі факти, які можуть мати пряме чи непряме відношення до події кримінального правопорушення: електронне листування, геолокаційні дані, записи систем відеоспостереження, відомості про з’єднання та транзакції, публікації в соціальних мережах тощо.

Завдяки цьому мережа Інтернет й інші електронні середовища перетворюються на самостійне джерело доказової інформації, здатне підтверджувати факт вчинення правопорушення, встановлювати коло причетних осіб, а також час, місце й обстановку події. Саме тому формування науково обґрунтованих підходів до збирання, перевірки й оцінки електронних доказів є нагальним завданням сучасної науки кримінального процесу.

На нашу думку, сучасні реалії засвідчують важливе значення електронних даних як доказів у кримінальному судочинстві, унаслідок чого в науці кримінального процесу з'явилася нова категорія доказів, а саме «електронні докази», що зумовлено практичною потребою у визначенні єдиних підходів до використання та оцінки електронних об'єктів як джерела доказів у кримінальному провадженні.

Відповідно до ст. 84 КПК України, доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому цим Кодексом 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.

Водночас у кримінальному процесуальному законодавстві України не визначено поняття електронних доказів, порядок їх збирання та оцінки.

Правозастосовна практика дає підстави стверджувати, що електронні докази в кримінальному процесі відносять до документів. Відповідно до ст. 99 КПК України, документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюють під час кримінального провадження. Частина 2 цієї статті регламентує, що документами можуть бути матеріали фотозйомки, звукозапису, відеозапису й інші носії інформації (зокрема електронні).

Неповнота правового регулювання процесуального порядку отримання інформації в електронній формі як джерела доказів позначається на якості досудового розслідування, а також на правильності збирання, фіксації та

процесуального оформлення доказів. Крім того, суперечливість правозастосовної практики та брак науково обґрунтованих рекомендацій щодо перевірки, оцінки й використання такої інформації негативно позначаються на забезпеченні її належності, допустимості та достовірності, що своєю чергою знижує ефективність досягнення завдань кримінального провадження.

Практика застосування інформації в електронній формі як джерела доказів, а також досвід інших країн засвідчують наявність в Україні потреби в додаткових наукових дослідження та процесуальній регламентації дій щодо фіксації та збереження таких відомостей, які можуть бути використані для встановлення фактів чи обставин у кримінальному провадженні.

Водночас важливим напрямом розвитку цієї сфери є питання належної оцінки такої інформації органами досудового розслідування та судом, що зумовлює необхідність формування єдиних науково обґрунтованих підходів і зосередження посиленої уваги на цьому аспекті в дослідженні.

Слід зауважити, що поняття «використання електронних доказів» використано в широкому процесуальному значенні й охоплює весь цикл роботи з електронним доказом: збирання, фіксацію, перевірку та оцінку (належність, допустимість, достовірність, достатність), а також безпосереднє застосування в кримінальному процесуальному доказуванні.

Стан дослідження проблеми в юридичній науці. Деякі питання використання електронних об’єктів як доказів у кримінальному процесі розглядали у своїх роботах такі українські вчені: Н. М. Ахтирська, Д. О. Алєксєєва-Процюк, І. В. Гора, А. В. Гутник (Ратнова), М. В. Гуцалюк, І. Г. Каланча, О. В. Капліна, О. Г. Козицька, В. А. Колесник, О. П. Метелев, Ю. Ю. Орлов, М. І. Пашковський, М. А. Погорецький, Д. Б. Сергєєва, О. В. Сіренко, І. А. Смаль, В. Г. Хахановський, Д. М. Цехан, С. С. Чернявський, М. В. Шепітько та ін.

Серед іноземних учених слід виокремити роботи М. Р. Аркфельда, Е. Кейсі, Г. Кесслера, В. С. Глайзнера, Дж. Е. Гренiга, Дж. Л. Керрола, Т. Ларсона, С. Мейсона, П. Грімма, М. Новак, М. Стойкової та ін.

На дисертаційному та монографічному рівні аспекти використання електронних доказів у кримінальному провадженні досліджувала А. В. Ратнова (Гутник) у дисертації на здобуття ступеня доктора філософії «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні» (2021), у якій проаналізовано криміналістичне забезпечення роботи з електронними доказами [113]; А. Я. Хитра у співавторстві з А. В. Ратновою в однойменній монографії (2022) продовжили комплексний аналіз процесуальних і криміналістичних підходів до використання електронних документів у доказуванні.

2025 року І. Г. Каланча в докторській дисертації «Докази електронної форми у кримінальному процесі України: теорія та практика» здійснила комплексне дослідження інституту доказів електронної форми, запропонувавши термінологічне розмежування понять «цифровий доказ», «електронний доказ» і «доказ електронної форми», а також обґрунтувавши п’ять елементів електронної складової кримінального процесу [61].

І. А. Смаль у дисертації на здобуття ступеня доктора філософії «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі» виокремила три періоди формування інституту електронних доказів і запропонувала визначення електронного доказу, а також розкрила загальнотеоретичні та криміналістичні аспекти використання електронних доказів. Водночас питання процесуального режиму окремих видів електронних доказів (зокрема листування в месенджерах) і правового реагування на виклики штучного інтелекту в доказуванні залишаються недостатньо розробленими, що й зумовлює актуальність цього дослідження.

Вагомим внеском у розроблення проблематики електронних доказів стала колективна монографія «Концептуальні основи цифровізації кримінального провадження України» (2024) за загальною редакцією Н. В. Глинської, у якій запропоновано систему концептуальних положень щодо застосування цифрових технологій у кримінальному судочинстві, зокрема проаналізовано поняття та властивості електронних доказів, особливості їх використання, питання технологій

штучного інтелекту, розвинуто в концепцію раннього збереження цифрових доказів у провадженнях щодо злочинів війни.

Попри наявність значного наукового доробку, проблематика використання електронних доказів у кримінальному провадженні залишається недостатньо розробленою в комплексному вимірі. У більшості наукових праць досліджено аспекти цієї теми: поняття електронних доказів, їх співвідношення з електронними документами, порядок збирання, допустимість або криміналістичні особливості роботи із цифровою інформацією.

Водночас недостатньо уваги спрямовано на комплексний порівняльно-правовий аналіз зарубіжних моделей регулювання електронних доказів, особливості оцінки листування в месенджерах, проблеми автентичності цифрових аудіовізуальних матеріалів в умовах розвитку технологій штучного інтелекту, а також розроблення цілісної моделі вдосконалення кримінального процесуального законодавства України.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Напрям дослідження обрано відповідно до Стратегії національної безпеки України (Указ Президента України від 14 вересня 2020 року № 392/2020), Державної стратегії регіонального розвитку на 2021–2027 роки (постанова Кабінету Міністрів України від 5 серпня 2020 року № 695), Національної економічної стратегії на період до 2030 року (постанова Кабінету Міністрів України від 3 березня 2021 року № 179).

Робота відповідає Тематиці наукових досліджень і науково-технічних (експериментальних) розробок Міністерства внутрішніх справ України на 2020–2024 роки (наказ МВС України від 11 червня 2020 року № 454) й Основним напрямам наукових досліджень Національної академії внутрішніх справ на 2021–2024 роки (рішення Вченої ради НАВС від 21 грудня 2020 року, протокол № 23).

Тему дисертації затверджено рішенням Вченої ради НАВС від 25 жовтня 2022 року (протокол № 14).

Мета роботи полягає у формуванні теоретико-правових засад використання електронних доказів у кримінальному провадженні та розробленні науково

обґрунтованих рекомендацій з удосконалення відповідного процесуального регулювання. Для досягнення поставленої мети необхідно було виконати такі *завдання*:

1) висвітлити поняття, правову природу й обґрунтувати самостійність електронного доказу як виду доказів у кримінальному провадженні України;

2) виокремити й систематизувати специфічні ознаки електронних доказів;

3) запропонувати авторську класифікацію електронних доказів у кримінальному процесі;

4) проаналізувати національне й міжнародне правове регулювання електронних доказів у кримінальному процесі;

5) окреслити порядок збирання та фіксації електронних доказів у кримінальному провадженні;

6) дослідити умови та критерії допустимості електронних доказів;

7) визначити критерії належності, достатності й достовірності електронних доказів;

8) з'ясувати особливості використання листування в месенджерах як виду електронних доказів;

9) розглянути особливості процесуальної оцінки електронних об'єктів, створених або модифікованих засобами штучного інтелекту, запропонувати відповідні зміни до КПК України;

10) вивчити досвід регулювання електронних доказів у країнах англо-саксонської правової системи;

11) дослідити досвід регулювання електронних доказів у країнах романо-германської правової системи та на рівні Європейського Союзу;

12) проаналізувати досвід регулювання електронних доказів у правових системах Китайської Народної Республіки та Республіки Індія;

13) обґрунтувати напрями вдосконалення правового регулювання електронних доказів у кримінальному процесі України на основі узагальнення іноземного досвіду.

Об'єктом дослідження є суспільні відносини, що виникають у кримінальному провадженні в процесі збирання, фіксації, перевірки, оцінки та використання електронних доказів.

Предметом дослідження є електронні докази як джерела доказів у кримінальному процесі в Україні та світі.

Методологія дисертаційного дослідження. Пізнання електронних доказів як порівняно нового феномену кримінального процесуального права неможливе без визначення методологічної основи, яка забезпечує системність і цілісність дослідження

Методологічною основою дослідження є система загальнонаукових та спеціальних наукових методів і підходів, що забезпечить об'єктивний аналіз досліджуваного предмета, зокрема:

– історично-правовий метод застосовано під час дослідження стану наукової розробленості електронних доказів в Україні та за кордоном (підрозділи 1.1, 3.3);

– діалектичний метод надав можливість розглянути всі питання в динаміці, виявити їх взаємозв'язок і взаємозумовленість, сприяв розумінню об'єкта дослідження щодо поєднання потреб наукової та практичної діяльності органів досудового розслідування й суду (підрозділи 2.1–2.4, 3.2);

– системно-структурний метод застосовано під час визначення ознак електронних доказів, формування авторської координатної класифікації, дослідження проблем, пов'язаних із процесуальним порядком доказування (підрозділи 1.2, 2.2, 3.4);

– порівняльно-правовий метод сприяв зіставленню норм нормативно-правових актів України й іноземних країн, що надало можливість сформулювати конкретні пропозиції для вдосконалення КПК України (підрозділи 1.1, 1.3, 2.2, 3.1–3.4);

– формально-юридичний метод використано для аналізу нормативно-правових актів, тлумачення процесуальних норм й обґрунтування пропозицій стосовно доповнення КПК України, зокрема запропонованої ст. 99-3 (підрозділи 1.3, 2.2, 2.4, 3.4);

– формально-логічні методи (аналіз, синтез, індукція, дедукція) застосовано для обґрунтування висновків і пропозицій стосовно доповнення або уточнення норм КПК України (у всіх підрозділах);

– статистичні методи використано в процесі вивчення й узагальнення слідчої та судової практики, формування та обґрунтування висновків (підрозділи 1.1, 2.1–2.4);

– конкретно-соціологічний метод (анкетування практичних працівників органів прокуратури) застосовано для з'ясування позицій суб'єктів кримінального провадження щодо проблем збирання, перевірки й оцінки електронних доказів, а також для емпіричної перевірки сформульованих у роботі висновків і пропозицій (підрозділи 1.1, 1.3, 2.1–2.4)

Емпіричну базу дослідження становлять Конституція України, Кримінальний процесуальний кодекс України, інші нормативно-правові акти України та зарубіжних країн (Канади, Сполучених Штатів Америки, Великої Британії, Французької Республіки, Федеративної Республіки Німеччина, Китайської Народної Республіки, Республіки Індія); міжнародні акти у сфері кібербезпеки й електронних доказів (Конвенція Ради Європи про кіберзлочинність 2001 року з Другим додатковим протоколом 2022 року; Регламент (ЄС) 2023/1543; Директива (ЄС) 2023/1544; тощо); судові рішення, внесені до Єдиного державного реєстру судових рішень (опрацьовано понад 300 судових рішень); рішення судів інших країн (опрацьовано понад 50 судових рішень); рішення ЄСПЛ; результати анкетування 130 працівників прокуратури з більшості регіонів України.

Під час підготовки дисертації використано досвід роботи дисертанта як захисника в межах кримінальних проваджень.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших в Україні комплексних досліджень теоретичних і практичних проблем використання електронних доказів у кримінальному провадженні з урахуванням зарубіжного досвіду та практики ЄСПЛ, у якому розкрито особливості збирання, перевірки й оцінювання електронних доказів, зокрема електронного листування в месенджерах та доказів, створених або модифікованих

засобами штучного інтелекту (у тому числі дипфейків), а також обґрунтовано пропозиції щодо вдосконалення кримінального процесуального законодавства України. За результатами дослідження сформульовано низку нових наукових положень, висновків і пропозицій, зокрема:

вперше:

– сформульовано авторське функціональне визначення електронного доказу як інформації в електронній формі, що створена, збережена, передана або відображена за допомогою електронних пристроїв, систем чи мереж, містить відомості про обставини, які мають значення для кримінального провадження, і може бути використана як доказ за умови її отримання та перевірки в порядку, передбаченому КПК України;

– запропоновано доповнити КПК України статтею 99-3 «Особливості оцінки електронних доказів, створених або модифікованих засобами штучного інтелекту», яка передбачає три взаємопов'язані елементи: обов'язок учасника провадження розкривати факт використання технологій штучного інтелекту; перерозподіл тягаря доказування автентичності в разі заявлення обґрунтованих сумнівів з підтверджувальними доказами про це; недопустимість електронного доказу штучного походження, не розкритого стороною, що його подала;

– запропоновано координатну авторську класифікацію електронних доказів за п'ятьма взаємодоповнюваними критеріями (способом створення інформації; процесуальним режимом отримання; процесуальним статусом носія; рівнем процесуальної верифікованості; рівнем втручання в право на повагу до приватного життя), що передбачає одночасну характеристику кожного електронного доказу за всіма критеріями і визначає процесуальний маршрут роботи з ним – від моменту виявлення до представлення суду;

– обґрунтовано концепцію трансформації електронного об'єкта на доказ через послідовну систему чотирьох технологічно зумовлених операцій (відтворення електронної інформації засобами програмно-апаратного забезпечення; аналіз її атрибутів і метаданих; описове закріплення в процесуальному документі; вилучення/копіювання з гарантією цілісності через

хешування та фіксацію chain of custody). На відміну від криміналістично-технічних моделей збирання електронних доказів (М. В. Салтевський, А. В. Гутник (Ратнова)), запропонована модель має процесуально-правову природу й визначає мінімальний стандарт належної фіксації, порушення якого тягне недопустимість доказу за ч. 1 ст. 87 КПК України;

– розроблено класифікацію листування в месенджерах як окремого виду електронних доказів за вісьмома критеріями (кількістю учасників, рівнем доступу, можливістю розміщення контенту, етапом створення, джерелом походження, форматом, змістово-інформаційною складовою, способом формування відповідей), що визначає процесуальний порядок його збирання, фіксації та оцінки;

удосконалено:

– доктринальний підхід до пріоритетності способів збирання електронних доказів шляхом обґрунтування трьох процесуально-правових аргументів – цілісності даних, пропорційності втручання за ст. 8 Конвенції про захист прав людини і основоположних свобод, тенденції судової практики Верховного Суду. На відміну від криміналістично-технічного підходу, який обстоюють М. В. Салтевський, О. В. Сіренко, Д. М. Цехан, запропоноване обґрунтування має процесуально-правову природу та надає можливість реалізувати принцип пропорційності в збиранні електронних доказів;

– доктринальний підхід до достовірності електронного доказу через обґрунтування її динамічної природи – як категорії, що верифікується на кожному наступному етапі провадження через ланцюг поводження (chain of custody). На відміну від традиційного розуміння достовірності як властивості, яку встановлюють одноразово, запропонована концепція переносить chain of custody в площину процесуальної оцінки доказу з кореляцією до норм ст. 87, 91, 95 КПК України;

– систематизовано шість специфічних ознак електронних доказів (нематеріальність, динамічність, відтворюваність, залежність від технічних засобів, відсутність жорсткої прив’язки до матеріального носія, наявність

метаданих) із виокремленням метаданих як ознаки, що має самостійне доказове значення;

набуло подальшого розвитку:

– наукове обґрунтування оптимальної моделі регулювання електронних доказів для України на підставі комбінованої моделі, що поєднує формалізований елемент (чіткі законодавчі критерії допустимості за зразком США й Канади), прагматичний елемент (суддівська дискреція в оцінці доказу за сутністю за зразком Великої Британії) і наднаціональний каркас транскордонного доступу (механізми European Production Order та European Preservation Order Регламенту (ЄС) 2023/1543). На відміну від підходів механічної рецепції окремих національних моделей, запропонована модель ґрунтується на інтегративному поєднанні елементів різних правових традицій в контексті курсу України на членство в Європейському Союзі;

– науковий напрям з удосконалення системи негласних слідчих (розшукових) дій у КПК України шляхом обґрунтування запровадження інституту дистанційного проникнення до інформаційних систем на трьох принципах, виявлених під час порівняльного аналізу моделей Великої Британії, Німеччини та Франції: обов'язковість попередньої судової санкції; обмеження кола злочинів вичерпним переліком тяжких й особливо тяжких кримінальних правопорушень; заборона збирання даних «ядра приватного життя»;

– аргументовано доктринальне положення про презумпцію допустимості електронної форми доказу, згідно з яким електронна форма не є самостійною підставою недопустимості, а підстави для визнання доказу недопустимим повинна доводити сторона, яка оспорює доказ, посилаючись на конкретні порушення процесуального порядку.

Практичне значення одержаних результатів полягає в тому, що обґрунтовані в дисертації положення впроваджено й може бути використано в:

науковій роботі – для подальших наукових досліджень проблем правового регулювання порядку збирання, фіксації, перевірки й оцінки електронних доказів у

кримінальному процесі (акт Національної академії внутрішніх справ від 20.05.2026 року № 177-нд);

практичній діяльності – у роботі Всеукраїнської громадської організації «Асоціація адвокатів України», зокрема під час проведення заходів з підвищення кваліфікації адвокатів і підготовки методичних матеріалів за напрямом використання електронних доказів у кримінальному провадженні. Практичну цінність для адвокатської діяльності становлять обґрунтовані здобувачем підходи до перевірки автентичності, допустимості й цілісності електронних доказів, оцінки окремих їх видів (листування в месенджерах, електронних об'єктів, створених за допомогою штучного інтелекту), а також до перевірки належного суб'єкта, способу та джерела отримання електронних доказів, що сприяє забезпеченню ефективного захисту прав і законних інтересів учасників кримінального провадження (довідка про провадження ВГО «Асоціація адвокатів України» від 08.06.2026 року № 364);

освітньому процесі – під час викладання навчальних дисциплін «Інформаційні технології та системи», «Застосування інформаційних технологій в правоохоронній діяльності», «Аналіз та прогнозування злочинності» під час підготовки навчально-методичних і дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти (акт Національної академії внутрішніх справ від 20.05.2026 року № 176-оп).

Особистий внесок здобувача. Дисертацію виконано самостійно, усі сформульовані наукові положення, висновки та пропозиції є результатом особистих досліджень автора. У наукових працях, опублікованих у співавторстві, особистий внесок здобувача полягає в такому:

– у статті «Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект)» (співавтор – В. Г. Хахановський) – особисто проаналізовано проблеми автентичності електронних доказів, створених або модифікованих засобами штучного інтелекту, обґрунтовано підходи до їх процесуальної перевірки (особистий внесок здобувача – 50 %);

– у статті «Відтворення англомовних назв програмних продуктів у кримінальному процесі: проблеми уніфікування» (співавтор – І. Б. Ментинська) –

особисто визначено процесуальні проблеми використання англомовних назв програмних продуктів і запропоновано підходи до їх уніфікування в кримінальному провадженні (особистий внесок здобувача – 50 %);

– у статті «Персональні дані як електронний доказ у кримінальному процесі» (співавтор – О. М. Машталяр) – особисто окреслено особливості використання персональних даних як електронного доказу та їх співвідношення з гарантіями захисту приватності (особистий внесок здобувача – 50 %);

– у статті «Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad» (співавтор – В. Г. Хахановський) – особисто розроблено класифікацію листування в месенджерах за вісьмома критеріями, досліджено процесуальний режим його збирання, фіксації та оцінки (особистий внесок здобувача – 90 %). Ідеї та розробки, що належать співавторам, у дисертації не використано.

Апробація матеріалів дисертації. Основні положення та висновки дисертації оприлюднено на міжнародних науково-практичних конференціях, зокрема: III Міжнародній науково-практичній конференції «Global trends in science and education» (м. Київ, 7–9 квітня 2025 року); IX Міжнародній науково-практичній конференції «Future of Science: Innovations and Perspectives» (м. Стокгольм, 14–16 липня 2025 року); Міжнародній науково-практичній конференції молодих вчених та здобувачів вищої освіти «Проблеми та перспективи використання можливостей систем штучного інтелекту в праві, психології та правоохоронній діяльності» (м. Київ, 27 травня 2026 року).

Публікації. Основні положення та висновки дисертації оприлюднено в сімох наукових статтях, опублікованих у наукових виданнях, включених до переліку фахових видань України, а також двох тезах доповідей на міжнародних науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, трьох розділів, що об’єднують одинадцять підрозділів, висновків, списку використаних джерел (242 найменувань на 25 сторінках) і 3 додатків. Повний обсяг дисертації становить 220 сторінок, із них основний текст – 159 сторінок.

РОЗДІЛ 1
ВИЗНАЧЕННЯ, ОЗНАКИ, КЛАСИФІКАЦІЯ ТА ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ

1.1. Стан наукових досліджень. Поняття електронних доказів

Розвиток електронного середовища зумовив активне використання інформації в електронній формі в кримінальному провадженні, однак у теорії кримінального процесу й досі не сформовано єдиного підходу до визначення її процесуальної природи. Дискусійними залишаються питання як термінології, так і місця електронних доказів у системі джерел доказів, їх співвідношення з документами та речовими доказами.

Причинами розбіжностей у підходах є специфічна природа інформації в електронній формі, її ознаки й особливості. На відміну від традиційних документів, електронні дані можуть бути змінені без видимих зовнішніх ознак, існувати в множинних ідентичних копіях, залежати від технічного середовища для сприйняття та містити метадані, що мають самостійне доказове значення. Саме ці властивості ускладнюють механічне застосування до них процесуальних конструкцій.

Однією з ключових особливостей електронних доказів є їхня відносна вразливість до змін. Це наочно простежується в порівнянні з паперовими документами: внесення непомітних суттєвих змін до тексту, виконаного ручкою на папері, є вкрай ускладненим, оскільки такі зміни залишають очевидні візуальні ознаки (почерк, колір чорнила, товщина ліній тощо).

Натомість перевірка внесення змін до електронного документа потребує використання спеціальних знань і технічних засобів. Зокрема, візуальний огляд електронного тексту не дає змоги встановити його первинний вигляд або виявити факт внесення змін, оскільки такі зміни можна виявити шляхом дослідження

метаданих, хеш-значень тощо. Для виявлення та оцінки таких даних необхідні спеціальні знання.

Детальне порівняння внесення змін до паперового й електронного документів здійснено в статті G. C. Kessler «Judges' Awareness, Understanding, and Application of Digital Evidence» («Обізнаність, розуміння та застосування цифрових доказів суддями») [208].

На нашу думку, специфіка інформації в електронній формі є не другорядною технічною особливістю, а обставиною, що безпосередньо визначає її процесуальну природу, порядок збирання, фіксації, дослідження та підходи до оцінки в кримінальному провадженні.

Саме тому в теорії кримінального процесу немає єдиного підходу до визначення поняття електронного доказу, його співвідношення з документами та речовими доказами, а також щодо питання доцільності виокремлення його як самостійної процесуальної категорії.

До найпоширеніших категорій електронних доказів у кримінальному процесі належать електронні документи, цифрові аудіо- та відеозаписи, а також інші електронні дані. Їхня унікальність полягає у високому рівні інформативності, мобільності й можливості швидкого аналізу, що додає їм значущості в процесах досудового розслідування та судового розгляду.

Серед науковців переважають два підходи до визначення електронних доказів як окремого виду:

– консервативна позиція полягає в тому, що електронний доказ не є окремим джерелом, а лише різновидом документа або речового доказу. Ця позиція ґрунтується на тому, що електронні докази відносять до документів або речових доказів, вони не потребують виокремлення як самостійної категорії [91];

– інноваційна позиція – електронний доказ є окремим видом джерела доказів, що має унікальні властивості та потребує спеціального правового режиму [60; 77].

Інноваційна позиція ґрунтується на специфічній електронній формі доказу, його природі й особливостях, що своєю чергою зумовлює окремий порядок

збирання, збереження та дослідження (вимагає використання комп'ютерних технологій для пошуку, збереження і використання).

Однак є й інші позиції стосовно того, чи є електронний доказ окремим видом.

Зокрема, М. А. Погорецький стверджує, що електронні докази не слід тлумачити як позначення окремого, самостійного виду доказів у кримінальному процесі, це узагальнена вказівка на електронну (цифрову) форму фіксації тих видів доказів, які вже визначені чинним кримінальним процесуальним законодавством України [91, с. 124].

У цьому сенсі йдеться про електронну (цифрову) форму показань, речових доказів, документів або висновків експертів, передбачених ч. 2 ст. 84 КПК України, процесуальна природа яких не змінюється залежно від способу їх технічного закріплення, а визначена джерелом походження, порядком отримання та легалізації в кримінальному провадженні.

Однак ми не поділяємо таку думку, оскільки жоден із доказів, передбачених КПК України, не має метаданих («мовчазних свідків» електронних доказів), які можуть підтвердити або спростувати відомості, що містить електронний об'єкт, а також те, що електронні докази містяться в електронному середовищі й не можуть бути вилучені в матеріальний світ.

М. А. Погорецький також доводить, що цифрова форма є «технічно зумовленим способом фіксації», аналогічним письмовій або матеріальній формі, а власне електронні дані можна звести до наявних видів доказів (речові докази або документи) [91, с. 120].

Проте цей підхід, на нашу думку, не цілком ураховує принципову онтологічну відмінність: традиційний документ невіддільний від свого матеріального носія, натомість електронний доказ від нього не залежить.

Водночас слід зазначити, що позиція М. А. Погорецького точно відображає стан чинного законодавства, у якому електронні докази справді не мають самостійного процесуального статусу. Однак це свідчить не про правильність доктринального підходу, а про прогалину в законодавстві, яку необхідно усунути.

Специфіка електронних доказів, зокрема технічна складність процесів їх збирання та зберігання, може створювати бар'єр для сприйняття учасниками процесу.

Показовим є випадок із французької судової практики: під час допиту експерта, який описував процедуру вилучення електронних об'єктів, суддя перервав його свідчення й зауважив: «Зараз ви розмовляєте з 12 громадянами. Будь ласка, розмовляйте французькою, бо те, що ви щойно сказали, незрозуміле», – вказуючи не на мову спілкування, а на перенасиченість свідчень технічною термінологією [155].

Зазначене засвідчує, що проблема визначення поняття та правової природи електронних доказів має не лише доктринальне, а й безпосередньо практичне значення: неналежне розуміння специфіки цифрових доказів учасниками кримінального провадження може призвести до неправомірного засудження або необґрунтованого виправдання [193; 236].

Визначення поняття електронних доказів є непростим завданням, оскільки, попри наукові дискусії, очевидної одностайності серед учених не вбачається.

Науковці під час дослідження інформації в електронному вигляді як доказу в кримінальному процесі використовують такі терміни: *«електронні відображення»* [84, с. 16; 85, с. 19]; *«електронні документи»* [113, с. 184; 140, с. 15]; *«електронні докази»* [2, с. 194; 73, с. 73]; *«електронні (цифрові) докази»* [51, с. 5]; *«цифрові докази»* тощо.

На нашу думку, така варіативність підходів зумовлена фрагментарністю наукових позицій, що ускладнює розроблення узгодженої процесуальної концепції. Дискусії щодо оптимального поняття «електронних доказів» триватимуть до моменту закріплення терміну в кримінальному процесуальному законодавстві.

Термін «електронне відображення» в науковий простір ввели Ю. Ю. Орлов і С. С. Чернявський, які дійшли висновку, що «електронним відображенням є цілісна система відомостей та (або) комп'ютерних інструкцій в інформаційній мережі або

на технічному носієві, яка може бути використана як доказ факту чи обставин, що встановлюють під час кримінального провадження» [86, с. 21].

Відповідно до визначення, яке пропонує тлумачний словник української мови, «відображення – це: зображення предмета, відбите в дзеркалі, на поверхні води, полірованій речі тощо» [7, с. 164].

Тобто поняття «електронне відображення», на нашу думку, застосовують щодо вже сформованих копій речового доказу або документа як електронних доказів.

С. М. Стахівський визначає електронний документ як комп'ютерну інформацію загалом, яка має доказове значення в кримінальному провадженні, та пропонує використання комп'ютерної мережі в процесі доказування [120, с. 21].

У дисертаційному дослідженні С. Й. Гонгало визначає електронний документ як різновид традиційного документа, що відрізняється від нього лише електронно-цифровою формою та потребує розкодування – візуалізації [45].

Підхід щодо віднесення інформації в електронній формі до різновиду документа має перевагу, яка полягає в узгодженості з чинною конструкцією ст. 99 КПК України, а також недоліки, які полягають у тому, що не цілком враховано такі властивості електронної інформації, як відсутність сталого зв'язку з матеріальним носієм, можливість існування в електронному середовищі й самостійне доказове значення метаданих.

На нашу думку, поняття «електронні відображення» та «електронні документи» є термінами, які характеризують певну форму (відображення) або вид доказу (документа).

У методичних рекомендаціях з використання доказів в електронній формі науковці В. Д. Гавловський, М. В. Гуцалюк, В. Г. Хахановський визначають електронні докази як докази в кримінальних провадженнях, які можна отримати в електронній формі [9, с. 7; 50, с. 8]. Автори зазначають, що їх отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, зокрема через інтернет. Допустимими для сприйняття

людиною вони стають після обробки засобами комп'ютерної техніки [10, с. 7; 50, с. 8].

Схоже визначення пропонують Д. Алєксєєва-Процюк і О. М. Брисковська, які вважають, що електронні докази – це фактичні дані, які зберігаються в електронному вигляді на будь-яких типах електронних носіїв і в електронних засобах та які після обробки спеціальними технічними засобами та програмним забезпеченням стають доступними для сприйняття людиною [1, с. 250].

О. В. Сіренко вважає, що електронні докази – це дані про обставини, що мають значення для кримінального провадження, існують у нематеріальному вигляді в межах технічного носія чи каналу зв'язку, сприйняття і дослідження яких можливе за допомогою технічних засобів і програмного забезпечення [127, с. 211].

Також О. Котляревський та Д. Киценко електронні докази визначають як сукупність інформації, яку зберігають в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах [73, с. 73].

З огляду на наукові джерела іноземних країн, у яких активно застосовують термін «digital evidence», що означає «цифровий доказ», Д. А. Цехан вважає за доцільне використовувати саме цей термін [137, с. 257, 259].

На думку О. Ю. Гусєва, інформацію, що зчитує електронно-обчислювальна машина, доцільно визначати як «цифрову», оскільки вона існує у формі закодованих символів, натомість пристрої для її обробки є електронними. Водночас питання про доцільність такого розмежування залишається дискусійним [48, с. 64].

На офіційних ресурсах органів судової влади, прокуратури та правоохоронних органів паралельно використовують терміни «електронні докази», «електронно-цифрові докази», «цифрові докази» та «цифрові зображення» [63; 64; 122; 123; 130; 131], що свідчить про термінологічну неузгодженість навіть на рівні державного управління.

Слід зазначити, що експерти Scientific Working Group on Digital Evidence визначили термін «цифрові докази» як будь-яку інформацію доказового значення, що зафіксована чи передана в цифровій формі [232].

Ю. Ю. Орлов визначає електронний слід як відображення матеріального сліду в інформаційно-телекомунікаційній системі та відмежовує його від електронного відображення, яке є ширшим поняттям й охоплює електронні сліди [85, с. 21].

І. А. Смаль пропонує тлумачити електронний доказ як інформацію в електронній формі, що відповідає трьом вимогам: містить відомості, релевантні для предмета доказування в кримінальному провадженні; створена, збережена або передана за допомогою електронних пристроїв, систем чи мереж; існує у формі, що забезпечує її автентичність, цілісність і придатність для дослідження [119, с. 97].

На нашу думку, включати до дефініції такі характеристики, як автентичність і цілісність поняття електронного доказу, є передчасним, оскільки ці властивості є критеріями оцінки вже отриманого доказу (допустимість, достовірність), а не ознаками, що конституюють його як процесуальну категорію. Включення оцінних критеріїв до визначення поняття призводить до логічного парадокса: доказ, автентичність якого поставлена під сумнів, формально перестає бути електронним доказом, хоча саме як електронний доказ він і підлягає дослідженню та оцінці.

І. Г. Каланча електронний доказ визначає як доказ, що існує в електронному середовищі та реалізується за допомогою електронних засобів фіксації, зберігання й обробки інформації [62, с. 65].

Тож у наукових колах тривають активні дискусії щодо визначення електронного доказу, на нашу думку, вони триватимуть до моменту нормативного закріплення поняття в кримінальному процесуальному законодавстві.

З огляду на правозастосовну практику, законодавчу термінологію, використання поняття електронного доказу видається оптимальним у кримінальному провадженні. Інші поняття не цілком відображають зміст, наприклад, у понятті «цифровий доказ» акцентовано на технічному способі фіксації доказу.

Поняття «електронний доказ» охоплює будь-яку інформацію в електронній формі, незалежно від конкретного способу її цифрового кодування, технічної архітектури носія або програмного середовища, у якому таку інформацію

створюють, зберігають чи передають, що забезпечить ефективну процесуальну функцію доказування.

Запропонований термін уже інтегровано в систему суміжних понять, які використовують у юридичній термінології, а саме: «кваліфікований електронний підпис», «електронна ідентифікація» «електронне судочинство», «електронна пошта», натомість «цифровий доказ» наштовхуватиме науковців і правників на дискусії щодо правильності застосування.

З огляду на прагматичний та комунікативний підходи, а також функціональний аналіз, термін оцінюють з позицій зручності використання, зрозумілості для учасників кримінального провадження та відповідності принципу процесуальної економії. У цьому контексті термін «електронний доказ» є інтуїтивно зрозумілим, не потребує спеціальних технічних пояснень і не ускладнює процесуальні документи.

Крім того, використання одного сталого поняття, на нашу думку, сприятиме уніфікуванню судової практики. Натомість застосування технічно ускладнених термінів, зокрема «електронно-цифровий доказ», може ускладнювати правову аргументацію та негативно позначатиметься на єдності правозастосування.

Емпіричні дані засвідчують доктринальну позицію щодо самостійності цієї категорії доказів. За результатами проведеного автором анкетування[1], найточнішим для позначення інформації в електронній формі, що використовують як доказ, 49,2 % опитаних вважають термін «електронний доказ»; натомість «електронний документ (як підвид документа)» обрали 24,6 %, «цифровий доказ» – 17,7 %, «електронне відображення» – 2,3 %, а 6,2 % не визначилися. Такі результати додатково підтверджують авторський підхід (додаток В, рис. 3).

З огляду на окреслені вище особливості електронних об’єктів як доказу, а також на підставі аналізу наявних підходів ми можемо сформулювати авторське

[1] Анкетування проведено за допомогою Google-форми. В опитуванні взяли участь 130 працівників прокуратури з більшості регіонів України (Вінницької, Волинської, Дніпропетровської та інших областей). Серед них переважають фахівці зі стажем служби понад 10 років (78,5 %); досвід роботи з електронними доказами мали 71,6 % опитаних. Зведені результати наведено в додатку В.

визначення поняття «електронний доказ»: це інформація в електронній формі, що створена, збережена, передана або відображена за допомогою електронних пристроїв, систем чи мереж, містить відомості про обставини, які мають значення для кримінального провадження, і може бути використана як доказ за умови її отримання та перевірки в порядку, передбаченому КПК України.

Запропоноване визначення відрізняється від наявних у доктрині за кількома принциповими параметрами. На відміну від визначення М. В. Гуцалюка, В. Д. Гавловського та В. Г. Хахановського, у якому акцентовано на технічному аспекті отримання інформації (за допомогою електронних пристроїв, комп'ютерних носіїв) та її подальшій обробці для сприйняття людиною, запропоноване визначення не зводить електронний доказ до результату технічної обробки, а охоплює інформацію в усіх формах її існування в електронному середовищі – від моменту створення до моменту процесуального використання.

На відміну від визначення І. Г. Каланчі, яке оперує категорією «електронне середовище» без його конкретизації, запропоноване визначення деталізує способи існування інформації (створеної, збереженої, переданої або відображеної), що забезпечує процесуально-операціональну дефініцію та її придатність для правозастосування.

Від визначень, закріплених у ч. 1 ст. 100 ЦПК України, ч. 1 ст. 96 ГПК України та ч. 1 ст. 99 Кодексу адміністративного судочинства України, запропоноване визначення відрізняється тим, що його сформульовано з огляду на специфіку кримінального провадження: замість вказівки на «обставини, що мають значення для справи» (цивілістична конструкція), використано формулювання «обставини, які мають значення для кримінального провадження» з прямою прив'язкою до порядку отримання та перевірки, передбаченого КПК України, що відображає публічно-правовий характер кримінального процесу й підвищені вимоги до законності збирання доказів.

Крім того, дефініції в інших процесуальних кодексах України побудовані на підставі переліку типових форм електронних доказів: «електронні документи,

вебсайти, текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі».

Такий перелік, на нашу думку, є невичерпним і швидко розширюється з розвитком технологій, що породжує сумніви щодо процесуального статусу нових цифрових об'єктів (об'єктів, створених штучним інтелектом, токенів блокчейну, NFT-об'єктів, скриптів тощо).

Запропоноване функціональне визначення через ознаки створення, збереження, передачі або відображення інформації за допомогою електронних пристроїв, систем чи мереж охоплюватиме будь-які майбутні форми електронних об'єктів незалежно від їх властивостей, призначення, що вкрай актуально, з огляду на стрімкий розвиток технологій штучного інтелекту.

Обраний нами підхід до формулювання через форму існування інформації та її процесуальну функцію без включення автентичності та цілісності до дефініції поняття кореспондує також із провідними іноземними моделями.

Зокрема, ст. 31.8 Canada Evidence Act [156] визначає електронний документ через дані, записані або збережені на будь-якому носії в комп'ютерній системі чи іншому схожому пристрої, які можуть бути прочитані або сприйняті особою, комп'ютерною системою чи іншим пристроєм. Він охоплює відображення, роздруківку або інший вид цих даних.

Однак алгоритм доведення автентичності та цілісності доказів закріплено в ст. 31.3 Canada Evidence Act [156] як окремий інститут презумпції цілісності системи.

Отже, ми розглядаємо електронний доказ як самостійне джерело доказів передусім через правову природу відповідного об'єкта: його доказова цінність зумовлена не матеріальними властивостями предмета, а інформацією, що існує в електронному середовищі. Така інформація може існувати незалежно від конкретного носія, містить метадані й потребує спеціальних технічних засобів для дослідження. Зазначені ознаки не дають змоги цілком звести електронний доказ ні до документа, ні до речового доказу в їх класичному процесуальному значенні.

Крім того, електронні дані, такі як логи автоматизованих систем, дані геолокації, записи смартконтрактів у блокчейні, не мають ані автора в правовому розумінні, ні матеріального носія в традиційному сенсі. Тому віднесення електронних доказів до «документів» (ч. 1 ст. 99 КПК) є тимчасовим юридичним механізмом, а не доктринальним рішенням.

Позицію щодо самостійності та широкого кола електронних доказів підтверджує і Верховний Суд. У постанові Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20) [107] сформульовано низку правових висновків, які мають значення для визначення поняття електронних доказів.

Зокрема, суд зазначив, що допустимість електронного документа як доказу не можна заперечувати виключно на підставі того, що він має електронну форму; один і той самий електронний документ може існувати на різних носіях, і всі ідентичні за змістом примірники електронного документа можна розглядати як оригінали; ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки відмітною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія [107].

Ця правова позиція є знаковою, оскільки ВС фактично визнав, що електронні докази вирізняються з-поміж традиційних видів доказів низкою сутнісних ознак, які не дозволяють повністю ототожнити їх ані з документами, ані з речовими доказами в їх класичному розумінні, що кореспондує з обґрунтованою вище позицією щодо необхідності законодавчого закріплення електронного доказу як самостійного виду доказів.

На нашу думку, за теперішньої ситуації практики змушені використовувати комп'ютерні дані як один із видів доказів, які передбачені КПК України, аби використати їх як докази. Водночас використання електронних даних у межах наявних видів доказів створює юридичні невизначеності.

З огляду на викладене, вважаємо обґрунтованою позицію, згідно з якою електронні об’єкти є окремим видом доказів у кримінальному процесі та потребують законодавчого закріплення.

1.2. Ознаки та класифікація електронних доказів

Для з’ясування правової природи електронних доказів необхідно виокремити їхні загальні та спеціальні ознаки. Загальні ознаки характеризують електронні докази як засіб доказування в кримінальному процесі, натомість спеціальні відображають їх відмінність від традиційних форм доказової інформації.

До загальних ознак, наприклад, можна віднести те, що для застосування в доказовому процесі електронні докази мають відповідати вимогам КПК України щодо належності, допустимості, достовірності й достатності [76].

До спеціальних ознак електронних доказів О. В. Гаран відносить такі:

1) використання спеціальних технічних засобів під час створення та відтворення; 2) незмінність під час копіювання; 3) можливість одночасного існування в кількох місцях; 4) нематеріальна форма; 5) можливий дистанційний вплив; 6) складне нормативно-правове регулювання; 7) різноманітність змісту; 8) динамічність правової природи; 9) потенційно безстрокове збереження [43, с. 127].

Меншу кількість ознак електронних доказів виокремлює А. Ю. Каламайко: 1) неможливість безпосереднього сприйняття інформації, що обумовлює необхідність використання технічних і програмних засобів для одержання відомостей; 2) наявність технічного носія інформації; 3) можливість легко змінювати носій без втрати змісту; 4) відсутність поняття «оригінал» електронних засобів доказування через цілковиту ідентичність електронних копій; 5) наявність специфічних «реквізитів», так званих метаданих – інформації технічного характеру, яку закодовано всередині файлів [61, с. 129].

На думку Д. О. Алєксєєвої-Процюк, О. М. Брисковської, загальними ознаками електронних документів є такі: 1) існують у нематеріальному вигляді; 2) створені людиною або комп'ютерною системою; 3) не можуть існувати поза межами фізичного носія або каналу зв'язку; 4) не мають нерозривного зв'язку з матеріальним носієм; 5) вільно переміщуються в електронній мережі; 6) сприйняття та дослідження таких документів можна здійснювати лише з використанням спеціальних програм і пристроїв; 7) потребують спеціального порядку збирання, перевірки й оцінки; 8) мають здатність до дубляжу, тобто копіювання або переміщення на інший носій без втрати характеристик; 9) можливість дистанційного внесення змін до них та їх знищення [1, с. 252].

Порівняльний аналіз різних позицій надає можливість виокремити ознаки, щодо яких більшість дослідників є одностайними: 1) неможливість безпосереднього сприйняття без спеціальних технічних і програмних засобів; 2) ідентичність копій оригіналу – здатність до дублювання без втрати змісту; 3) нематеріальна форма існування та відсутність жорсткої прив'язки до конкретного матеріального носія; 4) вразливість до дистанційного впливу – можливість модифікації або знищення без видимих зовнішніх ознак.

Однією з найважливіших ознак, на нашу думку, є наявність в електронних доказах такої властивості, як метадані. Електронний об'єкт під час створення, редагування, переміщення обов'язково залишає про це у відповідному середовищі сліди, які можуть містити різні відомості (час і дату, геодані, автора маніпуляцій тощо).

Саме метадані дають змогу встановлювати технічну історію створення, зміни, переміщення та використання електронного об'єкта. У цьому аспекті метадані можуть мати не лише допоміжне, а й самостійне доказове значення.

На нашу думку, критерії допустимості й достовірності, розроблені для письмових або матеріальних доказів, виявляються недостатніми, оскільки електронні дані потребують додаткової верифікації через технічні засоби підтвердження незмінності (наприклад, шляхом хешування, перевірки метаданих, дотримання chain of custody).

Ігнорування цих вимог рівнозначне оцінці доказу без урахування природи об’єкта, який оцінюють. На необхідності дотримання комплексу технологічних і процесуальних гарантій під час роботи з електронними доказами в кримінальному провадженні акцентують у монографії й А. В. Гутник та А. Я. Хитра [49, с. 75–85].

Аналіз правової природи електронних доказів дає змогу виокремити сукупність специфічних ознак, що принципово відрізняють їх від традиційних форм доказової інформації:

1) нематеріальність – електронний доказ існує поза фізичним субстратом у класичному розумінні: його зміст не тотожний матеріальному носію та не зникає разом із його знищенням, що унеможливлює застосування до нього традиційних підходів до вилучення та зберігання речових доказів;

2) динамічність – цифрова інформація здатна змінюватися, оновлюватися або знищуватися без зовнішніх видимих слідів, що суттєво підвищує ризик непомітної модифікації та обумовлює необхідність її невідкладної фіксації з моменту виявлення;

3) відтворюваність – електронний доказ допускає необмежене копіювання без втрати змісту, що знімає проблему «єдиного оригіналу» в традиційному розумінні, водночас породжуючи питання процесуальної рівнозначності копій та порядку підтвердження їх ідентичності першоджерелу;

4) залежність від технічних засобів – сприйняття, відтворення і дослідження електронного доказу неможливе без відповідного програмно-апаратного забезпечення, що на всіх стадіях роботи з ним об’єктивно вимагає залучення спеціальних знань у галузі інформаційних технологій та цифрової криміналістики;

5) відсутність жорсткої прив’язки до матеріального носія – одна й та сама інформація може одночасно існувати на кількох носіях або в хмарному середовищі, що ускладнює застосування класичних процесуальних механізмів тимчасового доступу, виїмки та забезпечення збереження доказів;

6) наявність метаданих – невіддільним атрибутом цифрової інформації є супутні технічні дані про час створення, джерело походження, історію змін і маршрут передачі, які можуть мати самостійне доказове значення та відкривають

можливості для встановлення обставин провадження, не доступні в роботі з традиційними документами.

Виокремлені ознаки електронних доказів знаходять підтвердження в практиці Верховного Суду. Зокрема, ознаку відсутності жорсткої прив'язки до матеріального носія та ознаку відтворюваності безпосередньо підтверджено в постанові Першої палати ККС ВС від 30 вересня 2021 року у справі № 498/582/18, де суд зазначив, що ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки відмітною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія (п. 31 постанови) [103].

Зазначена правова позиція ВС підтверджує обґрунтованість запропонованої класифікації ознак і водночас засвідчує, що судова практика вже фактично сприймає електронні докази як об'єкти з якісно іншими властивостями, порівняно з традиційними документами та речовими доказами, хоча законодавчо це розмежування досі не закріплено.

Класифікація доказів має на меті впорядкування неоднорідного доказового матеріалу та виокремленні груп, що мають спільні сутнісні риси. Прикладне призначення класифікації виявляється в тому, що віднесення доказу до певної групи безпосередньо орієнтує суб'єкта доказування у виборі способу його отримання, тактики перевірки та критеріїв оцінки.

Слід зазначити, що С. М. Стахівський визначає класифікацію доказів як їх поділ з метою дослідження складових цієї системи. Завдяки їй з'ясовують особливості збирання, перевірки та оцінки доказів, їх значущість для доведення обставин, що належать до предмета доказування. Таке багатопланове значення класифікації доказів свідчить, що здійснити поділ доказів за однією ознакою чи властивістю неможливо [120, с. 17].

Електронні докази вирізняються технологічною різноманітністю інформації – від статичних файлів аж до динамічних мережевих потоків, що своєю чергою не дає змоги застосовувати уніфікований процесуальний підхід.

Оскільки інформація в електронному вигляді може існувати в різноманітних форматах, її здобувають різними шляхами та на різних правових підставах, то є різні підходи до класифікації електронних доказів.

Залежно від джерел походження електронних доказів науковці пропонують такі класифікації:

– С. С. Чернявський, Ю. Ю. Орлов виокремлюють: портали, сайти в комп'ютерній мережі; електронні бази даних; файли та групи файлів; зміст електронної пошти, чатів; вихідні й виконувані модулі комп'ютерних програм; інші відомості та (або) комп'ютерні інструкції в інформаційній мережі або на технічному носієві [139, с. 112–124];

– І. Вернидуб, С. Белікова пропонують таку класифікацію: 1) електронні документи; 2) інформація, отримана з відкритих джерел мережі Інтернет; 3) аудіо- та відеозаписи; 4) електронні повідомлення: мультимедійні та голосові повідомлення [8, с. 302];

– деталізовану типологію джерел електронної інформації, які можна розглядати як докази в судовому процесі, запропонував О. Т. Боннер, який виокремлює: 1) аудіо- та відеозаписи; 2) електронні документи; 3) відомості, отримані з глобальних інформаційних систем (зокрема мережі Інтернет); 4) електронну пошту; 5) свідчення (показання) спеціальних технічних засобів (наприклад, прилади обліку витрат електроенергії, води, газу, тепла; прилади визначення швидкості транспортного засобу чи ступеня алкогольного сп'яніння водія тощо); 6) засоби «електронного судочинства» (відеоконференції, офіційні вебсайти судових органів, листування із судовими органами за допомогою електронної пошти, автоматизовані судові інформаційні системи тощо) [5, с. 46–48].

Перевага підходу, орієнтованого на джерело походження, полягає в його технологічній наочності. Дослідник одразу бачить, де саме слід шукати інформацію та яким способом її фіксувати.

Така диференціація має безпосереднє значення для оперативної роботи слідчого, оскільки вибір процесуальної дії (огляд, обшук, тимчасовий доступ, запит до провайдера) залежить від типу джерела.

Поширеність окремих видів електронних доказів підтверджують і результати проведеного автором анкетування: найчастіше в практичній діяльності респонденти опрацьовують листування в месенджерах (78,5 %) та відео-, аудіозаписами, фотографії (76,2 %); далі – вміст інтернет-сайтів і вебсторінок (47,7 %), дані соціальних мереж (46,2 %), інформацію електронних баз даних і реєстрів (38,5 %), дані геолокації (30,0 %), електронну пошту (27,7 %), дані хмарних сховищ (6,9 %) і матеріали, згенеровані штучним інтелектом (0,8 %). Це засвідчує доцільність класифікації електронних доказів, зокрема за джерелом походження інформації (додаток В, рис. 6).

Окремим способом класифікації електронних доказів є класифікація за критерієм юридичного статусу електронного об’єкта.

Наприклад, О. В. Шведова поділяє електронні документи на ті, що можуть бути перенесені на фізичний носій і не мають самостійної юридичної сили, і ті, що зберігають юридичну силу безвідносно до носія завдяки наявності електронного цифрового підпису [142].

С. Й. Гонгало вважає, що за стадіями виготовлення електронні документи поділяють на оригінали, дублікати, копії та витяги. Однак цей поділ є доволі умовним, оскільки в деяких випадках неможливо встановити оригінал електронного документа [45, с. 34].

Перевагою цієї класифікації є безпосередня прив’язка до процесуальних наслідків: наявність чи відсутність кваліфікованого електронного підпису істотно впливає на доказову вагу електронного документа, а статус оригіналу або копії визначає правила оцінки достовірності.

Розгорнуту класифікацію електронних доказів надає А. В. Гутник (Ратнова) у статті «Класифікація електронних документів як джерел доказів у кримінальному провадженні», яка пропонує власну класифікаційну систему, що ґрунтується на шести критеріях (за комбінацією метаданих – документи однорангові, дворангові,

трирангові, чотирирангові та п’ятирангові – гіпертекстові; за доступом до інформації – з відкритими та прихованими метаданими; за ступенем захисту – відкриті та закриті; за джерелом походження – створені користувачем або електронним середовищем; за розміщенням – на персональних пристроях, серверах, носіях побутової техніки; за формою подання – відеозаписи, аудіозаписи, повідомлення, вебсайти тощо) [112, с. 42–47].

І. А. Смаль, аналізуючи різноманітні підходи, зазначає, що складність класифікації електронних доказів зумовлена їхньою технічною неоднорідністю, мінливістю форм існування інформації та постійною появою нових технологій, які виходять за межі усталених класифікаційних рамок [119, с. 77].

Ми поділяємо думку дослідника, що блокчейн-технології, криптовалютні транзакції, дані із систем штучного інтелекту й нейромережевих алгоритмів є тими формами електронної інформації, для яких класифікаційні моделі попередніх років виявилися непридатними.

І. Г. Каланча своєю чергою зауважує, що класифікаційні поділи не повинні підміняти оцінні критерії доказів (належність, допустимість, достовірність, достатність) і виконують насамперед упорядковувальну й евристичну функції [62, с. 67].

Підходи до класифікації електронних доказів за джерелом походження, способом отримання та характеристиками інформації, а також відповідний закордонний досвід (США, Велика Британія, Канада, Австралія, Німеччина, Японія) узагальнено в попередній публікації [89]. Водночас подальший аналіз засвідчив, що такі моделі залишаються переважно одновимірними та не враховують, зокрема, об’єктів, створених штучним інтелектом.

Узагальнюючи проаналізовані підходи українських дослідників, можна стверджувати, що вони не цілком охоплюють специфіку електронних доказів у комплексному процесуально-правовому вимірі: класифікації за джерелом походження орієнтовані переважно на технічну природу носія; класифікації за формою подання змішують різні підстави поділу; класифікації за юридичним статусом поки обмежені сферою електронних документів і не охоплюють

динамічних форм електронної інформації; жодна з наявних класифікацій не враховує об’єктів, створених штучним інтелектом.

З огляду на викладене, на основі систематизації наявних доктринальних підходів й узагальнення матеріалів судової практики видається обґрунтованим запропонувати авторську класифікацію електронних доказів у кримінальному процесі, побудовану на п’яти координатних критеріях: 1) за способом створення інформації; 2) за процесуальним режимом отримання; 3) за процесуальним статусом носія; 4) за рівнем процесуальної верифікованості; 5) за рівнем втручання в право на повагу до приватного життя.

За цією класифікацією кожен конкретний електронний доказ може бути одночасно описаний за всіма п’ятьма критеріями, а їх комбінація визначає процесуальний режим його отримання, перевірки й оцінки.

Критерій способу створення інформації залежить від ступеня та характеру участі людини у формуванні електронної інформації і може бути таких видів: електронні докази, створені людиною, створені комп’ютером, комбіновані електронні докази; електронні докази, створені ШІ.

Електронні докази, які створені людиною, створює безпосередньо особа з використанням електронних технологій як інструменту, вони можуть бути, наприклад, у формі електронного листування в месенджерах і поштових сервісах, текстових або голосових повідомлень тощо.

Доказове значення цієї групи зосереджене в змісті інформації, а технічна форма є лише носієм авторської волі. Типовий приклад: листування підозрюваного в месенджері Telegram, у якому викладено зміст домовленостей про вчинення кримінального правопорушення.

Електронні докази, створені комп’ютером, – це інформація, що утворюється внаслідок звичайного функціонування технічних засобів й інформаційних систем без безпосередньої спрямованої діяльності людини, може бути у формі записів камер відеоспостереження, даних відеореєстраторів, GPS-трекерів тощо.

Доказове значення цієї групи зосереджене переважно у факті створення (що зафіксовано системою), і ця обставина зумовлює специфічні правила оцінки:

відсутність авторського наміру не виключає, а посилює доказову значущість, оскільки інформація менше піддається довільному маніпулюванню. Типовий приклад – запис камери відеоспостереження банківської установи, на якому зафіксовано момент вчинення кримінального правопорушення.

Під час створення інформації доказового значення, у якій поєднані авторська воля людини й автоматичні процеси інформаційної системи, ідеться про комбіновані електронні докази. Такі докази можуть бути у формі електронних документів із кваліфікованим електронним підписом (де змістова частина створена особою, а реквізити автентифікації – технічно фіксовані), електронна пошта з повним заголовком (де лист є створеним особою, а службові метадані сервера – технічно фіксованими) тощо

Особливість цієї групи полягає в тому, що різні елементи доказу можуть оцінювати за різними доказовими стандартами (авторський зміст – за стандартами оцінки людських тверджень, технічні реквізити – за стандартами оцінки технічно фіксованих даних). Типовий приклад – електронний лист із вкладеним документом, у якому текст листа і вкладення створені людиною, а службові заголовки маршрутизації (Received, Message-ID, часові мітки, тощо) згенеровані автоматично поштовою системою.

Окрему категорію, яку неможливо віднести до перелічених вище, становлять електронні докази, створені засобами ШІ. Така доказова інформація є результатом самостійної роботи алгоритмів і систем штучного інтелекту без безпосередньої авторської волі людини стосовно конкретного результату: тексти, зображення, аудіо- й відеоконтент, згенеровані генеративними нейромережами (ChatGPT, Midjourney). Типовий приклад такого доказу – штучно згенероване (дипфейк) відео або зображення, яке зовні відтворює образ певної особи, але створене засобами ШІ без її участі.

Виокремлення цієї групи як самостійної є принципово важливим з огляду на її швидке поширення в сучасній правозастосовній практиці та специфічні проблеми верифікації, які детальніше розглянуто в підрозділі 2.4 цього дослідження.

Така класифікація кореспондує і з підходом D. Seng, який класифікує електронні докази за ступенем участі людини в їх створенні: real evidence (дані, згенеровані системою без участі людини), hearsay evidence (записи людських тверджень) та derived evidence (результати алгоритмічної обробки) [216].

За процесуальним режимом отримання електронних доказів, які вилучають залежно від процесуальної дії, передбаченої КПК України, можна виокремити чотири взаємовиключні групи: безпосередньо вилучені; отримані через тимчасовий доступ до речей і документів; отримані через негласні слідчі (розшукові) дії; отримані через міжнародне співробітництво.

Безпосередньо вилучені електронні докази отримують шляхом вилучення відповідних електронних носіїв або їх копіювання електронних доказів під час обшуку (ст. 234–236 КПК України), огляду (ст. 237 КПК України) або добровільного надання учасником провадження: дані з вилучених комп'ютерів, смартфонів, флешнакопичувачів, жорстких дисків, серверів, що знаходяться у фізичному володінні особи. Типовий приклад – жорсткий диск, вилучений з персонального комп'ютера підозрюваного під час обшуку за місцем його проживання.

Отримані через тимчасовий доступ до речей і документів – це докази, які знаходяться переважно у володінні третьої особи (наприклад, оператора електронних комунікацій, провайдера хмарних послуг, банківської установи, провайдера соціальної мережі) й отримання яких потребує ухвали слідчого судді на тимчасовий доступ за ст. 159–166 КПК України: вміст електронних поштових скриньок на серверах провайдера, дані банківських транзакцій, записи телефонних з'єднань, листування в месенджерах за серверним протоколом. Типовий приклад – витяг про банківські транзакції, отриманий від банківської установи на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів.

Електронні докази, отримані через негласні слідчі (розшукові) дії, здебільшого пов'язані з обмеженням конституційних прав особи, тож вимагають застосування процесуальних дій, передбачених главою 21 КПК України, зокрема зняття інформації з електронних інформаційних систем (ст. 264 КПК України),

зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України), спостереження за особою в публічно доступному місці з використанням технічних засобів (ст. 269 КПК України), установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України). Типовий приклад – інформація про телефонні з'єднання й мережевий трафік підозрюваного, отримана в порядку зняття інформації з транспортних телекомунікаційних мереж на підставі ухвали слідчого судді.

Окреме місце посідають електронні докази, отримані внаслідок міжнародного співробітництва. У такому випадку електронні докази розміщені на серверах, контрольованих суб'єктами поза юрисдикцією України, їх отримання вимагає направлення запиту про міжнародну правову допомогу за главою 43 КПК України або застосування механізмів, передбачених Конвенцією Ради Європи про кіберзлочинність 2001 року. Типовий приклад – вміст електронної поштової скриньки користувача, розміщеної на серверах провайдера в іншій державі, отриманий через запит про міжнародну правову допомогу до компетентного органу відповідної юрисдикції.

Слід зазначити, що прикладне значення виокремлення електронних доказів у цьому контексті полягає в тому, що віднесення електронного доказу до певної групи безпосередньо орієнтує слідчого або прокурора у виборі належної процесуальної дії (обшук, тимчасовий доступ, НСРД чи міжнародне співробітництво), що своєю чергою визначатиме допустимість отриманого доказу.

Порушення нормативної процедури отримання доказів залежно від способу може призвести до недопустимості доказу за ч. 1 ст. 87 КПК України. Такий підхід узгоджується з практикою ЄСПЛ. Наприклад, у справі «Benedik v. Slovenia» [163] Суд визнав порушення ст. 8 Конвенції, оскільки доступ до даних, які ідентифікують користувача за динамічною IP-адресою, здійснено без судового дозволу та на підставі норми, що не відповідала вимозі якості закону.

Залежно від носія електронного доказу можна виокремити такі види: локальні, мережеві, локально-мережеві, транзитні.

Докази, що зберігають на фізично ідентифікованому носії, відносять до локальних електронних доказів. Такі докази можуть бути безпосередньо вилучені у володіння органу досудового розслідування (пам'ять комп'ютерів, смартфонів, жорсткі диски, флешнакопичувачі, карти пам'яті, SIM-карти).

Процесуальною особливістю цієї групи є застосовність класичних правил роботи з матеріальними носіями – вилучення, опечатування, забезпечення цілісності. Типовий приклад – флешнакопичувач з електронними документами, виявлений під час обшуку службового приміщення.

У випадку якщо докази зберігають на віддалених ресурсах, контрольованих третіми особами (хмарні сховища, поштові сервери, сервери соціальних мереж і месенджерів), без чіткої географічної прив'язки до території юрисдикції йдеться про мережеві електронні докази. Такими доказами можуть бути дані, розміщені на сервісах Google Drive, iCloud, Dropbox, Microsoft OneDrive тощо. Процесуальною особливістю цієї групи є обов'язкова взаємодія з третьою особою – володільцем носія, а інколи й потреба в міжнародному співробітництві. Типовий приклад – фотознімки, що зберігають у хмарному сервісі iCloud особи, доступ до яких отримано через звернення до Apple Inc.

Інколи електронні докази можуть знаходитися одночасно в кількох взаємопов'язаних середовищах без єдиного оригіналу, наприклад, синхронізовані дані між пристроями одного користувача, дзеркальні копії баз даних. У такому випадку такі електронні докази є локально-мережевими, оскільки в них немає єдиного чіткого «місцезнаходження» доказу. Типовим прикладом такого доказу є запис криптовалютної транзакції в блокчейн-реєстрі мережі Bitcoin, що одночасно існує на тисячах вузлів мережі без виокремлення «оригіналу».

Окремою категорією є транзитні електронні докази. Їх особливість полягає в тому, що інформація існує тільки в процесі передачі й потребує невідкладної фіксації до моменту її зникнення або модифікації, наприклад, мережевий трафік у момент передачі, вміст оперативної пам'яті системи, що працює (live memory), активні мережеві з'єднання тощо.

Фіксація таких доказів потребує залучення профільних спеціалістів і спеціального технологічного обладнання. Такі докази критично залежні від часу проведення процесуальної дії, адже затримка у фіксації фактично знищує доказ. Типовий приклад – вміст оперативної пам'яті комп'ютера підозрюваного, що містить криптографічні ключі активної сесії й автоматично зникає після вимкнення пристрою.

Залежності від механізму підтвердження автентичності й цілісності електронного доказу можна виокремити чотири групи: самоверифіковані; технічно верифіковані; експертно підтверджені; презумптивно верифіковані.

Самоверифікований електронний доказ має вбудовані технічні засоби підтвердження автентичності та цілісності, які можуть бути перевірені безпосередньо засобами доказу, наприклад, документи із кваліфікованим електронним підписом, записи в блокчейн-реєстрах тощо. Доказова цінність цієї групи полягає в тому, що автентичність встановлюють алгоритмічно, це не потребує залучення зовнішніх засобів верифікації. Типовий приклад – електронний договір, підписаний обома сторонами кваліфікованим електронним підписом за допомогою чинного сертифіката, автентичність якого перевіряють безпосередньо засобами електронного підпису.

Технічно верифіковані електронні докази – це докази, автентичність яких підтверджують опосередковано через технічні атрибути, що супроводжують основну інформацію: метадані файлу, IP-адреси, часові мітки серверів, дані заголовків електронних листів, дані ланцюга збереження доказів (chain of custody).

Верифікація цієї групи відбувається не власне доказом, а через аналіз його технічного оточення. Типовий приклад – фотографія, автентичність часу й місця зйомки якої підтверджують аналізом EXIF-метаданих, що містять часові мітки камери та геолокаційні координати.

Встановлення автентичності й цілісності експертно підтверджених електронних доказів можливе виключно через залучення спеціальних знань і проведення судової експертизи (наприклад, дані з пошкоджених або частково перезаписаних носіїв, відновлені після видалення файли тощо). Верифікація цієї

групи потребує висновку експерта й не може бути проведена сторонами провадження самостійно. Типовий приклад – фрагменти видалених файлів, відновлені з нерозподіленого простору жорсткого диску, автентичність і повноту яких встановлюють виключно через висновок судової комп'ютерно-технічної експертизи.

Самостійною категорією, яку слід виокремити серед електронних доказів, є презумптивно верифіковані електронні докази, тобто докази, щодо яких діє нормативно або судово закріплена презумпція цілісності, що покладає тягар доказування протилежного на сторону, яка її оспорює.

До цієї групи можна віднести електронні документи органів державної влади, отримані в установленому порядку через офіційні інформаційні системи (ЄДРСР, державні реєстри); електронні докази, надані операторами електронних комунікацій у відповідь на офіційний запит із дотриманням процедури їх формування. Типовим прикладом такого доказу є судове рішення з ЄДРСР (цілісність такого рішення презюмують доти, доки протилежне не буде обґрунтовано поставлене під сумнів учасником провадження).

Цей критерій є близьким до шкали визначеності (certainty scale) E. Casey [164], проте відрізняється від них процесуально-правовою, а не криміналістично-технічною природою, оскільки критерій оперує не ступенем переконливості висновку експерта, а доступним у межах кримінального провадження механізмом перевірки, що безпосередньо корелює зі стандартом «поза розумним сумнівом», закріпленим у ч. 2 ст. 17 КПК України.

Окремим критерієм розмежування електронних доказів, щодо якого триває активна дискусія серед науковців і практиків, є рівень втручання в право на повагу до приватного життя. Він ґрунтується на єдиній підставі поділу – ступені обмеження, гарантованого ст. 8 Конвенції про захист прав людини і основоположних свобод, – права на приватність, що зумовлене отриманням відповідного електронного доказу.

В основі цього критерію лежить ширша вимога розумного балансу між державними, суспільними й особистими інтересами у кримінальному провадженні, ґрунтовно обґрунтована у праці Л. Д. Удалової та О. Ю. Хабло [132].

Стосовно електронних доказів цей баланс набуває форми співмірності (пропорційності) втручання в гарантоване ст. 8 Конвенції право на повагу до приватного життя з потребами кримінального переслідування.

Для обґрунтування цього критерію розглянемо практику ЄСПЛ, який розробив стандарти оцінки електронних доказів крізь призму ст. 8 (право на повагу до приватного життя), ст. 6 (право на справедливий суд) і ст. 10 (свобода вираження поглядів) Конвенції про захист прав людини і основоположних свобод.

Важливе значення для побудови запропонованої класифікації має рішення Великої палати ЄСПЛ у справі Big Brother Watch and Others v. the United Kingdom (об'єднані заяви № 58170/13, 62322/14 та 24960/15, рішення від 25 травня 2021 року).

У цьому рішенні Суд уперше системно концептуалізував процес отримання електронних даних як поступовий поетапний процес: первинне зберігання отриманої інформації; застосування селекторів – програмних фільтрів, що відбирають релевантні дані; дослідження відібраного контенту й даних аналітиками; подальше зберігання, використання та обмін кінцевим продуктом обробки (§325 рішення) [162].

Крім того, Суд зазначив, що на будь-якому рівні дослідження перехоплених даних державою існує втручання в особисте життя в розумінні ст. 8 Конвенції. Це стосується навіть звичайного зберігання персональних даних, а з кожним етапом рівень втручання підвищується [162].

Концептуальним є і рішення Великої палати Суду справедливості Європейського Союзу в об'єднаних справах Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung and Others [206], яким суд визнав недійсною Директиву 2006/24/ЄС про збереження даних як таку, що непропорційно обмежує гарантовані ст. 7 і 8 Хартії основоположних прав ЄС права на повагу до приватного життя та на захист

персональних даних.

Суд зазначив, що метадані електронних комунікацій становлять інформацію, яка в сукупності дає змогу робити точні висновки стосовно приватного життя осіб, чиї дані були збережені, зокрема щодо повсякденних звичок, постійних чи тимчасових місць проживання, щоденних або інших переміщень, здійснюваної діяльності, соціальних зв'язків і соціального оточення цих осіб (§27 рішення) [206].

Нормативне закріплення градація рівня втручання в приватність дістала в Регламенті (ЄС) 2023/1543 Європейського парламенту та Ради Європи від 12 липня 2023 року щодо європейських ордерів про надання та збереження електронних доказів у кримінальних провадженнях і Директиві (ЄС) 2023/1544 від 12 липня 2023 року («пакет e-evidence»). Зазначені акти диференціюють процесуальні гарантії за чотирма категоріями даних: дані абонента (subscriber data), дані доступу (access data), трафік-дані (traffic data) і контент-дані (content data), запроваджуючи посилений судовий контроль для трафік- і контент-даних.

Хоча перелічені судові рішення та нормативні акти безпосередньо не визначають класифікаційної моделі електронних доказів, однак дають змогу встановити орієнтири й виокремити такі групи електронних доказів: електронні докази, отримані без втручання в приватність; електронні докази з мінімальним рівнем втручання в приватність; електронні докази із середнім рівнем втручання в приватність; електронні докази з високим рівнем втручання в приватність.

До доказів, які не порушують права на приватність, можна віднести публічно доступну інформацію, отримання якої не вимагає судового санкціонування, наприклад, відкриті публікації в соціальних мережах, дані з відкритих джерел розвідки (OSINT), інформація з вебсайтів державних реєстрів відкритого доступу.

До доказів мінімального втручання в приватність слід віднести, зокрема, дані абонента і трафік-дані, що дають змогу встановити особу користувача й обставини комунікації без розкриття її змісту, ідентифікаційні дані власника номера телефону тощо. Слід зауважити, що такі дані можуть підпадати під категорію персональних даних, які своєю чергою охороняються положеннями Конституції України, Закону України «Про захист персональних даних».

На нашу думку, нормативна охорона персональних даних та їх використання як електронних доказів становить окремий науковий інтерес та потребує спеціального наукового опрацювання, оскільки положення кримінального процесуального законодавства та законодавства про персональні дані не гармонізовані між собою [80].

До доказів середнього рівня втручання в приватність слід віднести зміст електронного листування та особисті файли користувача, що розкривають приватну сферу, наприклад, зміст повідомлень у месенджерах, особисті файли в особистих пристроях, дані хмарних сховищ, історія браузера.

Найвищим рівнем втручання в приватність є інформація, що зачіпає особливо чутливі категорії даних або приватне життя, наприклад, біометричні дані, медичні записи, фото- й відеоматеріали, дані геолокації в реальному часі, результати масового перехоплення трафіка тощо.

Вважаємо, що запропонована диференціація відповідає підходу Європейського суду з прав людини щодо градації рівня втручання в право на повагу до приватного життя.

Сукупність рішень ЄСПЛ та ССЄС, нормативного закріплення вказує на визначення різних рівнів втручання в приватність, який Україна як держава – учасниця Конвенції про захист прав людини і основоположних свобод зобов’язана враховувати під час застосування КПК України.

Слід зауважити, що ст. 31 і 32 Конституції України гарантують таємницю листування та недоторканність приватного життя, що також дає змогу визначати градацію електронних доказів. Структуру запропонованої класифікації представлено в табл. 1.1, яка ілюструє паралельне застосування п’ятьох критеріїв до одного й того самого електронного доказу.

Таблиця 1.1

Класифікація електронних доказів у кримінальному процесі

Критерій	Підстава поділу	Класифікаційні групи
Критерій 1. За способом створення інформації	Ступінь і характер участі людини у формуванні електронної інформації	• створені особою • технічно фіксовані (створені комп'ютером) • комбіновано сформовані (гібридні) • створені засобами штучного інтелекту
Критерій 2. За процесуальним режимом отримання	Процесуальна дія за КПК України як належний інструмент отримання	• безпосередньо вилучені • отримані через тимчасовий доступ до речей і документів • отримані через негласні слідчі (розшукові) дії • отримані через міжнародне співробітництво
Критерій 3. За процесуальним статусом носія електронної інформації	Процесуально-правовий режим носія, на якому розміщена електронна інформація	• локальні • мережеві • локально-мережеві • транзитні
Критерій 4. За рівнем процесуальної верифікованості	Механізм підтвердження автентичності та цілісності електронного доказу	• самоверифіковані • технічно верифіковані • експертно підтверджені • презумптивно верифіковані
Критерій 5. За рівнем втручання у право на повагу до приватного життя	Ступінь обмеження, гарантованого ст. 8 Конвенції права на приватність	• без втручання у приватність • мінімальний рівень втручання у приватність • середній рівень втручання у приватність • високий рівень втручання у приватність

Джерело: розроблено автором.

Наочно проілюструвати запропоновану класифікацію можна на прикладі із судової практики.

У постанові ККС ВС від 31 березня 2026 року у справі № 175/10123/23 [102] ключовими доказами державної зради стали відеоповідомлення в месенджері Telegram. За запропонованою класифікацією такий доказ кваліфікують як:

– створений особою (відеоповідомлення створене безпосередньо особою);

– такий, який отримують під час обшуку;

– комбіновано розміщений (відомості містилися як на пристрої, так і на серверах Telegram);

– технічно верифіковний (через дослідження метаданих повідомлення, часових міток сервера, ідентифікації акаунта);

– такий, що має середній рівень втручання в приватність.

Повна координатна характеристика надає можливість одразу визначити процесуальний порядок роботи з доказом – від моменту виявлення до представлення суду.

Цей приклад демонструє, що окреслена модель забезпечує системний процесуальний інструментарій для роботи з електронними доказами різної природи.

Також слід зазначити, що класифікація має прикладне значення в трьох аспектах: орієнтує сторону обвинувачення на дотримання принципу пропорційності під час обрання процесуального інструменту збирання електронного доказу; надає стороні захисту аргумент для оскарження допустимості доказу, отриманого з невідповідним рівнем правових гарантій; забезпечує суду додатковий критерій оцінки доказу в аспекті дотримання конституційних прав особи, гарантованих ст. 31 і 32 Конституції України та ст. 8 Конвенції про захист прав людини і основоположних свобод.

Отже, запропонована класифікація електронних доказів є не просто теоретичною конструкцією, а інструмент, що забезпечує методологічне підґрунтя для подальшого дослідження електронних доказів, їх збирання, фіксації, оцінки та використання в кримінальному процесуальному доказуванні.

Класифікація додатково підтверджує обґрунтовану в підрозділі 1.1 позицію щодо самостійності електронного доказу як виду доказів, оскільки жоден із

запропонованих класифікаційних критеріїв не може бути повноцінно реалізований у межах традиційних категорій «документ» або «речовий доказ».

1.3. Правове регулювання електронних доказів у кримінальному процесуальному законодавстві України та міжнародних актах

Положення КПК України передбачають можливість використання електронних об'єктів під час кримінального провадження, оскільки в ньому йдеться про такі поняття, як «електронний документ» (ч. 3 ст. 99 КПК України), «комп'ютерні дані» (п. 1 ч. 2 ст. 99 КПК України), «електронні інформаційні системи» (ст. 264).

Зокрема, ч. 3 ст. 99 КПК, розміщена в параграфі 4 «Речові докази і документи», закріплює обов'язок сторони кримінального провадження, потерпілого та представника юридичної особи, щодо якої здійснюють провадження, надавати суду оригінал документа. Водночас законодавець виокремлює поняття оригіналу: для традиційного документа оригіналом є власне документ, натомість для електронного – його відображення, якому надають рівнозначної юридичної сили.

Умови та порядок обігу електронних документів у кримінальному судочинстві визначено в ч. 5 ст. 106 КПК, яка містить бланкетну норму: у частині, не врегульованій КПК, застосовують спеціальне законодавство про електронні документи й електронний документообіг.

Відповідно до ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг» [109], електронним документом вважають документ, інформацію в якому зафіксовано у вигляді електронних даних із дотриманням обов'язкових реквізитів.

Електронні документи становлять лише частину ширшого поняття електронних доказів, не вичерпуючи його.

Електронним документам властива низка специфічних ознак. За формою це можуть бути текстові файли, графічні зображення, плани, фотографії, аудіо- та відеозаписи тощо. За місцем зберігання – карти пам'яті, мобільні пристрої, сервери, системи резервного копіювання та інші носії, зокрема хмарні ресурси мережі Інтернет. Обов'язковим реквізитом електронного документа є електронний цифровий підпис, що забезпечує ідентифікацію його автора та підтверджує цілісність змісту.

Водночас слід зазначити, що жодне з цих означень у КПК України не забезпечує прямого визначення терміна «електронний доказ», що підпадає під категорію «документи» (ч. 2 ст. 99 КПК України).

Непослідовність кваліфікації електронних доказів підтверджує і судова практика. В одних випадках суди розглядають їх як документи, в інших – як речові докази:

– «речові докази носіїв, на яких знаходиться інформація» (Вирок у кримінальній справі № 711/4173/22 від 28 лютого 2023 року Золотоніського міськрайонного суду Черкаської області) [36];

– «речові докази відеозаписів, що розміщені на CD-дисках» (Вирок у кримінальній справі № 352/1477/21 від 5 квітня 2023 року Тисменицького районного суду Івано-Франківської області) [35].

Однак визначальною ознакою процесуальної категорії «документ» у кримінальному провадженні є його матеріальна форма (ч. 1 ст. 99 КПК України). Комп'ютерні дані такої властивості у звичному розумінні не мають: їх неможливо безпосередньо сприйняти без застосування спеціальних технічних засобів, які здійснюють відтворення та перетворення цифрової інформації у форму, доступну для сприйняття людиною.

Отже, здійснений аналіз засвідчує, що КПК України, на відміну від процесуальних кодексів інших юрисдикційних порядків, не містить визначення електронного доказу. Проте процесуальні кодекси в інших видах судочинства (цивільному, господарському, адміністративному) уже містять визначення електронних доказів.

Відповідно до ст. 100 ЦПК України, електронними доказами є інформація в електронній (цифровій) формі, що містить 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 та інші дані в електронній формі [138]

Відповідно до положень цієї статті, 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).

Слід зауважити, що ЦПК вирізняє оригінал і копію електронних доказів. У ч. 2 ст. 100 ЦПК України зазначено, що електронні докази подають в оригіналі або в електронній копії, на яку накладено кваліфікований електронний підпис відповідно до вимог законів України «Про електронні документи та електронний документообіг» [109] та «Про електронну ідентифікацію та електронні довірчі послуги» [108]. Законом може бути передбачено інший порядок засвідчення електронної копії електронного доказу.

Аналогічний підхід застосовують і в господарському й адміністративному судочинстві, що свідчить про визнання законодавцем широкого переліку форм цифрової інформації як потенційних доказів ст. 96 Господарського процесуального кодексу України [47], ст. 99 Кодексу адміністративного судочинства України [67].

Отже, електронну інформацію в кримінальному провадженні наразі розглядають крізь призму традиційних категорій доказів: як різновид документів (нематеріальний носій інформації) й одночасно пов'язана з матеріальним носієм (файли можуть зберігатися на дисках, телефонах, серверах тощо, які є речовими доказами).

Важливе значення в контексті регулювання певних правових аспектів електронних доказів відіграють рішення Верховного Суду, які надають можливість реагувати на швидкі зміни обставин, а також на життєдіяльність у правовому полі, не вносячи змін до нормативних законодавчих актів.

У цьому контексті важливою є позиція Верховного Суду, висловлена під час розгляду справи № 569/1908/23. Попри те що електронні докази не фігурують серед процесуальних джерел доказів, визначених ст. 84 КПК України, суд прямо зазначив: «основними доказами у кримінальних провадженнях про злочини проти основ національної безпеки України є електронні (цифрові) докази» [96].

Така позиція виявляє принципову суперечність між нормативним регулюванням і реальними потребами правозастосування. Верховний Суд, а за ним – і суди нижчих інстанцій фактично вдаються до розширювального тлумачення КПК України, легітимізуючи тим самим окремий вид доказів, якого чинний процесуальний закон не знає.

Це свідчить не лише про прогалину в законодавстві, а й про те, що судова практика об’єктивно випередила нормотворення: Верховний Суд формує правозастосовну практику в умовах нормативної невизначеності, однак не знімає потреби в законодавчому врегулюванні.

Виразний запит практиків на вдосконалення правового регулювання засвідчили й результати проведеного анкетування. Зокрема, 49,2 % опитаних вважають чинне регулювання використання електронних доказів лише частково достатнім (є певні прогалини), ще 29,2 % – таким, що потребує суттєвого доопрацювання; достатнім його визнали лише 11,5 %.

Понад половина респондентів (54,6 %) схвалюють запровадження окремої статті КПК України, яка визначала б поняття «електронний доказ» і закріплювала його як самостійне джерело доказів. Доцільність єдиного стандарту збирання, фіксації та зберігання електронних доказів визнали 87,7 % опитаних (57,7 % – «украй необхідно», 30,0 % – «бажано»).

Стан регулювання транскордонного отримання електронних доказів 48,5 % оцінили як такий, що потребує вдосконалення механізмів практичного застосування, а 13,1 % — суттєвої законодавчої реформи. Наведені дані емпірично підкріплюють авторську пропозицію стосовно доповнення КПК України (додаток В, рис. 4, 5, 7, 22).

Міжнародне регулювання електронних доказів має багаторівневу структуру, яка поєднує міжнародні правові акти, національне законодавство в частині регулювання електронних доказів і кримінального процесу, спеціальні технічні стандарти.

Фундаментом міжнародного регулювання в цій сфері є Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року [71]. Цей акт уперше в міжнародно-правовій практиці запровадив поняття комп'ютерних даних як самостійного об'єкта доказування та закріпив механізми їх збереження, вилучення й обробки в межах кримінального провадження. Будапештська конвенція заклала концептуальні та процесуальні засади, що стали відправною точкою для подальшої еволюції правового режиму електронних доказів.

Другий додатковий протокол до Конвенції про кіберзлочинність, спрямований на посилення транскордонного співробітництва та розкриття електронних доказів, підписаний Україною 30 листопада 2022 року [233], однак станом на 2026 рік його ратифікація ще не завершена, що обмежує можливості застосування передбачених ним механізмів прямого доступу до електронних даних у постачальників послуг інших держав.

2023 року Європейський Союз ухвалив Регламент (EU) 2023/1543 про European Production Orders та European Preservation Orders для електронних доказів у кримінальних провадженнях [229], який набирає чинності 18 серпня 2026 року. Зазначений Регламент встановлює правила, за якими судовий орган однієї держави-члена може безпосередньо витребувати електронні докази від постачальника послуг в іншій державі-члені, незалежно від місця зберігання даних.

Постачальник послуг зобов'язаний виконати European Production Order протягом 10 днів, а у невідкладних випадках – протягом 8 годин. Паралельно було ухвалено Директиву (EU) 2023/1544 про гармонізовані правила призначення правових представників для збирання електронних доказів [179], а також чинною залишається Директива 2014/41/EU про Європейський ордер на розслідування у кримінальних справах [180].

Важливе значення в системі регулювання має Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108) [69], яка встановлює загальні принципи обробки персональних даних і створює правові межі, у яких здійснюють збирання та використання електронних доказів.

Слід зазначити і про технічні стандарти роботи з електронними доказами. Стандарт EN ISO/IEC 27037:2016 «Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence» окреслює послідовні стадії поводження з електронними доказами: виявлення (identification), вилучення (collection), отримання (acquisition), перевезення (transportation) і зберігання (preservation) [184]. Саме ці стандарти були імплементовані в Україні до ДСТУ ISO/IEC 27037:2017 [57].

Метою цих процедур є забезпечення цілісності, автентичності й доказового значення цифрової інформації, що потрапляє до процесу доказування. На основі зазначених стандартів розроблено Берклійський протокол цифрових відкритих розслідувань (Berkeley Protocol on Digital Open Source Investigations), який встановлює етичні та процедурні стандарти збирання, збереження та верифікації відкритих цифрових даних (зокрема контенту соціальних мереж, супутникових зображень, відеоматеріалів) для використання в правозастосуванні й судочинстві, зокрема в провадженнях за міжнародні злочини [153].

Отже, законодавче регулювання використання електронних доказів не забезпечує на належному рівні потреби правозастосування, оскільки Верховний Суд, а за ним – і суди нижчих інстанцій, фактично здійснюючи розширювальне тлумачення нормативного акта, виокремлюють новий вид доказів, який не передбачений КПК України.

Висновки до розділу 1

У першому розділі здійснено теоретичне дослідження електронних доказів у кримінальному процесі, що дає змогу сформувати такі висновки.

1. Сформульовано авторське визначення електронного доказу як інформації в електронній формі, що створена, збережена, передана або відображена за допомогою електронних пристроїв, систем чи мереж, містить відомості про обставини, які мають значення для кримінального провадження, і може бути використана як доказ за умови її отримання та перевірки в порядку, передбаченому КПК України. На відміну від наявних у доктрині визначень, запропоноване визначення сформульовано на підставі способу існування інформації в електронному середовищі, без оцінних категорій (автентичності, цілісності) у дефініції. Обґрунтовано необхідність виокремлення електронного доказу як самостійного джерела доказів у кримінальному процесі України.

2. Виокремлено шість специфічних ознак електронних доказів, серед яких: нематеріальність, динамічність, відтворюваність, залежність від технічних засобів, відсутність жорсткої прив'язки до матеріального носія та наявність метаданих. Аргументовано доцільність виокремлення метаданих як ознаки із самостійним доказовим значенням.

3. Запропоновано авторську класифікацію електронних доказів за п'ятьма критеріями: 1) способом створення інформації; 2) процесуальним режимом отримання; 3) процесуальним статусом носія; 4) рівнем процесуальної верифікованості; 5) рівнем втручання в право на повагу до приватного життя. Координатний характер класифікації надає можливість описувати кожен електронний доказ за всіма критеріями одночасно, що визначає процесуальний маршрут роботи з ним – від моменту виявлення до оцінки судом.

4. Встановлено, що КПК України, на відміну від ЦПК, ГПК і Кодексу адміністративного судочинства, не містить визначення поняття «електронний доказ», що створює прогалину в нормативному регулюванні. Аналіз міжнародних актів засвідчив наявність розвинутої багаторівневої міжнародної нормативної бази, орієнтири якої доцільно врахувати під час формування національної моделі регулювання електронних доказів.

РОЗДІЛ 2
ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

2.1. Використання електронних доказів у кримінальному процесі. Питання допустимості електронних доказів

Ключовим завданням органу досудового розслідування є своєчасне виявлення, належна фіксація та вилучення відповідних електронних доказів, запобігання їх втраті, знищенню або несанкціонованій модифікації.

Законодавець зобов'язує орган досудового розслідування дотримуватися положень кримінального процесуального законодавства під час вчинення таких дій з метою дотримання прав людини.

Порядок пошуку, збирання та фіксації електронних доказів досліджували науковці, йому присвячено значну кількість наукових робіт, зокрема методичних рекомендацій.

У посібнику «Криміналістична тактика і методика розслідування окремих видів злочинів» надано визначення електронного доказу. Науковці акцентували на особливості підготовки фахівців для роботи з електронними доказами та роз'яснили методологію розслідування злочинів з використанням електронних документів та електронних речових доказів [4, с. 451–452].

У методичних рекомендаціях «Використання електронних носіїв інформації з медіаконтентом у якості джерел доказів», автори дослідили поняття, види й тактичні особливості отримання доступу до електронних носіїв інформації, порядок пошуку власника інтернет-сторінки, особливості призначення експертиз носіїв інформації та інші питання [10].

Розширення поняття документа в криміналістиці за рахунок об'єктів, створених засобами електронно-обчислювальної техніки, було обґрунтовано ще наприкінці 1990-х років у працях М. В. Салтевського, який запропонував концепт

«криміналістичної документалістики» як розділу, що вивчає документи в широкому, кібернетичному сенсі [116, с. 209].

На нашу думку, такий започаткований розширений підхід до вивчення документів, не обмежуючись тільки матеріальними документами в класичному його вигляді, дістав закономірне продовження в сучасній концепції електронного доказу, у межах якої електронний об'єкт розглядають не лише як похідний від матеріального носія, а як самостійне явище, що вирізняється власною технологічною природою – цілісністю, метаданими, можливістю автентифікації.

О. В. Сіренко стверджує, що першочерговим питанням щодо використання електронних доказів у кримінальному процесі, яке потребує негайного врегулювання, є встановлення порядку збору та фіксації електронних доказів, формування методики їх дослідження [127, с. 211].

Д. М. Цехан зазначає, що ключовою перешкодою, що в умовах сьогодення унеможливлює використання цифрової інформації як доказу, є брак експертних методик її ідентифікації та аутентифікації [137, с. 121].

Такі позиції засвідчують, що національна доктрина протягом тривалого часу розглядала електронні докази переважно крізь призму криміналістичної техніки – як об'єкт ідентифікації, фіксації та експертного дослідження.

Загальну характеристику проблем збирання, перевірки й оцінки електронних доказів у кримінальному провадженні, зокрема щодо забезпечення їх автентичності та допустимості, здійснено в попередній публікації [87].

Питання теоретико-методологічних засад роботи з електронними доказами комплексно проаналізовано в праці І. В. Гори, В. А. Колесника й І. І. Поповича, зокрема окреслено сучасні підходи українських і зарубіжних науковців до збирання, оцінки та використання електронних доказів, а також з'ясовано зміст поняття «цифрова криміналістика», її місце в системі криміналістичних знань [46]. Проаналізувавши закордонний досвід нормативно-методичного забезпечення роботи із цифровими доказами, зокрема Практичне керівництво Асоціації керівників поліції Англії, Уельсу та Північної Ірландії (ACPO, 2012) і Базовий посібник Агентства Європейського Союзу з мережевої та інформаційної безпеки

(ENISA, 2014), автори дійшли висновку про необхідність комплексного вдосконалення нормативної та технічної бази під час розслідування злочинів з електронними об’єктами. Автори методологічно обґрунтували необхідність розроблення комплексної моделі організації роботи із цифровими доказами.

Водночас процесуально-правовий аспект, а саме порядок збирання електронних доказів як самостійна процесуальна процедура, відрізняється від збирання речових доказів чи документів, має низку невирішених питань, що потребують уваги й досліджень. Саме зазначений процесуальний аспект є предметом подальшого аналізу в цьому підрозділі.

Пошук й ідентифікація електронних доказів є обов’язковим елементом початкового етапу більшості сучасних кримінальних розслідувань. Для отримання або копіювання криміналістично значущої інформації необхідно встановити місцезнаходження електронного пристрою, у якому є доступ до доказів (мобільний телефон, планшет, комп’ютер).

Такі електронні пристрої можуть зберігати електронні докази як безпосередньо на накопичувачі пристрою, так і у віддалених хмарних сховищах, місцезнаходження яких може не збігатися із фізичним розміщенням електронного пристрою.

Доступ до електронних пристроїв може бути захищений, а тому слідчі дії мають ураховувати цю обставину для обрання правильних стратегії, тактики та психологічних прийомів для отримання доступу до таких пристроїв.

Якщо питання подолання захисту до пристрою вирішено, то наступним етапом є належне вилучення інформації та її долучення до матеріалів кримінального провадження, що залишається дискусійним і пов’язано з низкою процесуальних проблем.

У сучасній слідчій практиці електронні докази можуть бути отримані на підставі запиту, зафіксовані під час огляду місця події, речей, виїмки, обшуку або інших слідчих (процесуальних) дій.

Під час огляду місця події доцільно зважати не лише на наявність електронних пристроїв, а й на інші пов’язані з ними речі, наприклад, зарядні

пристрої, кабелі до електронних пристроїв, наявність інших систем, які можуть бути пов’язані з такими пристроями.

Наприклад, наявність камер спостереження може свідчити про наявність сервера для зберігання відео, наявність Wi-Fi роутера – про наявність пристроїв, які можуть бути з ним пов’язані, а відомості з Wi-Fi роутера можуть розкрити дані щодо комунікації з іншими пристроями.

Для збирання електронних доказів у кримінальному провадженні використовують носії інформації, призначені для безпосереднього копіювання та збереження електронних даних, до яких належать жорсткі диски, флешнакопичувачі, інші електронні засоби зі здатністю копіювання доказів, які мають власні накопичувачі або доступ до хмарних середовищ.

Слід також зазначити, що для збирання таких електронних доказів можуть знадобитися й інші засоби чи обладнання, зокрема технічні засоби для доступу та демонтажу обладнання, фіксації процесу слідчих дій, пакування і транспортування носіїв інформації, спеціалізовані програмно-апаратні комплекси цифрової криміналістики тощо.

Початкова процедура опрацювання електронних носіїв передбачає ідентифікацію, збирання, вилучення та збереження потенційних доказів. Електронні об’єкти можуть мати нестабільний характер. Вони можуть змінюватися або знищуватися внаслідок неналежного поводження чи огляду.

У зв’язку з цим особи, які працюють з електронними доказами, повинні бути компетентними та керуватися чіткими вимогами з метою уникнення ризиків. Неналежне поводження з електронними пристроями може призвести до непридатності потенційних електронних доказів, що містяться на них.

У разі виявлення електронних носіїв інформації під час проведення слідчих (розшукових) дій збирання доказів (інформації, що міститься на носії) можуть здійснювати двома способами:

1) шляхом вилучення носія або інформаційної системи;

2) шляхом копіювання інформації, що зберігається на відповідному електронному носії (у цьому випадку питання фіксації даних із кіберпростору не розглядають).

Зазначені способи збирання доказів мають як переваги, так і недоліки, а також певні обмеження щодо застосування.

На нашу думку, у сучасних умовах пріоритетним способом збирання електронних доказів має бути саме копіювання інформації, а не вилучення матеріального носія.

Такий висновок випливає з трьох обставин: вилучення носія не гарантує збереження цілісності інформації (зокрема, у разі шифрування або залежності від мережевого середовища); вилучення носія здебільшого є непропорційним втручанням у права особи, оскільки обмежує доступ до всієї інформації на пристрої, а не лише до процесуально релевантної; сучасна судова практика послідовно рухається в напрямі розмежування носія та інформації як самостійного об’єкта процесуального впливу, що підтверджує аналіз ст. 159 і 168 КПК України.

Традиційним способом збирання доказів у кримінальному провадженні є вилучення матеріальних об’єктів, зокрема електронних носіїв та інформаційних систем. Однак фізичне вилучення не завжди є технічно можливим. Наприклад, складність вилучення інформаційних систем може бути зумовлена їх громіздкістю, загрозою зупинення виробничих процесів або небезпекою втрати доступу до інформації (зокрема в разі неможливості подальшого успішного запуску дешифрування, якщо систему з активним шифруванням буде вимкнено).

Необхідно акцентувати на окремих слідчих діях, які законодавець пов’язує з електронними доказами.

У ч. 1 ст. 237 КПК України йдеться про комп’ютерні дані, які можуть бути оглянуті під час огляду. Зокрема, у положенні цієї статті зазначено, що з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів і комп’ютерних даних [76].

Комп’ютерні дані за своєю природою не вкладаються в класичну модель ані об’єкта огляду як слідчої (розшукової) дії, ані документа як процесуального джерела доказової інформації, оскільки їх зміст стає доступним лише через технічне посередництво, а не через безпосереднє «оглядове» сприйняття матеріального об’єкта [50].

У ч. 2 ст. 237 КПК України деталізовано, що огляд комп’ютерних даних проводить слідчий, прокурор шляхом відображення в протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або в паперовій формі).

Проте вчинення таких дій не узгоджується з природою електронних доказів, оскільки, щоб здійснити таке відображення відомостей, які містяться в комп’ютерних даних, і належно зафіксувати їх у протоколі, суб’єкт розслідування має попередньо ознайомитися з такою інформацією шляхом сприйняття органами чуття – побачити, прослухати.

Тобто законодавець прирівняв електронну інформацію до матеріальних речей, однак це логічно не прийнятно, оскільки відтворити таку інформацію можна за допомогою електронних пристроїв, а безпосереднє сприйняття людиною інформації на той час є нереальним.

У ч. 2 ст. 159 КПК України законодавець прямо закріплює, що тимчасовий доступ до електронних інформаційних систем, комп’ютерних систем (їх частин) і мобільних терміналів реалізується не через вилучення носія, а шляхом зняття копії інформації, яка в них міститься.

Така конструкція демонструє, що об’єктом процесуального впливу в цьому випадку є саме інформація (дані) як окрема процесуально релевантна категорія, а не матеріальний носій чи технічний пристрій.

Тож ми поділяємо наукову позицію І. А. Смаль щодо необхідності запровадження дієвого судового контролю під час отримання та дослідження інформації в електронному вигляді, оскільки саме такий підхід найбільше

відповідає стандартам захисту прав людини, гарантованим ст. 8 Конвенції про захист прав людини і основоположних свобод [119].

Доступ до відомостей, що містяться в мобільних телефонах, комп'ютерах та інших електронних пристроях, об'єктивно пов'язаний із ризиком ознайомлення органів досудового розслідування не лише з інформацією, що має доказове значення, а й з даними приватного чи сімейного характеру, особистим листуванням, професійною таємницею та іншими конфіденційними відомостями.

У зв'язку з цим навіть перегляд змісту електронного носія вже становить втручання в право на повагу до приватного життя та кореспонденції.

З огляду на це, доцільним видається застосування моделі, за якої процес пошуку й відбору релевантної інформації супроводжується попереднім або подальшим ефективним судовим контролем. Такий контроль має передбачати визначення меж доступу до електронних даних, перевірку обґрунтованості втручання, його необхідності та пропорційності, а також запобігання ознайомленню слідства з відомостями, що не стосуються предмета доказування.

Поділяємо також ідею функціонального розмежування повноважень, коли технічний огляд значного масиву даних може здійснювати незаінтересований спеціаліст чи експерт, а подальше використання відібраної інформації допускається лише після перевірки слідчим суддею.

Такий підхід сприятиме дотриманню балансу між інтересами кримінального провадження та правом особи на приватність, а також забезпечить відповідність національної практики європейським стандартам захисту прав людини.

Аналогічний підхід простежується і в ч. 2 ст. 168 КПК України, яка, визначаючи порядок тимчасового вилучення майна, одночасно передбачає можливість слідчого або прокурора виготовляти копії інформації з інформаційних (автоматизованих) систем, електронних комунікаційних та інформаційно-комунікаційних систем, комп'ютерних систем і їх невіддільних частин за допомогою технічних, програмно-технічних й апаратно-програмних засобів.

Важливо, що норма містить обов'язкову умову, за якою копіювання здійснюють із залученням спеціаліста, що посилює тезу про технічну зумовленість

роботи з комп’ютерними даними й необхідність спеціальних знань для належного процесуального фіксування та збереження їх цілісності.

Отже, сукупний аналіз цих норм засвідчує: КПК України концептуально розрізняє матеріальний носій електронної інформації та комп’ютерні дані (електронні об’єкти), а також орієнтує правозастосувача на модель доказування, у якій ключовим є процесуально контрольоване копіювання даних (із залученням спеціаліста), а не механічне вилучення техніки.

Перетворення електронного об’єкта на доказ у кримінально-процесуальному значенні відбувається не в момент його існування у віртуальному середовищі, а внаслідок системи процесуальних дій, спрямованих на належну фіксацію відомостей та їх формальне закріплення в матеріалах провадження.

Така фіксація передбачає послідовне виконання уповноваженим суб’єктом кількох технологічно зумовлених операцій: відтворення електронного об’єкта засобами програмного забезпечення; його змістовий і технічний аналіз зі встановленням ключових атрибутів (формату, метаданих, часових міток); описове закріплення виявленої інформації у відповідному процесуальному документі; вилучення електронного об’єкта або зняття його копії на окремий технічний носій із забезпеченням цілісності даних. Завершення цього циклу й надає електронному об’єкту юридичної якості доказу в кримінальному провадженні.

Слід ураховувати, що спосіб фіксації електронного об’єкта в матеріалах провадження може набувати різного процесуального оформлення – повністю електронного або змішаного, з частковим використанням паперових носіїв, однак на правову якість доказу така варіативність процесуальної форми не впливає за умови забезпечення вимог процесуального закону.

Необхідно зазначити, що використання електронних доказів пов’язане з низкою проблемних аспектів, серед яких помилки програмного забезпечення, використання несертифікованих програмних продуктів під час збирання доказової інформації, а також відсутність у суду або сторін процесу можливості здійснити їх належне дослідження без залучення спеціальних знань і відповідних фахівців.

У разі встановлення збою (помилки) програмного забезпечення, його виявлення та процесуальна оцінка мають відповідати сукупності взаємопов'язаних умов, на яких зосереджували увагу І. Вернидубов і С. Белікова:

1) належне підтвердження факту помилки. Наявність програмного збою має бути верифікована службою технічної підтримки розробника, офіційним представником правовласника або іншою компетентною організацією, що здійснює фаховий аналіз і систематизацію програмних дефектів;

2) причиново-наслідковий зв'язок із фіксацією даних. Виявлена помилка повинна бути безпосередньо пов'язана з процесом формування/запису (фіксації) інформації та мати потенціал спричиняти її зміну чи спотворення; це має бути підтверджено експертним висновком;

3) вплив саме на доказово релевантну інформацію. Помилка повинна модифікувати (спотворювати) не будь-які дані, а саме ті відомості, що мають значення для доказування в конкретному провадженні; зазначене також підлягає доведенню шляхом спеціального експертного дослідження [8].

Зазначені критерії заслуговують на підтримку, оскільки вони створюють чіткий алгоритм процесуальної оцінки впливу програмних помилок на достовірність електронного доказу.

Водночас, на нашу думку, цей перелік потребує доповнення четвертою умовою: встановлення того, чи могла помилка бути навмисно ініційована або використана з метою фальсифікації доказу. Ця умова набуває особливого значення в контексті розвитку технологій штучного інтелекту, здатних генерувати правдоподібний, але не автентичний цифровий контент.

Аналіз положень КПК України дає підстави стверджувати, що, з огляду на актуальність і значущість електронних доказів, норми процесуального закону не відповідають фундаментальним ознакам і природі електронних доказів.

Ключовою проблемою є неможливість їх «органічного поглинання» категорією документа. Адже електронні докази за своєю суттю є значно ширшими та виходять за межі класичного поняття документа. У цьому контексті доцільно зауважити, що законодавче регулювання поняття

електронних доказів із пріоритетом електронної інформації, а не матеріального носія, є коректнішим і відповідає сучасним умовам розвитку інформаційного суспільства.

Слід також розробити комплексну нормативну модель, яка охоплюватиме питання їх співвідношення з іншими видами доказів, принципи фіксації, оцінки та зберігання. Це сприятиме не лише уніфікуванню підходів до регулювання доказування в процесуальних галузях права, а й реалізації засад, завдань і принципів кримінального судочинства.

За результатами досудового розслідування прокурор складає обвинувальний акт (ст. 291 КПК України) і направляє його разом з доданими матеріалами до суду першої інстанції (ст. 293 КПК України) для здійснення судового провадження щодо обвинуваченого.

Під час оцінки судом доказів учасники та суд перевіряють доказ на відповідність вимогам кримінального процесуального законодавства, зокрема допустимості такого доказу.

Судова практика засвідчує, що не завжди суд визнає надані стороною обвинувачення електронні докази такими, що відповідають вимогам кримінального процесуального законодавства з певних підстав.

Серед усіх процесуальних властивостей електронних доказів саме допустимість становить найдискусійніший та практично проблемний аспект їх використання в кримінальному провадженні.

Основні практичні проблеми збирання та використання електронних доказів ілюструють результати проведеного нами анкетування. Найвагомішою респонденти вважають відсутність єдиної методики збирання та фіксації (60,0 %), а також складність забезпечення автентичності й цілісності даних (43,1 %), складнощі отримання даних від постачальників послуг (40,0 %), обмеженість технічних засобів (36,9 %) і недостатню кваліфікацію спеціалістів (30,0 %). (додаток В, рис. 8).

Серед елементів допустимості найпроблемнішими визнано належне джерело отримання доказу (48,5 %) і належний спосіб його збирання (46,2 %) (додаток В, рис. 9).

Показово, що 34,6 % опитаних не застосовують жодних спеціальних інструментів забезпечення автентичності та цілісності, натомість геш-суми обчислюють лише 24,6 %, а спеціалізоване криміналістичне програмне забезпечення використовують 13,1 %; комп'ютерно-технічну експертизу електронних доказів не призначали 51,5 % респондентів. (додаток В, рис. 13).

Найбільше доказове значення електронні докази, на думку опитаних, мають у провадженнях щодо кіберзлочинів (64,6 %), злочинів проти власності (50,0 %) і проти основ національної безпеки (48,5 %). (додаток В, рис. 16).

Це підтверджує потребу в стандартизації процедур і належному техніко-криміналістичному забезпеченні

Електронний доказ може бути покладено в основу обвинувального вироку лише за умови відповідності сукупності критеріїв, передбачених законом, – належності, допустимості й достовірності.

На думку Л. М. Лобойка, допустимість доказів – це дозвіл для органу чи посадової особи, яка веде кримінальний процес, у межах положень процесуального права використати їх як докази. Умовами допустимості доказів є: 1) одержання фактичних даних із належного процесуального джерела; 2) одержання фактичних даних належним суб'єктом; 3) одержання фактичних даних у належному процесуальному порядку; 4) належне оформлення джерела фактичних даних [77, с. 120].

О. Толочко зауважує, що допустимість – це властивість доказу, що характеризує його з погляду законності джерела фактичних даних (відомостей, інформації), а також способів одержання та форм закріплення фактичних даних, які містяться в такому джерелі, у порядку, передбаченому кримінальним процесуальним законом, тобто уповноваженими на це особою або органом унаслідок проведення ними слідчої дії за суворого дотримання кримінально-процесуального закону, що визначає форми цієї слідчої дії [129, с. 189].

Визначають такі критерії допустимості доказу: отриманий належним суб'єктом; належне джерело; отриманий з додержанням належної правової процедури; не повинен бути отриманий на підставі неприпустимого доказу; повинен містити дані, походження яких відомо і які можуть бути перевірені; силу доказу, що перевіряють, не повинна перевищувати небезпека несправедливого упередження [125, с. 245–250].

Варто звернути і на дослідження Т. О. Лоскутова, присвячене критеріям визначення допустимості доказів у кримінальному провадженні; автор слушно наголошує, що проблема допустимості посідає одне з центральних місць у теорії доказів і доказування [78]. Ці загальнотеоретичні критерії зберігають значення й для електронних доказів і слугують відправною точкою для подальшого аналізу особливостей їх допустимості, зумовлених електронною формою інформації, що здійснюється далі в цьому підрозділі.

Аналізуючи питання правової регламентації допустимості доказів, необхідно зазначити, що згідно зі ст. 86 та 87 КПК України доказ визнають допустимим, якщо його отримано в порядку, передбаченому КПК України. Недопустимим є доказ, отриманий внаслідок істотного порушення прав і свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також будь-який інший доказ, здобутий завдяки інформації, отриманій внаслідок істотного порушення прав і свобод людини [76]

Слід зазначити, що належність і допустимість доказів є самостійними правовими властивостями, що оцінюють за різними критеріями і не зумовлюють одна одну: належний доказ може виявитися недопустимим, якщо отриманий з порушенням процесуального порядку, а неналежний – залишатися допустимим за умови дотримання процедури його отримання [6, с. 365].

На наше переконання, у контексті електронних доказів зазначений принципово незалежний характер належності й допустимості набуває додаткового змісту: електронний об'єкт, отриманий з дотриманням технологічної процедури (фіксації хеш-суми, забезпечення цілісності файлу, збереження метаданих),

залишається допустимим, навіть якщо в конкретному провадженні не виявиться належним. І навпаки, релевантність електронного доказу не вирішує питання щодо порушень процедури його отримання.

М. М. Стоянов зазначає, що вчені-процесуалісти називають серед умов допустимості доказів у кримінальному провадженні такі елементи: належний суб'єкт, належний спосіб, належне джерело, належна форма закріплення відомостей про факти [126, с. 245].

Бути визнані допустимими та використаними як доказ у кримінальному провадженні можуть тільки фактичні дані, одержані згідно з вимогами КПК України.

Згідно з Рішенням Конституційного Суду України від 20 жовтня 2011 року № 12-рп/2011, «визнаватися допустимими і використовуватися як докази в кримінальній справі можуть тільки фактичні дані, одержані відповідно до вимог кримінально-процесуального законодавства. Перевірка доказів на їх допустимість є найважливішою гарантією забезпечення прав і свобод людини й громадянина в кримінальному процесі та ухвалення законного і справедливого рішення у справі» [114].

Оцінка доказів на предмет їхньої допустимості є однією з гарантій забезпечення прав і свобод людини й громадянина в кримінальному процесі та прийняття законного і справедливого рішення [113, с. 210].

Конституційно-правовою основою інституту допустимості доказів у національній правовій системі є положення ч. 3 ст. 62 Конституції України, згідно з якою обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом.

Зосередимо увагу на окремих елементах допустимості.

Належний суб'єкт отримання доказу як критерій його допустимості означає, що збирання, перевірка та формальне закріплення фактичних даних має здійснювати виключно той учасник кримінального провадження, на якого процесуальний закон покладає відповідні повноваження.

Належність суб'єкта доказування чітко пов’язано із колом осіб, уповноважених на досудове розслідування, а саме слідчі органу досудового розслідування - одноособово або у складі слідчої групи (ч. 2 ст. 38 КПК). Реалізація цих повноважень у конкретному провадженні потребує, як належної підслідності органу (ст. 216 КПК), так і персонального визначення слідчого, оскільки керівник органу досудового розслідування уповноважений визначати слідчого (слідчих), який здійснюватиме розслідування у конкретному кримінальному провадженні (п. 1 ч. 2 ст. 39 КПК).

КПК передбачає й інші підстави, за яких слідчий (дізнавач) зберігає чи набуває статусу належного суб'єкта. Якщо особі стало відомо про правопорушення, розслідування якого не віднесене до її компетенції, вона повідомляє про це прокурора і проводить розслідування доти, доки той не визначить іншу підслідність (ч. 2 ст. 218 КПК). Повноваження виникають також у разі доручення, тобто слідчий чи прокурор своєю постановою може доручити проведення слідчих (розшукових) та негласних слідчих (розшукових) дій органу, під юрисдикцією якого перебуває відповідна територія (ч. 6 ст. 218 КПК).

Поряд із цими юридичними підставами належність суб'єкта має, на наш погляд, і інші юридичні факти, які мають бути враховані, а саме повноваження слідчого реально існують лише тоді, коли особа на момент проведення процесуальних дій фактично обіймає відповідну посаду й виконує службові обов'язки.

Процесуальний інструментарій збирання електронних документів у кримінальному провадженні має диференційований характер залежно від суб’єкта доказування. Для сторони обвинувачення такий інструментарій охоплює: гласні слідчі (розшукові) дії, передбачені главою 20 КПК України, насамперед огляд електронних інформаційних систем, обшук із можливістю фіксації комп’ютерних даних, тимчасове вилучення майна; негласні слідчі (розшукові) дії, врегульовані главою 21 КПК України, які застосовують за умов, визначених ст. 246, 248 цього Кодексу; заходи забезпечення кримінального провадження, серед яких ключове

значення для електронних об’єктів має тимчасовий доступ до речей і документів (ст. 159–166 КПК України).

Сторона захисту, не маючи повноважень на проведення слідчих (розшукових) дій, реалізує своє право на збирання електронних доказів через подання запитів, ініціювання процесуальних дій шляхом подання клопотань, а також через звернення до слідчого судді з клопотанням про надання тимчасового доступу (інструмент, потенціал якого в національній практиці використовують недостатньо).

Тимчасовий доступ до речей і документів як один із заходів забезпечення кримінального провадження (п. 5 ч. 2 ст. 131 КПК України) у контексті електронних доказів набуває особливого значення з огляду на специфіку об’єкта, до якого надають доступ.

Відповідно до абзацу 2 ч. 1 ст. 159 КПК України, тимчасовий доступ до електронних інформаційних систем, комп’ютерних систем або їх частин, мобільних терміналів систем зв’язку здійснюють шляхом зняття копії інформації – без вилучення носія, що принципово відрізняє цей інститут від типового тимчасового доступу до матеріальних документів. Інформація, яка знаходиться у володінні операторів і провайдерів телекомунікацій про зв’язок, абонента, надання телекомунікаційних послуг, віднесена законодавцем до охоронюваної законом таємниці (п. 7 ч. 1 ст. 162 КПК України), її отримання потребує дотримання посиленої процедури за участю особи-володільця (ч. 4 ст. 163 КПК України).

Попри формальну рівність сторін у можливості звернутися з клопотанням про тимчасовий доступ (ст. 22 КПК України), правозастосовна практика вказує на наявність системної асиметрії в користуванні цим інститутом.

У дослідженні практичних аспектів тимчасового доступу за клопотаннями захисту В. Михайленко доводить, що представники сторони захисту недостатньо активно використовують цей захід забезпечення, а наявні відмови в задоволенні клопотань переважно зумовлені недоліками в обґрунтуванні чи формуванні клопотання, а не упередженістю слідчих суддів [83].

Цей висновок засвідчують і кількісні дані узагальнень судової практики: за результатами розгляду клопотань про тимчасовий доступ у судах першої інстанції рівень задоволення сягає 83–97 %, однак переважну більшість таких клопотань становлять клопотання сторони обвинувачення, що свідчить про асиметричну активність сторін, а не про принципову відмову судів захищати інтереси сторони захисту [52].

Водночас сучасна практика Вищого антикорупційного суду демонструє позитивну тенденцію до фактичного врівноваження процесуальних можливостей. Показовою в цьому контексті є ухвала слідчого судді ВАКС від 25 червня 2025 року, постановлена за результатами розгляду клопотання захисника підозрюваного про тимчасовий доступ до інформації оператора мобільного зв'язку – відомостей про з'єднання абонентів, тривалість і час дзвінків, локаційні дані базових станцій, IMEI мобільних терміналів.

Такі відомості були необхідні для перевірки даних протоколу огляду, на якому ґрунтується повідомлення про підозру, і для проведення експертизи електронних комунікацій за ініціативою сторони захисту. Слідчий суддя задовольнила клопотання частково, що свідчить про принципову готовність судової практики визнавати за стороною захисту автономний інструмент збирання електронних доказів через інститут тимчасового доступу [135].

Зазначене дає підстави стверджувати, що проблема дисбалансу процесуальних можливостей сторін під час отримання тимчасового доступу до електронних доказів має двоїсту природу: з одного боку, це недостатня активність сторони захисту в обґрунтуванні відповідних клопотань, з іншого – брак у чинному КПК України спеціалізованих процесуальних механізмів, які враховували б специфіку електронних об'єктів доказування (наприклад, відсутність обов'язку для сторони обвинувачення складати звітний документ про виконання ухвали створює асиметрію у фіксації доказової бази).

Зазначені аспекти потребують самостійного розгляду в контексті вдосконалення інституту тимчасового доступу до електронних інформаційних

систем і мобільних терміналів, що буде запропоновано у висновках до цього розділу.

Отримання електронного доказу не завжди потребує дозволу слідчого судді: якщо відповідну інформацію добровільно надає її володілець або власник, застосування інституту тимчасового доступу до речей і документів не є обов'язковим.

Важливою для оцінки допустимості доказів є правова позиція, висловлена Верховним Судом у постанові Касаційного кримінального суду від 29 вересня 2020 року у справі № 601/1143/16 [94], згідно з якою законодавець застосовує асиметричний підхід до правил доказування в кримінальному процесі: ч. 3 ст. 17 КПК України забороняє ґрунтувати обвинувачення на доказах, отриманих незаконним шляхом, однак не містить аналогічної категоричної заборони стосовно доказів, які надають на спростування обвинувачення і свідчать на користь сторони захисту.

Суд зауважив, що правила оцінки доказів мають на меті запобігання неправомірному втручанню держави та заохочення доброчесної поведінки правоохоронних органів, а визнання доказів недопустимими внаслідок порушень має позбавити сторону, яка їх допустила, можливості скористатися результатами такого порушення; тож застосування цих правил на шкоду стороні, не відповідальній за процесуальні порушення, суперечить їх меті [94].

Критерій належного процесуального джерела є однією із фундаментальних передумов допустимості електронного доказу: відсутність такого джерела унеможливлює використання відповідних фактичних даних у доказуванні незалежно від їх інформаційної цінності.

Водночас слід розмежовувати два рівні аналізу цієї проблематики. На рівні de lege ferenda (з позиції закону, який має бути ухвалено) обґрунтована в попередньому підрозділі позиція щодо необхідності законодавчого закріплення електронного доказу як самостійного джерела доказів у ст. 84 КПК України є незмінною.

Однак на рівні de lege lata (з погляду наявного закону), з огляду на чинне законодавче регулювання, яке закріплює вичерпний перелік із чотирьох процесуальних джерел доказів (ч. 2 ст. 84 КПК України), електронний доказ на сучасному етапі підлягає процесуальному оформленню або як документ, або як речовий доказ. До внесення відповідних законодавчих змін практичне значення має коректне розмежування цих двох форм процесуального оформлення.

Розмежування електронного документа та речового доказу в електронній формі слід здійснювати з урахуванням того, що саме становить доказову цінність для встановлення обставин кримінального провадження, – інформаційний зміст електронного об'єкта чи його матеріальний (технічний) носій: у першому випадку йдеться про електронний документ, у другому – про речовий доказ в електронній формі.

Сформульований методологічний критерій дає змогу коректно вирішувати на практиці проблему процесуальної кваліфікації одного й того самого електронного об'єкта.

Розглянемо ситуацію, коли в матеріалах провадження фігурує електронне листування, отримане з облікового запису підозрюваного в певному месенджері або поштовому сервісі. Доказова цінність такого об'єкта зумовлена змістом повідомлення, тобто інформацією, що має значення для кримінального провадження, а не фізичними характеристиками пристрою, з якого це повідомлення було відкрито чи скопійовано.

У таких випадках телефон, комп'ютер або інший термінал є лише технічним засобом доступу до інформації, що первинно зберігається на віддаленому сервері постачальника послуг, натомість власне доказом у вигляді документа є саме інформаційний зміст повідомлення, незалежно від того, чи представлений він в оригіналі (через прямий доступ до облікового запису), чи у вигляді похідного об'єкта (скриншоту, експортованого файлу, належно засвідченої паперової роздруківки).

Зазначене розмежування має пряме процесуальне значення: збирання, перевірку й оцінку електронного документа здійснюють за правилами,

передбаченими ст. 99 КПК України, натомість речовий доказ в електронній формі підпорядковується режиму, встановленому ст. 98 КПК України, що передбачає принципово різні вимоги до процесуального оформлення та оцінки.

На думку А. П. Запотоцького, доказове значення в документах як джерелах доказів має лише зміст, натомість у документах як речових доказах має значення не лише зміст, а й форма, місце та час їх виявлення тощо [59, с. 8].

Поряд із вимогою щодо належного суб'єкта й належного джерела критерій допустимості охоплює дотримання процесуальної форми закріплення фактичних даних, передбаченої КПК України.

Ця форма реалізується через комплекс взаємопов'язаних процесуальних інструментів: процедуру проведення слідчих (розшукових) і негласних слідчих (розшукових) дій (глави 20–21 КПК), застосування заходів забезпечення кримінального провадження (розділ ІІ КПК України), а також їх документальне закріплення в протоколах і додатках, які складають за положеннями ст. 103–105 КПК України.

У кримінальних провадженнях з електронними доказами, на нашу думку, вимога процесуального закріплення набуває розширеного змісту, оскільки, крім традиційного протокольного оформлення, вона передбачає документування технічних параметрів операцій з електронним об'єктом (наприклад, застосованого програмного забезпечення, хеш-сум, метаданих і часових міток фіксації, без яких процесуальна форма не може забезпечити верифікованості доказу).

Схожу позицію щодо розширеного змісту процесуальної форми в провадженнях з електронною доказовою базою послідовно обґрунтовують А. В. Гутник й А. Я. Хитра [49, с. 88–95].

Для того щоб предмет матеріального світу отримав процесуальний статус «речового доказу», зазначає І. Л. Чупрікова, він повинен не лише містити сліди, а й бути належно зафіксованим, оформленим, залученим до справи тощо [141, с. 268].

Відповідно до ст. 103 КПК України, процесуальні дії під час кримінального провадження можуть фіксувати: у протоколі; на носії інформації, на якому за

допомогою технічних засобів зафіксовано процесуальні дії; у журналі судового засідання.

Порядок складання протоколу й додатків, ведення журналу судового засідання, створення носія інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії, їх обов'язкові реквізити та вимоги до них передбачені в главі 5 КПК України.

Правозастосовна практика українських судів містить численні приклади визнання електронних доказів недопустимими через недоліки їх процесуальної фіксації на стадії досудового розслідування.

У цьому контексті орієнтиром для правозастосування стають висновки Верховного Суду, які дають змогу учасникам кримінального провадження передбачити оцінку доказів, які збирають, ужити заходів для належного збирання та фіксування доказів.

Порядок оцінки електронного доказу та його допустимості конкретизовано в низці постанов ККС ВС.

У постанові колегії суддів Першої палати ККС ВС від 30 вересня 2021 року у справі № 498/582/18 визначено, що ототожнення електронного доказу як засобу доказування та матеріального носія такого документа – безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія (п. 31 постанови) [103].

На нашу думку, саме цей висновок суду вніс у нормативну сферу окреме розуміння електронного доказу як джерела доказу та поклав початок утвердженню в національному кримінальному процесі його як виду доказу.

Подальший розвиток зазначені позиції отримали в постанові об'єднаної палати ККС ВС від 25 вересня 2023 року у справі № 208/2160/18, яка закріпила правило, згідно з яким допустимість електронного документа як доказу не можна заперечувати лише на підставі того, що він має електронну форму [106].

Аналіз зазначених судових рішень дає підставу констатувати формування на рівні найвищого органу окремої гілки влади – Верховного Суду, стійкої правової позиції, яку можна визначити як «презумпцію допустимості електронної форми

доказу», тобто електронна форма доказу не є підставою для визнання такого доказу недопустимим.

Підставою для визнання електронного доказу недопустимим мають бути пов’язані з порушенням процесуального порядку його отримання, а не з формою існування інформації.

Окремо слід зауважити, що в електронного доказу переважно немає жорсткої прив’язки до конкретного матеріального носія, що має принципові практичні наслідки для оцінки допустимості електронних доказів: копія електронного документа, отримана в процесуально належний спосіб, за своєю доказовою силою не є похідним доказом у класичному розумінні, це самостійний примірник оригіналу.

Сформована судовою практикою презумпція рівнозначності електронних примірників створює сприятливий процесуальний режим для доказування в кримінальному провадженні, оскільки слідчий чи прокурор не зобов’язані пред’являти саме оригінальний пристрій фіксації (камеру, реєстратор, сервер), а можуть оперувати будь-яким технічним носієм, на якому зафіксовано відповідний цифровий об’єкт, за умови дотримання вимог щодо належного процесуального джерела та порядку отримання.

Це Верховний Суд обґрунтував ще раніше. У постанові ККС ВС від 10 вересня 2020 року у справі № 751/6069/19 суд зазначив, що записаний на оптичний диск – носій інформації електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа, один і той самий електронний документ може існувати на різних носіях, і всі ідентичні за змістом примірники електронного документа можуть розглядати як оригінали та відрізнятися один від одного лише часом і датою створення [101].

Додатковим підтвердженням цієї позиції є постанова ККС ВС від 26 січня 2021 року у справі № 236/4268/18, у якій суд, посилаючись на ст. 7 Закону України «Про електронні документи та електронний документообіг», констатував, що якщо сторона захисту не оспорює достовірності відображення слідчих дій на електронних записах, то факт долучення до матеріалів провадження копій цих

записів, зафіксованих на оптичних дисках, не суперечить вимогам кримінального процесуального закону, оскільки у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважають оригіналом [100].

Показовим прикладом практичного застосування правових позицій ККС ВС щодо недопустимості копій електронних доказів є вирок Ковельського міськрайонного суду Волинської області від 5 квітня 2024 року у справі № 159/4835/19 [25].

Розглядаючи допустимість USB-накопичувача SanDisk 128 GB як речового доказу, суд встановив низку процесуальних недоліків, зокрема розбіжності в номерах кримінальних проваджень, у межах яких надавали дозвіл на обшук, проводили обшук й ухвалювали рішення про визнання накопичувача речовим доказом.

Суд констатував, що за відсутності підстав для використання копій, передбачених ч. 5 ст. 99 КПК України, такі фотокопії є недопустимим доказом, а наявні сумніви, що виникли з процесуальних розбіжностей, витлумачив на користь сторони захисту відповідно до ч. 4 ст. 17 КПК України [25].

Таке рішення ілюструє поступове утвердження в національному кримінальному процесі жорсткого стандарту оцінки допустимості електронних доказів, згідно з яким тягар доказування дотримання процесуального порядку отримання електронного доказу та його автентичності покладено на сторону, що його подає, а будь-які обґрунтовані сумніви щодо цілісності процесуальної «біографії» електронного носія, від моменту вилучення до долучення як доказу, можуть тлумачити на користь сторони захисту.

Такий підхід, сформований судовою практикою ще до широкого поширення генеративних технологій штучного інтелекту, закладає нормативне підґрунтя для подальшого впровадження посилених вимог щодо перевірки автентичності електронних доказів на предмет можливого штучного генерування чи модифікації, що набуває особливої актуальності в умовах технологічної еволюції засобів фальсифікації цифрового контенту.

Про формування системного підходу Верховного Суду до електронних доказів свідчать і тематичні заходи судової влади.

У лютому 2025 року суддя ВС у ККС Наталія Марчук під час курсу програми HELP Ради Європи «Кіберзлочинність та електронні докази» акцентувала, що прокурор має обґрунтувати походження електронних доказів для оцінки їх належності й допустимості, а докази, отримані з відкритих джерел, необхідно перевіряти крізь призму Берклійського протоколу [124].

Суддя Верховного Суду Надія Стефанів у межах круглого столу «Електронні докази в кримінальному процесі» зазначила, що суди повинні перевіряти цілісність й автентичність електронних доказів, а Верховний Суд 2023 року закріпив концепцію презумпції цілісності електронних доказів: їх можуть подавати в цифровому вигляді з електронним підписом, а учасник, що сумнівається в достовірності, має обґрунтувати свої сумніви [58].

Водночас Голова ВС Станіслав Кравченко зазначив, що поширеними стали випадки, коли сторона захисту заявляє клопотання про недопустимість електронних доказів на підставі копіювання файлу на різні носії, однак за аргументами про недопустимість радше криється сумнів у достовірності (автентичності), а не в допустимості [58]. Зазначене спостереження Голови ВС підтверджує висновок, сформульований вище: критерій допустимості електронного доказу слід оцінювати через дотримання процесуального порядку його отримання, а не через форму чи кількість копій носія.

У дослідженні порушеного питання вбачаємо за необхідне зазначити, що в судових процесах Європейський суд з прав людини повноцінно використовує електронні докази, а суд сформував ґрунтовну практику щодо оцінки та характеристики електронних доказів.

Наприклад, у справі «Georgia v. Russia (II)», заява № 38263/08 від 21 січня 2021 року, ЄСПЛ урахував електронну інформацію, отриману з відкритих джерел. Суд посилався на доповідь, опубліковану Американською асоціацією сприяння розвитку науки (AAAS), «Супутникові знімки високої якості та конфлікт у Південній Осетії» від 9 жовтня 2008 року. Суд урахував, що AAAS є міжнародною

недержавною, некомерційною організацією, метою якої є сприяння розвитку науки у світі. Аналіз супутникових знімків у цій доповіді врахував суд як доказ (§ 66, 188, 205) [160].

2.2. Належність, достатність і достовірність електронних доказів

Належність і допустимість електронних доказів хоча і є взаємопов'язаними категоріями, однак є окремими характеристиками доказу.

Відповідно до ст. 85 КПК України, належними є докази, які прямо чи непрямо підтверджують існування 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.

Отже, належність доказів – це внутрішня властивість доказу, унаслідок якої він здатний встановити обставини, необхідні для повного та правильного вирішення кримінального провадження.

М. М. Стоянов визначає належність доказів як властивість доказу, що характеризує зв'язок відомостей, які становлять його зміст, з обставинами, що підлягають доказуванню в кримінальному провадженні [126, с. 9].

О. С. Степанов зазначає, що належність доказів – це один із критеріїв оцінки доказів, що виражає об'єктивний зв'язок будь-яких відомостей, що пов'язані з обставинами конкретного кримінального провадження, а точніше – з обставинами, що належать до предмета доказування [121, с. 10].

В. В. Вапнярчук вважає, що зміст доказу має підтверджувати принаймні один з трьох видів обставин: 1) належать до загального предмета доказування (ст. 91 КПК); 2) мають значення доказових фактів (тобто використовують як аргументи, логічні посилки для встановлення перших); 3) мають значення допоміжних фактів, зокрема тих, що стосуються достовірності чи недостовірності, допустимості чи

недопустимості отримання інших доказів (неналежність понятих, які перебували під час проведення слідчої (розшукової) дії) [6, с. 242].

Слушним є твердження Д. Б. Сергєєвої: «Тільки визначивши, які саме обставини кримінального провадження необхідно встановити, можна вирішити питання про належність конкретних фактичних даних до кримінального провадження» [117, с. 236].

Зазначений підхід отримав подальший розвиток у дослідженнях стосовно електронних доказів з відкритих джерел.

На основі узагальнення положень ст. 85 КПК України та судової практики систематизовано три групи обставин, що можуть встановлювати електронними доказами та доказами з відкритих джерел: 1) обставини, передбачені ст. 91 КПК України (головний факт); 2) обставини локального предмета доказування – фактичні обставини, що підлягають доказуванню під час прийняття окремих процесуальних рішень (зокрема щодо застосування заходів забезпечення кримінального провадження, спеціального досудового розслідування або судового провадження, належних викликів учасників); 3) допоміжні факти – обставини для виявлення та перевірки інших обставин чи доказів, зокрема щодо місцезнаходження осіб, речей і документів, перевірки достовірності інших доказів [72, с. 239–240].

Положення ч. 1 ст. 91 КПК України визначає обставини, які підлягають доказуванню, зокрема подія кримінального правопорушення, винуватість обвинуваченого тощо [76].

Тому в разі використання електронного доказу він, як і інші види доказів, має встановлювати певну обставину, яка належить до предмета доказування.

Слід зауважити, що для різних категорій кримінальних проваджень притаманні предмет доказування та види електронних доказів. Це виявляється на прикладі вибірки вироків у кримінальних провадженнях щодо незаконного обігу наркотичних засобів і психотропних речовин за 2023–2026 роки.

У цій категорії справ електронні джерела доказової інформації найчастіше фіксують у формі електронного листування через месенджер Telegram щодо

замовлення, придбання, фасування, пересилання або збуту заборонених речовин [11–13; 18; 21; 24; 26; 28; 32; 33; 38; 39].

Також поширеним є використання інтернет-крамниць, телеграм-каналів, чат-ботів і сторінок користувачів у Telegram для прийняття замовлень, організації комунікації між учасниками схеми та покупцями, а також отримання оплати [13; 21; 22; 32; 39].

У низці вироків прямо описано створення або адміністрування телеграм-каналів, чат-ботів чи інтернет-магазинів, через які здійснювали віддалений збут наркотичних засобів і психотропних речовин [13; 21; 22; 39].

Окрему групу електронних слідів становлять відомості про розміщення «закладок», а саме адреси, фотознімки місцевості, координати, геолокаційні дані, описи місць приховання та повідомлення про виконання завдань із розкладання наркотичних засобів чи психотропних речовин [11–13; 24; 26; 32; 33; 38; 41].

Зокрема, у вироках зафіксовано, що особи, які виконували роль «закладчиків», фотографували місця приховання, зазначали геолокацію або координати кожної «закладки» та надсилали ці відомості через Telegram організатору, адміністратору або іншому учаснику злочинної схеми для подальшого збуту [11; 12; 26; 32; 38; 41].

У деяких провадженнях також описано використання спеціальних застосунків для створення фотозображень із геолокаційною прив’язкою, зокрема GPS MAP CAMERA або NoteCam [26; 28].

Крім того, судова практика підтверджує використання поштових сервісів, насамперед ТОВ «Нова Пошта», для отримання, пересилання або подальшого збуту наркотичних засобів і психотропних речовин [12; 13; 18; 32; 33; 38; 39; 41].

У вироках підтверджено отримання відправлень у поштоматах або відділеннях, пересилання заборонених речовин покупцям, використання вигаданих чи змінених анкетних даних, а також фіксацію номерів товарно-транспортних накладних та інших відомостей про поштові відправлення [18; 28; 33; 39; 41].

Отже, листування в Telegram, дані телеграм-каналів і чат-ботів, фотознімки місць «закладок», координати й геолокаційні дані, відомості про поштові

відправлення та електронні платіжні операції утворюють комплекс електронних доказів у кримінальних провадженнях цієї категорії.

Відомості, що містяться в електронних документах та відкритих онлайн-джерелах, можуть використовувати в кримінальному провадженні як фактичні дані, що мають значення для встановлення обставин, передбачених ст. 91 КПК України, а також для висунення й перевірки слідчих версій, ідентифікації можливих учасників кримінального правопорушення, з'ясування характеру їхньої діяльності, встановлення зв'язків між ними та перевірки інших доказів у їх сукупності.

Показовим у цьому контексті є вирок Івано-Франківського міського суду Івано-Франківської області від 23 грудня 2025 року у справі № 344/19190/25 [23], у якому суд досліджував протоколи огляду електронної інформації, отриманої з відкритих джерел мережі Інтернет, зокрема матеріали телеграм-каналу, відеозапис, фотознімки, текстові публікації, а також відомості з вебсайту «народного совета луганской народной республики», що стосувалися організації та проведення незаконного референдуму на тимчасово окупованій території.

У цьому кримінальному провадженні суд визнав відповідні дані належними, допустимими й достовірними, оскільки вони підтверджували обставини, що підлягали доказуванню, були отримані у встановленому КПК України порядку та не були спростовані іншими доказами.

Важливим є те, що суд окремо зазначив про використання даних, зібраних із відкритих джерел за допомогою розвідки з відкритих джерел – OSINT, з посиланням на Протокол Берклі як орієнтир мінімальних стандартів пошуку, збирання, зберігання, перевірки й аналізу цифрової інформації з відкритих джерел.

Такий підхід узгоджується з правовою позицією Касаційного кримінального суду Верховного Суду, висловленою в постанові від 21 липня 2025 року у справі № 201/11849/23, відповідно до якої протоколи огляду інтернет-сторінок і телеграм-каналів разом із додатками, у яких за допомогою скриншотів, друку або запису на технічні носії зафіксовано зміст електронної інформації, можуть визнавати

допустимими доказами за умови їх отримання в порядку, передбаченому КПК України, і здатності підтверджувати обставини, що підлягають доказуванню [98].

У контексті нашого дослідження увагу привертають і непрямі електронні докази. Слід зазначити, що такі непрямі докази обов'язково слід оцінювати не ізольовано, а в сукупності – як цілісну систему, у межах якої кожен елемент є взаємоузгодженим з іншими та посилює їх доказове значення. Тож між непрямими доказами має простежуватися внутрішній логічний зв'язок, що забезпечує їх взаємне підтвердження.

У кримінальному провадженні учасники процесу нерідко формують відмінні версії події правопорушення, у зв'язку з чим оцінка належності одного й того самого доказу може істотно варіюватися.

Вирішення питання про належність, з одного боку, ґрунтується на нормативних критеріях, закріплених, зокрема, у ст. 85 та ст. 91 КПК України, а з іншого – залежить від суб'єктивного сприйняття суб'єкта доказування. Таке сприйняття ґрунтується на його уявленні про логічний зв'язок між фактичними даними, що становлять зміст доказу, й обставинами, які підлягають доказуванню у кримінальному провадженні відповідно до ст. 91 КПК України.

У судовій практиці трапляються випадки, коли електронні дані, отримані з електронного середовища, не набувають самостійного доказового значення через відсутність належного зв'язку з предметом доказування, неперевіреність джерела їх походження або істотні недоліки процесуальної фіксації.

З позицій кримінального процесу ключовим є не електронний характер інформації, а її здатність підтверджувати чи спростовувати обставини, передбачені ст. 91 КПК України, а також дотримання встановленого законом порядку її отримання, фіксації та перевірки.

Показовим у цьому аспекті є вирок Нововоронцовського районного суду Херсонської області від 24 березня 2026 року у справі № 954/674/25, постановлений у кримінальному провадженні за обвинуваченням особи у вчиненні кримінального правопорушення, передбаченого ч. 5 ст. 111-1 КК України [27].

У цьому провадженні суд, з одного боку, досліджував протоколи огляду інтернет-ресурсів й інші матеріали електронного походження, що стосувалися функціонування окупаційної адміністрації. Водночас суд не надав оцінки тим показанням свідків, у яких відомості про діяльність обвинуваченої та її співпрацю з окупаційною владою ґрунтувалися не на безпосередньому сприйнятті обставин, а лише на інформації із соціальних мереж або зі слів місцевих жителів.

Крім того, у цій справі суд визнав недопустимими окремі протоколи пред'явлення особи для впізнання за фотознімками, оскільки до них не було долучено додатків, за якими можливо було б встановити, чи зображена обвинувачена на відповідному фотознімку та під яким номером.

Інші протоколи впізнання суд визнав неналежними доказами, оскільки вони не містили відомостей про номер фотокартки, обраної свідком, або не давали змоги встановити особу, яку фактично впізнавали.

Така позиція узгоджується із загальними положеннями кримінального процесуального закону, відповідно до яких доказами є фактичні дані, отримані в передбаченому КПК України порядку, а належність і допустимість доказів визначають з огляду на їх зв'язок з обставинами, що підлягають доказуванню, та законність способу їх одержання.

Отже, відомості з електронних джерел, соціальних мереж, фотозображень або інтернет-ресурсів не можуть використовувати як повноцінні докази лише з огляду на факт їх виявлення чи долучення до матеріалів кримінального провадження.

Для набуття доказового значення вони мають бути належно процесуально зафіксованими, мати встановлене або перевірюване джерело походження, бути пов'язаними з предметом доказування, їх оцінює суд у сукупності з іншими доказами.

Специфіка електронних доказів ставить перед критерієм належності додаткові питання, не характерні для традиційних джерел доказів. Зокрема, метадані електронного файлу (дата створення, дата останньої модифікації, геолокація, IP-адреса, ідентифікатор пристрою) можуть самостійно встановлювати

обставини, що належать до предмета доказування за ст. 91 КПК України (надзвичайно актуальними є час, місце й обстановку вчинення кримінального правопорушення).

Тобто, на нашу думку, належність електронного доказу не обмежується тільки його змістовою складовою (текстом повідомлення, зображенням, відеозаписом), а поширюється також на службову інформацію, яка супроводжує електронний об'єкт.

Практичне значення цього висновку полягає в тому, що під час збирання електронних доказів суб'єкт доказування має фіксувати не лише зміст електронного об'єкта, а й повний масив його метаданих, оскільки їхня втрата може призвести до звуження доказового потенціалу

Достатність доказів визначає необхідний і достатній обсяг відомостей для висновку про встановлення предмета доказування.

За результатами оцінки доказів суд може прийняти рішення стосовно доведеності таких обставин (ч. 1 ст. 368, ст. 373 КПК України): 1) чи наявна подія вчинення кримінального правопорушення; 2) чи містить це діяння склад кримінального правопорушення; 3) чи кримінальне правопорушення вчинене обвинуваченим і чи винен обвинувачений у його вчиненні [76].

На нашу думку, оцінка достатності доказів становить методологічно найскладніший етап доказової діяльності, оскільки результати всіх попередніх етапів (перевірки належності, допустимості й достовірності кожного окремого доказу) слугують підготовкою саме для цього висновку.

На відміну від інших властивостей доказу, достатність характеризує не одиничний доказ, а їх сукупність і зумовлена спроможністю цієї сукупності обґрунтувати конкретне процесуальне рішення.

У зв'язку з цим достатність не має кількісного критерію, оскільки в конкретному провадженні висновок може бути обґрунтований і незначною кількістю доказів, натомість в іншому навіть значно більший обсяг доказової бази може виявитися недостатнім для однозначного висновку.

Тобто, визначальною є не кількість, а змістовна спроможність наявної сукупності встановити обставини, що підлягають доказуванню (ст. 91 КПК України).

За оцінками практиків, електронні докази посідають вагоме місце в системі засобів доказування: за результатами проведеного автором анкетування, 55,4 % опитаних вважають їх рівнозначними іншим видам доказів, 6,2 % – такими, що превалюють, і лише 36,9 % відводять їм допоміжну (другорядну) роль. Це підтверджує тезу про посилення доказового значення електронної інформації та обґрунтованість підвищених вимог до її перевірки й оцінки (додаток В, рис. 15).

Природа електронних об’єктів дає змогу швидко збирати (агрегувати) у великих обсягах як самі електронні докази та формувати численні похідні об’єкти від них (копії, скриншоти, витяги), що створює оманливе враження «кількісної надлишковості» електронних доказів за реальної відсутності їх змістовної унікальності.

Також ефективна перевірка електронного доказу часто потребує супутніх доказів (метаданих, протоколів огляду, висновків експертів щодо цілісності), без яких цифровий об’єкт не утворює достатньої сукупності для обґрунтування процесуального рішення.

В. В. Вапнярчук акцентує, що на підставі певної сукупності доказів може бути сформульовано певний висновок (імовірний чи достовірний) та прийнято відповідне процесуальне рішення [6, с. 290].

Стосовно електронних доказів питання достатності має ще один додатковий важливий аспект. Окремий електронний доказ, наприклад, скриншот листування в месенджері, за певних обставин може бути визнано недостатнім для встановлення обставин, що підлягають доказуванню.

Зазначене підтверджує і судова практика, оскільки в низці рішень судів у сфері цивільного та господарського судочинства здійснено висновки щодо недостатності скриншотів для встановлення обставин.

Скриншот фіксує лише візуальне відображення інформації на екрані в конкретний момент часу, але не підтверджує ні автентичність повідомлення, ні ідентичність співрозмовника, ні відсутність модифікацій.

Для формування достатньої сукупності доказів скриншот потребує підкріплення метаданими повідомлення, логами сервера месенджера, результатами експертного дослідження пристрою та, за необхідності, показаннями учасників листування.

Отже, електронні докази за своєю природою тяжіють до функціонування в сукупності, а не ізольовано, що зумовлює підвищені вимоги до повноти їх збирання.

У контексті електронних доказів критерій достатності актуалізує питання верифікованості, оскільки один електронний об’єкт без супутніх метаданих, протоколу огляду й підтвердження походження не утворює достатньої сукупності для прийняття процесуального рішення на його основі [54, с. 7].

Оцінку достатності зібраної сукупності доказів здійснює суб’єкт доказування (слідчий, дізнавач, прокурор, слідчий суддя, суд) на кожному етапі кримінального провадження, що передує прийняттю процесуального рішення або ініціюванню чергової процесуальної дії, зокрема слідчих (розшукових) і негласних слідчих (розшукових) дій.

Висновок про достатність формують на основі внутрішнього переконання відповідного суб’єкта згідно з вимогами ч. 1 ст. 94 КПК України. Одна й та сама сукупність доказів може бути визнана як достатньою (наприклад, судом першої інстанції), так і недостатньою (наприклад, судом апеляційної інстанції) [6, с. 290].

Якщо під час судового розгляду буде встановлено, що сторона обвинувачення не довела винуватість особи поза розумним сумнівом, суд ухвалює виправдувальний вирок.

У контексті кримінального процесу це є наслідком не лише фактичної недостатності доказової сукупності, а й виключення з неї доказів, які не відповідають вимогам належності, допустимості, достовірності та взаємозв’язку.

Відповідно до ст. 86 КПК України, доказ є допустимим лише за умови його отримання в порядку, встановленому законом, а недопустимий доказ не може бути використаний під час ухвалення судового рішення. Стаття 87 КПК України також передбачає недопустимість доказів, отриманих унаслідок істотного порушення прав і свобод людини, а також похідних від них доказів.

Показовим у цьому аспекті є вирок Івано-Франківського міського суду Івано-Франківської області від 29 квітня 2025 року у справі № 344/7425/16-к, у якому особу обвинувачували у вчиненні кримінального правопорушення, передбаченого ч. 4 ст. 354 КК України [22].

У цьому провадженні суд визнав недопустимими результати негласних слідчих (розшукових) дій, а також похідні від них докази, зокрема висновки експертів, протокол освідування особи, протокол огляду місця події та протокол огляду предметів із записом розмови на DVD-R диску. Суд обґрунтував це тим, що такі докази були здобуті або використані внаслідок істотного порушення процесуального порядку, а тому підпадають під дію доктрини «плодів отруєного дерева».

Унаслідок виключення недопустимих доказів суд дійшов висновку, що досліджена доказова сукупність, оцінена з погляду належності, допустимості та взаємозв’язку, не підтверджує наявності в діянні обвинуваченого складу кримінального правопорушення. На цій підставі особу було визнано невинуватою та виправдано за ч. 4 ст. 354 КК України у зв’язку з недоведеністю наявності в її діянні складу кримінального правопорушення.

Отже, недостатність доказів у судовому провадженні може бути наслідком не лише об’єктивної відсутності доказової інформації, а й втрати окремих фактичних даних процесуального значення через визнання їх недопустимими.

За таких умов решту доказів має оцінювати судом у сукупності; якщо вона не забезпечує доведення обставин, передбачених ст. 91 КПК України, обвинувальний вирок не може бути ухвалено. Це узгоджується з положеннями ст. 373 КПК України, згідно з якою виправдувальний вирок ухвалюють, зокрема,

якщо не доведено, що кримінальне правопорушення вчинене обвинуваченим або що в його діянні є склад кримінального правопорушення.

У доктрині кримінального процесу України усталеним є розуміння *достовірності* доказу як його процесуальної властивості, що відображає відповідність змісту доказу обставинам об'єктивної дійсності й визначає придатність цього доказу для встановлення фактів, які підлягають доказуванню в кримінальному провадженні [66, с. 133; 75, с. 190].

У такому значенні достовірність становить категорію, що з'єднує дві площини: онтологічну – реальну наявність або відсутність обставини в дійсності, гносеологічну – точність процесуального відображення цієї обставини в матеріалах справи.

Саме друга, гносеологічна площина є тим, на що спрямована процесуальна перевірка доказу, оскільки об'єктивне існування обставин не залежить від процесуальної діяльності, натомість їх відображення в доказах залежить цілком.

Достовірність електронного доказу верифікується шляхом його комплексного співвіднесення з усім масивом доказових даних, як уже зібраних на момент оцінки, так і тих, що можуть бути отримані в подальшому перебігу провадження за допомогою передбачених КПК України процесуальних дій – допиту свідків, призначення відповідної експертизи, проведення огляду або обшуку.

На наше переконання, специфіка електронного об'єкта в цьому контексті полягає в його подвійній ролі, оскільки він не лише підлягає перевірці іншими доказами, а й слугує засобом перевірки достовірності інших доказів. Прикладом цього можуть бути метадані електронного об'єкта, що підтверджують або спростовують показання свідків стосовно часу, місця або обставин описуваних подій.

Достовірність як критерій оцінки доказу посідає особливе місце в системі властивостей доказу, оскільки саме від результатів її перевірки залежить можливість покладення відповідних фактичних даних в основу процесуального рішення. На наше переконання, специфіка цього критерію полягає в тому, що він

стосується не обставин певної події, які існують незалежно від процесу пізнання, а тих знань про ці обставини, які формуються в суб'єкта доказування внаслідок процесуальної діяльності.

Недостовірним може виявитися процесуально зафіксоване відображення обставини, натомість обставина залишається такою, що була або якої не було в реальності. У контексті електронних доказів зазначене методологічне розмежування набуває додаткового значення, оскільки технологічна природа цифрового відображення створює специфічні ризики його розходження з первинною обставиною – від помилок фіксації до прямих маніпуляцій із цифровим об'єктом.

У загальнотеоретичному аспекті зазначену позицію підтверджено і в колективній монографії за редакцією В. П. Пєткова, де достовірність доказів визначають як властивість, що означає безсумнівність їхньої істинності, акцентуючи на відносній самостійності цієї властивості стосовно належності й допустимості доказів [56, с. 84].

Отже, попри різні підходи до формулювання, у науковій літературі простежується усталена концепція, яка полягає в тому, що перевірка доказів охоплює як встановлення надійності їх процесуального джерела, так і з'ясування відповідності змісту зафіксованих відомостей дійсності.

Достовірність електронного доказу має двовимірний характер, одночасно охоплюючи як надійність джерела доказової інформації, так і відповідність зафіксованих у ньому відомостей дійсності.

С. Мейсон зауважує, що автентичність електронного джерела й істинність його змісту є принципово різними питаннями, які потребують окремої верифікації. Встановлення справжності джерела не є підставою для автоматичного визнання достовірності відомостей, що в ньому містяться [215].

Достовірність цифрового доказу невіддільна від його здатності відображати об'єктивну реальність. К. Харгрівз, Г. ван Бік та Е. Кейсі зазначають, що оцінка якості й надійності електронного доказу передбачає системний аналіз результатів

дослідження, і коли зміст одного джерела доказів суперечить іншому, лише одне з них може відповідати реальним обставинам події [198].

Для електронних доказів проблема достовірності набуває особливої гостроти, зумовленої їхньою технічною природою. На відміну від паперового документа, модифікація якого залишає фізичні сліди (виправлення, підчистки, дописки), електронна інформація може бути змінена без будь-яких видимих ознак втручання. Це означає, що традиційні методи перевірки достовірності – візуальний огляд, порівняння з іншими примірниками – є недостатніми для електронних доказів.

Ключовими інструментами верифікації достовірності електронного доказу є:

– хешування (обчислення контрольної суми файлу на момент його вилучення, що дає змогу виявити будь-яку подальшу модифікацію);

– аналіз метаданих (зіставлення дати створення, модифікації та доступу з хронологією подій у кримінальному провадженні);

– експертне дослідження (висновок спеціаліста з цифрової криміналістики щодо цілісності й автентичності електронного об’єкта).

За відсутності хешування на момент вилучення електронного доказу його достовірність може бути поставлена під обґрунтований сумнів стороною захисту, що створює ризик визнання доказу недостовірним навіть за умови його формальної допустимості.

Між властивостями належності, допустимості та достовірності є різні види зв’язку. Належність і достовірність є порівняно автономними категоріями: належний доказ може бути як достовірним, так і сумнівним; достовірний доказ – як належним, так і не належним.

Натомість допустимість і достовірність знаходяться в тісному зв’язку, оскільки окремі вимоги допустимості спрямовані саме на забезпечення достовірності доказової інформації. У таких випадках доказ визнають недопустимим саме внаслідок невідновних сумнівів у його достовірності. Водночас зазначений зв’язок не виключає необхідності розмежування цих властивостей:

допустимість оцінюють за формальними ознаками, прямо передбаченими законом, натомість достовірність підлягає змістовній оцінці [6].

Якщо сумніви в достовірності зумовлені прямим порушенням процесуального закону, доказ є недопустимим; якщо ж такі сумніви виникли з інших причин, зокрема внаслідок неякісно проведеного експертного дослідження, доказ визнають недостовірним.

Зазначений зв'язок між критеріями оцінки доказів набуває особливого значення стосовно електронної форми доказування. З огляду на п. 21, 22 Керівництва Комітету міністрів Ради Європи «Електронні докази в цивільному та адміністративному процесі» від 30 січня 2019 року [192], достовірність електронних доказів презюмується доти, доки не виникне обґрунтованих сумнівів у протилежному; суд має право вимагати експертного дослідження доказу, якщо порушуються складні питання його автентичності або є підозри щодо маніпулювання ним.

На нашу думку, ця презумпція має дві принципові особливості, порівняно з традиційними доказами. Перша полягає в тому, що її спростування у випадку електронного доказу вимагає не загальної логічної аргументації, а спеціальних технологічних засобів верифікації.

До таких засобів П. С. Матвєєв обґрунтовано відносить: кваліфікований електронний підпис, який забезпечує ідентифікацію автора і гарантує цілісність даних; хеш-функції, що створюють унікальний «відбиток» документа і дають змогу виявити будь-яке його подальше спотворення; аналіз метаданих, які слугують «цифровим відбитком» доказу – містять відомості про автора, час створення, модифікації та доступу [79, с. 237–238].

Інша ж особливість полягає в тому, що оцінка достовірності електронного доказу одним суб'єктом доказування не є остаточною для інших.

У постанові Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к [107] сформульовано висновок, що всі ідентичні за змістом примірники електронного документа можна розглядати як оригінали, а питання

ідентифікації документа як оригіналу вирішують через перевірку контрольної суми файлу або за допомогою спеціального дослідження.

Отже, висновок слідчого, який ґрунтується на висновку спеціаліста про цілісність хеш-суми, не позбавляє суд можливості дійти протилежного висновку за результатами призначеної повторної експертизи.

Викладене дає підстави стверджувати, що достовірність електронного доказу – це не статична властивість, фіксована в момент його вилучення, а динамічна характеристика, яка верифікується на кожному наступному етапі кримінального провадження і безпосередньо залежить від процедури поводження з електронним об'єктом – від моменту його виявлення до дослідження в суді.

Така процедура в міжнародній доктрині дістала назву ланцюга забезпечення зберігання доказів (chain of custody), і формалізованих вимог до неї в чинному КПК України немає.

Верифікацію достовірності електронного документа в системі доказів кримінального провадження здійснюють не ізольовано, а через його співвіднесення з масивом інших доказових даних, які або підтверджують походження та зміст електронного об'єкта, або ставлять їх під сумнів.

Така перехресна перевірка може бути реалізована як стороною обвинувачення через комплекс слідчих (розшукових) дій, передбачених КПК України (допит свідків, призначення комп'ютерно-технічної експертизи, тимчасовий доступ до речей і документів, обшук, огляд електронних інформаційних систем).

Сторона захисту також може вчиняти заходи щодо перевірки, зокрема через подання альтернативних доказів і клопотання про проведення процесуальних дій.

У науковій літературі виокремлюють такі послідовні етапи встановлення достовірності фактичних даних: на першому з'ясовують надійність джерела; на другому – оцінюють коректність методу, за допомогою якого ці дані було отримано; на третьому – здійснюють зіставлення з іншими матеріалами кримінального провадження [55, с. 59].

Перевірку електронного документа на предмет достовірності здійснюють шляхом його зіставлення з доказами, зібраними в межах кримінального провадження.

Французькі науковці L.-A. Beaulieu, M. Bérubé, та інші зауважують, що достовірність цифрового сліду як доказового джерела не може бути встановлена відокремлено – її визначають через співвіднесення із сукупністю доказів, що стосуються фактичних даних [155].

Слід акцентувати на перевірці окремих видів електронних доказів, зокрема електронного документа й електронного відеозапису.

Перевірка достовірності електронного документа як джерела доказу має багатоаспектний характер й охоплює щонайменше три напрями: дослідження технічної справності пристрою або носія, на якому міститься інформація; встановлення відомостей про джерело походження електронного об'єкта (наприклад, власника вебсайту чи облікового запису в соціальній мережі); ідентифікацію часово-просторових обставин (метаданих) створення електронного запису.

На нашу думку, відеозапис як вид електронного доказу не можна досліджувати ізольовано від технічних параметрів пристрою, що його зафіксував, оскільки саме від характеристик обладнання залежить можливість встановлення часу, місця та змісту події, відображеної в записі.

У правозастосовній практиці типовим є випадок, коли на відеозаписі з камер зовнішнього або внутрішнього спостереження, нагрудних камер працівників поліції чи відеореєстраторів неправильно зазначено дату і час або таких відомостей взагалі немає.

Можливі три причини виникнення таких неточностей: технічна несправність пристрою; неправильні налаштування часу користувачем; автоматичний перехід пристрою між літнім і зимовим часом без своєчасного оновлення параметрів. Юридичні наслідки кожної з цих ситуацій принципово різні, оскільки за наявності документально підтвердженої технічної несправності пристрою відомості, отримані з нього, втрачають доказове значення, натомість збій у налаштуваннях

часу, не пов’язаний з апаратною несправністю, не свідчить автоматично про недостовірність запису, а потребує верифікації іншими доказами.

Засобами такої верифікації можуть бути показання свідків (очевидців події) або власників технічних пристроїв; зіставлення з відеозаписом, зробленим у тому самому часовому інтервалі іншим пристроєм; інші електронні докази, що фіксують одночасні дії (банківські транзакції через термінал, телефонний дзвінок, повідомлення в месенджері); технічна документація щодо налаштувань і обслуговування пристрою.

Запропонована ідея відповідає логіці, яку послідовно обстоює ККС ВС у практиці 2024 року: електронні дані, отримані в передбачений КПК спосіб, приймають як автентичний доказ доти, доки інша сторона не наведе обґрунтованих доводів на спростування цього [105].

Водночас обов’язковість фіксації параметрів пристрою-першоджерела на момент створення запису випливає з потреби забезпечити можливість експертної верифікації, про що неодноразово зазначали в касаційній практиці [104].

Ключове значення для оцінки достовірності електронного об’єкта має не власне факт призначення експертизи, а можливість стороною захисту самостійно перевірити запис на ознаки редагування або монтажу, для чого матеріали мають бути своєчасно відкриті в порядку ст. 290 КПК України; саме нездатність сторони обвинувачення забезпечити таку перевірку в низці справ ставала підставою для визнання відповідних доказів недопустимими [128].

У контексті відеозаписів з камер спостереження це означає, що технічна верифікація первинних параметрів пристрою (часові мітки, налаштування, технічний стан) має бути зафіксована вже на стадії огляду або вилучення, а не залишена на пізніший етап судового розгляду.

Окремою складовою оцінки достовірності є аналіз методу отримання електронних даних: характеристик програмного забезпечення (комп’ютерних програм, браузерів, додатків), використаного під час огляду чи копіювання електронного об’єкта, а в разі дослідження висновку експерта – особливостей застосованої методики.

На нашу думку, метадані файлу (відомості про автора, дату створення, модифікації та доступу) є своєрідними «мовчазними свідками» електронних доказів, які дають змогу об’єктивно встановити обставини його походження.

Також ми вважаємо, що перевірку достовірності окремого електронного доказу слід здійснювати не тільки шляхом зіставлення з усім масивом матеріалів провадження, а й у межах тієї сукупності фактичних даних, що стосуються одного й того самого факту або обставини, що його підтверджує.

Слушно зазначає Д. Б. Сергєєва, що, попри те що тягар доказування переважно покладають на сторону обвинувачення, оцінка доказів є невіддільним елементом доказування і для сторони захисту та потерпілого. Тому захисник, як і слідчий, дізнавач та прокурор, має попередньо оцінювати кожен поданий до суду доказ за критеріями належності, допустимості й достовірності [118, с. 107].

2.3. Електронне листування в месенджерах як вид електронних доказів

Попри загальний характер правового регулювання електронних доказів у кримінальному процесуальному законодавстві України, практика доказування демонструє, що різні види електронних доказів мають специфічні особливості щодо їхнього збирання, фіксації, дослідження та оцінки.

Зазначена обставина зумовлює необхідність окремої характеристики тих різновидів електронних доказів, які найпоширеніші в сучасній судовій практиці та ставлять перед правозастосуванням якісно нові проблеми, що не вирішують загальними правилами доказування.

Цим двом критеріям відповідає листування в месенджерах як найпоширеніший вид електронних доказів, що фігурує в кримінальних провадженнях різних категорій.

Слід зауважити, що використання інтернету як способу комунікації та джерела інформації остаточно посідає панівне місце серед інших форм спілкування та форм отримання новин, таких як газети, телебачення та радіо.

Дані вебпорталу «Statista» засвідчують, що близько 5,32 млрд людей сьогодні дивляться телебачення, однак кількість користувачів інтернету за даними вебпорталу «Datareportal» більше ніж на пів мільярда чисельніша й становить близько 6 млрд [178; 219].

Цікавим є факт посилення пов'язаності людського життя з електронними комунікаційними смартпристроями (мобільні телефони, годинники тощо). Такі пристрої збирають і зберігають не тільки ті дані, які були введені користувачем або щодо яких було надано згоду на таке збирання, а й дані, які збирає пристрій згідно з налаштуваннями виробника та на підставі функціональних можливостей.

Наприклад, увімкнені Wi-Fi мережі й мобільні пристрої під час роботи обмінюються пакетами даних між собою без окремої згоди користувачів таких пристроїв і створюються відповідні Wi-Fi сліди [144].

Одним із показових є дослідження, яке довело, що навіть в разі ввімкнення режиму «Airplane mode» такі пристрої продовжують збирати відомості про ввімкнені Wi-Fi мережі поруч, надалі обмінюються пакетами даних і зберігають відомості про комунікацію з такими мережами [144].

Отже, сучасні електронні пристрої «комунікують» між собою та залишають електронні сліди. Це свідчить про нову еру електронного спілкування, оскільки, крім невпинного переходу до електронного спілкування, пристрої здатні обмінюватися інформацією між собою без втручання людини як користувача такого пристрою.

Стрімке поширення мобільних застосунків для обміну повідомленнями суттєво трансформувало характер суспільної комунікації, перемістивши значну частину міжособистісної взаємодії в цифровий простір. За даними світових досліджень, станом на 2025 рік частка користувачів мережі Інтернет, які щомісячно послуговуються месенджерами, перевищує 94 %, а найпоширенішими платформами залишаються WhatsApp, Telegram, WeChat та Messenger. В умовах воєнного стану в Україні месенджери фактично перетворилися на основний, а подекуди і єдиний засіб комунікації між громадянами, правоохоронними органами та військовими підрозділами. Унаслідок цього листування в месенджерах дедалі

частіше постає як джерело інформації про подію кримінального правопорушення, обставини його планування, вчинення та коло причетних осіб.

Як окремий вид електронного доказу листування в месенджерах має низку специфічних ознак: створення та зміна за допомогою комп'ютерних пристроїв; зберігання на різних носіях і серверах провайдерів; можливість багаторазового відтворення без втрати якості; підвищена вразливість до модифікації та знищення. Саме ці ознаки зумовлюють потребу в окремих підходах до його збирання, фіксації та оцінки.

Кримінальний процесуальний кодекс України не містить визначення електронного доказу, немає спеціальних норм щодо порядку збирання та оцінки листування в месенджерах як самостійного виду електронного доказу. Відсутність єдиного нормативного підходу породжує неоднорідність судової практики, що негативно позначається на якості доказування та дотриманні гарантій справедливого судового розгляду, закріплених у ст. 6 Конвенції про захист прав людини і основоположних свобод [70].

Різноманітність програмного забезпечення для обміну повідомленнями, яке розрізняють за функціональними властивостями й технічною архітектурою, зумовлює необхідність систематизації видів листування в месенджерах. Така систематизація має не лише теоретичне, а й практичне значення, оскільки від конкретного виду листування залежать процесуальний порядок його збирання, методи фіксації та критерії оцінки допустимості. На підставі здійсненого аналізу запропоновано класифікацію листування в месенджерах як електронного доказу за вісьмома критеріями (табл. 2.1), її основні положення оприлюднено в публікації [207].

Таблиця 2.1

Класифікація листування в месенджерах як електронного доказу

Критерій класифікації	Вид	Характеристика
За кількістю учасників	Моночат (канал)	За участю однієї особи
	Діалог	За участю двох учасників
	Груповий чат	Три і більше учасників
За доступом осіб	Приватне	Доступне за запрошенням або закрите
	Публічне	Доступне необмеженому колу осіб
За можливістю розміщення	Канали	Розміщують лише особи, наділені правами
	Бесіди	Розміщення доступне всім учасникам
За етапом створення	Оригінал	Зберігається на первинному пристрої
	Електронна копія	Формат фото, відео, PDF, TXT, HTML
	Паперова копія	Роздруківка скриншотів
За джерелом походження	З пристрою учасника	Смартфон, комп’ютер, планшет
	Від провайдера послуг	Через механізм запитів
	Від третіх осіб	Особи, обізнані про листування
За форматом передачі інформації	Текстове	SMS, месенджери, чати
	Мультимедійне	Фото, відео, аудіо, документи
За видом інформації	Зміст листування	Текст, файли
	Системна інформація	Метадані: геолокація, дата, час, IP-адреса
За способом відповідей	Чат-боти	Автоматичні відповіді
	Штучний інтелект	ШІ для ведення спілкування
	Живе спілкування	За участю фізичних осіб

Джерело: розроблено автором.

Запропонована класифікація охоплює ключові параметри, що впливають на процесуальну оцінку листування в месенджерах як електронного доказу, створює методологічне підґрунтя для подальшого дослідження порядку збирання, фіксації та оцінки окремих видів такого листування в кримінальному провадженні.

Вона розвиває підхід А. В. Коваленка [65] до класифікації електронних (цифрових) слідів кримінального правопорушення: якщо зазначений автор зосередився на технічних характеристиках цифрових слідів загалом, то запропонована класифікація орієнтована на процесуальне значення різних видів листування, що має безпосередню практичну цінність для оцінки їх допустимості.

Аналіз судових рішень у кримінальних провадженнях, наявних у Єдиному державному реєстрі судових рішень, засвідчує, що суди здебільшого визнають листування в месенджерах допустимим електронним доказом. Водночас підходи різних судів до оцінки такого виду доказів суттєво різняться, що засвідчує несформованість усталеної практики й необхідність її уніфікації.

Емпіричну базу аналізу практики становили 12 судових рішень судів різних інстанцій, ухвалених протягом 2022–2026 років, у яких предметом оцінки було листування в месенджерах як доказ у кримінальному провадженні. Обраний період зумовлений тим, що саме в умовах воєнного стану суттєво збільшилася кількість проваджень, де електронне листування використовували як ключовий доказ. Рішення відібрано з різних регіонів України для забезпечення репрезентативності вибірки; пошук здійснювали в ЄДРСР за ключовими словами «месенджер», «електронне листування», «листування в месенджері».

Принципове значення має правова позиція Верховного Суду, сформульована в постанові від 12 червня 2024 року у справі № 569/1908/23 [96], згідно з якою електронні (цифрові) докази, зокрема матеріали з приватних месенджерів і телеграм-каналів, зібрані оперативними підрозділами з дотриманням вимог процесуального законодавства, є основними доказами в кримінальних провадженнях щодо злочинів проти основ національної безпеки. Зазначений

висновок Верховного Суду є принципово важливим, оскільки він одним із перших чітко визначив статус електронних повідомлень з месенджерів як основних, а не лише допоміжних доказів у цій категорії кримінальних проваджень.

Продовженням цієї практики є постанова ККС ВС від 31 березня 2026 року у справі № 175/10123/23 [102]. У кримінальному провадженні щодо державної зради встановлено, що обвинувачений передав представнику збройного формування держави-агресора інформацію про місцезнаходження військовослужбовців Збройних Сил України шляхом запису й відправлення двох відеоповідомлень у месенджері Telegram. Того самого дня було здійснено ракетний удар по зазначеному об’єкту.

Електронні повідомлення з месенджера стали ключовими доказами в провадженні. Ця справа підтверджує тезу про те, що в умовах воєнного стану електронне листування в месенджерах трансформувалося з допоміжного у визначальне джерело доказової інформації в провадженнях щодо злочинів проти основ національної безпеки, а належне процесуальне забезпечення його збирання та фіксації набуває критичного значення для ефективності кримінального переслідування.

Згідно з вироками, які розміщені в ЄДРСР, ця правова позиція була застосована в низці кримінальних проваджень (№ 334/2045/24 [14], № 334/4126/24 [15], № 334/5278/24 [16], № 334/9999/23 [17]), у яких суди визнали листування в месенджерах допустимим доказом за сукупності двох умов: дотримання вимог закону щодо порядку збирання доказів і форми фіксування (шляхом складання протоколів огляду з додатками у вигляді скриншотів або файлів), а також неспроможності сторони захисту спростувати такі докази.

Аналогічний підхід обстоював Хортицький районний суд м. Запоріжжя у вироку від 6 січня 2025 року у справі № 337/862/23 [40], у якому суд оцінив листування в месенджері як належний, допустимий і достовірний доказ, що в сукупності з іншими доказами доводить обставини кримінального правопорушення поза розумним сумнівом.

Водночас непоодинокими є випадки відхилення судами листування в месенджерах з підстав, передбачених ст. 86, 87 КПК України. Роздільнянський районний суд Одеської області у вироку від 29 лютого 2024 року у справі № 511/563/19 [30] дійшов висновку про недопустимість усіх доказів, отриманих під час досудового розслідування, оскільки розслідування було проведено без належної постанови про доручення. Жовківський районний суд Львівської області у вироку від 8 березня 2024 року у справі № 461/3477/22 [20] зазначив, що посилання на протокол огляду мобільних телефонів є процесуально некоректним, оскільки не було надано експертних висновків про те, що листування через месенджери вів обвинувачений.

Також в ухвалі Апеляційної палати Вищого антикорупційного суду від 1 лютого 2022 року у справі № 991/492/19 [133] суд визнав недопустимими докази, зібрані слідчими ТУ ДБР, на підставі того, що їх отримали неуповноважені особи з порушенням встановленого законом порядку. Велика Палата Верховного Суду в постанові від 21 червня 2023 року у справі № 916/3027/21 [95] дійшла висновку, що повідомлення, відправлені через застосунки-месенджери, є електронним доказом, який оцінює суд за внутрішнім переконанням у сукупності з іншими доказами, причому суд може розглядати електронне листування як доказ лише тоді, коли воно надає можливість встановити авторів і зміст листування.

Ще одним прикладом проблемності оцінки електронного листування є вирок Турківського районного суду Львівської області від 18 липня 2024 року у справі № 458/465/22 [34], у якому суд відхилив доказ обвинувачення, зазначивши, що інформація в скриншотах не дає змоги беззаперечно встановити застосунок, авторів, час листування та зв’язок змісту з подією. Суд дійшов висновку, що таке електронне листування не є ні письмовим, ні електронним доказом на підтвердження вчинення злочину. Зазначене рішення є яскравою ілюстрацією ситуації, коли відсутність чітких нормативних критеріїв оцінки електронних доказів призводить до їх повного відхилення судом.

Узагальнення проаналізованих судових рішень дає змогу виокремити основні підстави визнання листування в месенджерах недопустимим доказом,

якими є порушення процесуального порядку збирання доказів, зокрема відсутність належної постанови або проведення слідчих дій неуповноваженими суб'єктами; відсутність підтвердження авторства повідомлень, тобто неможливість однозначно встановити, що саме обвинувачений є автором конкретних повідомлень; ненадання експертних висновків щодо автентичності та цілісності електронних даних; подання доказів у формі, яка не дозволяє встановити їх походження та зв'язок з подією кримінального правопорушення.

Натомість визнання листування допустимим доказом корелює з дотриманням процесуального порядку фіксування, наявністю протоколів огляду з додатками, а також з відсутністю обґрунтованих заперечень сторони захисту.

Аналіз судової практики в кримінальних провадженнях, де листування в месенджерах використовували як електронний доказ, виявив й іншу дотичну проблему, а саме неуніфіковане відтворення англомовних назв програмних продуктів, що, на нашу думку, впливає на правозастосування.

У текстах судових рішень найменування тих самих месенджерів подають по-різному – то мовою оригіналу (Telegram, WhatsApp, Viber), то в транслітерованій формі («Телеграм», «Вотсап»).

Така непослідовність ускладнює однозначну ідентифікацію застосунку, пошук релевантних рішень у Єдиному державному реєстрі судових рішень й однакове сприйняття змісту доказу учасниками провадження.

Процесуальні проблеми використання англомовних назв програмних продуктів і підходи до їх уніфікування в кримінальному провадженні запропоновано в окремій публікації [90].

Специфіку роботи з листуванням у месенджерах відображають і результати проведеного автором анкетування. Найпоширенішими способами його фіксації респонденти назвали протокол огляду мобільного пристрою із фотофіксацією екрана (79,2 %) і скриншоти (59,2 %); комп'ютерно-технічну експертизу застосовують 40,0 %, експорт файлів листування – лише 15,4 %. (додаток В, рис. 10).

Найсерйознішими проблемами використання такого листування як доказу опитані вважають ідентифікацію особи, яка фактично надсилала повідомлення (73,8 %), функції «зникаючих» повідомлень (59,2 %), наскрізне шифрування (42,3 %), відмову провайдерів передавати дані (26,2 %), відсутність метаданих у скриншотах (24,6 %) і можливість підробки скриншотів (23,1 %). (додаток В, рис. 11).

Водночас 57,7 % респондентів не мали справ із запереченням автентичності листування, 30,0 % зазначили, що такі заперечення були, але суд переважно визнавав докази допустимими, а 10,8 % – що це вплинуло на оцінку доказу судом. Отримані результати засвідчують необхідність чітких процесуальних вимог до фіксації листування та забезпечення його автентичності (додаток В, рис. 12).

Водночас на практиці переважає підхід, за яким листування в месенджерах оцінюють «у сукупності з іншими доказами», що не гарантує належної перевірки автентичності повідомлень, оскільки за відсутності нормативних вимог до автентифікації суд фактично покладається на пасивність сторони захисту, а не на об’єктивну верифікацію походження та цілісності даних.

Прикметно, що результат оцінки нерідко залежить не стільки від об’єктивної якості доказу, скільки від процесуальної активності захисту, оскільки в провадженнях, де захист не заявляв клопотань про експертизу чи про визнання доказів недопустимими, суди здебільшого визнавали листування допустимим; натомість активне оспорювання авторства й автентичності могло мати результатом отримання судового висновку про недопустимість.

Для максимально повного дослідження національної практики доцільним є аналіз закордонного досвіду.

У правовій системі Сполучених Штатів Америки допустимість електронних доказів, зокрема повідомлення месенджерів і текстові повідомлення, регулюють Федеральні правила доказування (Federal Rules of Evidence, FRE) [187]. На відміну від українського законодавства, FRE містять чіткі правила автентифікації, що застосовують до всіх видів електронних доказів. Відповідно до Rule (правила) 901(a), сторона, яка подає доказ, повинна надати достатні підстави для висновку

про те, що цей доказ є тим, чим його подавач стверджує. Правило 901(b) передбачає десять невичерпних прикладів методів автентифікації, серед яких свідчення обізнаної особи (правило 901(b)(1)), характерні ознаки змісту й інші відмітні характеристики (правило 901(b)(4)), що охоплюють метадані.

У практиці судів штатів США розвинуто підхід автентифікації текстових повідомлень через «confirming circumstances» (підтверджувальні обставини), що охоплюють реєстрацію мобільного пристрою на ім'я відповідача, захист паролем, використання характерних прізвиськ і змісту, який відповідає обставинам справи. Суди послідовно підтверджують, що факт зазначення імені відправника в повідомленні є недостатнім для автентифікації, то необхідними є додаткові підтверджувальні обставини, що співзвучні з підходом українських судів.

Водночас суттєвою відмінністю американської системи від української є передбачена FRE можливість самоавтентифікації електронних записів відповідно до Правила 902(13)–(14), доданих 2017 року, які дають змогу визнавати електронні записи автентичними без додаткових свідчень за умови наявності сертифікації кваліфікованого спеціаліста. Такої можливості не передбачено в українському процесуальному законодавстві, що ускладнює процедуру доказування та збільшує навантаження на сторону обвинувачення.

Зазначені практики федеральних судів США підтверджують дослідження M. Novak [218], який констатував збільшення кількості справ, у яких цифрові докази відіграють ключову роль, і виокремив актуальні питання їх допустимості й автентифікації.

Принципове значення для практики допустимості перехоплених повідомлень зашифрованих месенджерів має рішення Суду Європейського Союзу від 30 квітня 2024 року у справі C-670/22 (EncroChat) [205], у якому Суд ЄС установив, що European Investigation Order (EIO) для отримання доказів, які вже знаходяться в розпорядженні виконавця – держави-члена, може бути виданий лише компетентним органом відповідно до національного законодавства держави, що видає наказ.

Справа EncroChat стосувалася масового перехоплення повідомлень зашифрованого месенджера, який використовували організовані злочинні групи: французькі та нідерландські правоохоронні органи 2020 року встановили шкідливе програмне забезпечення на сервери EncroChat, отримавши доступ до мільйонів повідомлень, які згодом були передані правоохоронним органам інших держав – членів ЄС через механізм ЕІО.

Аналіз наднаціонального рівня регулювання ЄС засвідчує принципово інший підхід до проблеми електронних доказів, порівняно з національними моделями. Якщо Франція та Німеччина зосереджені на питаннях допустимості й оцінки доказів, то Регламент (ЄС) 2023/1543 розв'язує попередню проблему – фізичний доступ до даних, які знаходяться на серверах в іншій юрисдикції.

Справа EncroChat (C-670/22) виявила проблему між ефективністю транскордонного збирання доказів і процесуальною гарантією. Масове перехоплення повідомлень зашифрованого месенджера забезпечило докази проти тисяч підозрюваних, проте поставило питання про відповідність такого перехоплення принципу пропорційності та праву на приватність.

Рішення Суду ЄС, яке встановило вимогу дотримання національних процесуальних стандартів під час видачі European Investigation Order, фактично засвідчило, що наднаціональні механізми доступу не можуть підміняти національні гарантії допустимості. Для України цей висновок є принципово важливим, оскільки імплементація транскордонних механізмів доступу має супроводжуватися одночасним закріпленням у КПК чітких стандартів допустимості отриманих у такий спосіб доказів.

У Сполучених Штатах Америки 2018 року ухвалили Clarifying Lawful Overseas Use of Data Act (CLOUD Act) [171], який дозволяє правоохоронним органам США витребувати дані від американських технологічних компаній незалежно від місця зберігання даних.

Цей нормативний інструмент, як і Регламент (EU) 2023/1543, паралельно відходить від принципу, за яким юрисдикцію визначають фізичним місцем

зберігання даних, що відображає глобальну тенденцію до спрощення транскордонного доступу до електронних доказів.

Для України зазначена тенденція має особливе значення, оскільки сервери провайдерів більшості популярних месенджерів (Telegram, WhatsApp, Signal) знаходяться за кордоном, що суттєво ускладнює процедуру отримання електронних доказів через механізм міжнародної правової допомоги. Наразі українське законодавство не передбачає механізму прямого звернення до іноземних провайдерів послуг, що зумовлює необхідність інтеграції відповідних норм.

Верховний Суд Канади у справі R. v. Mills [227] дійшов висновку, що електронне листування є допустимим доказом, а копія такого листування, відображена на скриншоті, також є допустимою за умови підтвердження її автентичності. Канадський підхід характеризується прагматизмом, оскільки суд оцінює насамперед надійність і достовірність доказу, а не формальну відповідність процедурним вимогам, що відрізняється від формалізованого підходу як в Україні, так і в США. У Великій Британії допустимість цифрових доказів регулюють переважно через правила виключення, закріплені в Police and Criminal Evidence Act 1984 (PACE) [222]. Британські суди застосовують гнучкий підхід, оцінюючи три аспекти потенційного доказу: релевантність, надійність і справедливість його використання.

Порівняльний аналіз законодавства та практики чотирьох юрисдикцій дає підстави виокремити три основні підходи до регулювання електронних доказів з месенджерів: формалізований підхід (США), за якого автентифікацію здійснюють відповідно до кодифікованих правил із чіткими критеріями допустимості; прагматичний підхід (Велика Британія, Канада), за якого суд оцінює доказ за його сутністю та надійністю, а не за формальними ознаками; комбінований підхід ЄС, який поєднує нормативне регулювання на наднаціональному рівні (Регламент 2023/1543) із дискрецією національних судів щодо оцінки допустимості. Україна нині тяжіє до прагматичного підходу, проте без належного нормативного підґрунтя, що створює невизначеність і нерівність у застосуванні права.

З огляду на обґрунтовану в підрозділі 1.1 пропозицію щодо закріплення поняття електронного доказу, доцільно також передбачити в главі 15 КПК України окрему статтю щодо порядку тимчасового доступу до електронних повідомлень, а також внести зміни до ст. 86, 87 КПК України, щоб встановити окремі вимоги до порядку збирання та фіксації електронних доказів, зокрема обов'язковість фіксації метаданих (дати, часу, IP-адреси, ідентифікаторів пристроїв й акаунтів).

2.4. Об'єкти, створені штучним інтелектом: проблеми оцінки в доказуванні

Поява генеративних моделей ШІ, здатних створювати текст, зображення, аудіо- й відеоматеріали, які складно відрізнити від реальних, ставить перед правоохоронними та судовими системами нові виклики. За результатами дослідження P. Korshunov та S. Marcel [210], проведеного на основі 120 відеозаписів із платформи Facebook (60 з яких були реальними, а 60 – згенерованими за допомогою технологій штучного інтелекту), встановлено, що в 75,5 % випадків глядачі помилково ідентифікували високоякісні дипфейки як реальні відео. Отже, у переважній більшості випадків глядач, переглядаючи штучно згенероване відео, сприймає його як автентичне.

Високий рівень занепокоєння практиків щодо викликів штучного інтелекту та браку належного інструментарію протидії засвідчили й результати проведеного автором анкетування. Хоча безпосередньо з доказами, згенерованими ШІ, працювали лише 4,6 % респондентів, переважна більшість (77,7 %) сприймає це як актуальну загрозу. (додаток В, рис. 17).

З аудіо-, відео- чи фотоматеріалами, автентичність яких ставили під сумнів через можливе застосування технологій ШІ (дипфейк), працювали 6,9 % респондентів, ще 16,9 % чули про такі випадки від колег. Інструменти ШІ для оцінки електронних доказів регулярно використовують лише 4,6 % опитаних, натомість 48,5 % вважають їх упровадження перспективним. (додаток В, рис. 18).

Щодо тягаря доказування автентичності цифрових аудіо- й відеоматеріалів 63,1 % респондентів констатували, що нині його де-факто покладено на сторону, яка подає доказ, а 16,9 % схвалили запровадження механізму його перерозподілу за наявності обґрунтованого сумніву (додаток В, рис. 20). Ці дані емпірично обґрунтовують авторську пропозицію щодо доповнення КПК України статтею 99-3, про що йшлося в попередній публікації [88].

Невпинна й агресивна імплементація злочинним світом ШІ у свій арсенал знарядь створює низку невідкладних питань, які потребують наукового дослідження та правового врегулювання. У КК України немає норм, що передбачали б відповідальність за створення та поширення об'єктів, створених за допомогою ШІ, з використанням голосу, зовнішності осіб без їхньої згоди. Крім того, у кримінальному процесуальному законодавстві немає норм, які регулюють порядок оцінки судами доказів, створених або модифікованих за допомогою ШІ, що є простором для наукових досліджень у цьому напрямі.

Проблематику автентичності електронних доказів, створених або змінених засобами штучного інтелекту, зокрема технічні засоби її забезпечення (хешування, цифровий підпис), розглянуто також у попередній публікації [136].

Матеріали, згенеровані ШІ, як електронні докази мають певні особливості, не властиві іншим електронним доказам, оскільки є результатом складних програмних систем, процеси роботи яких інколи не можуть пояснити навіть розробники; мають унікальну здатність переконувати глядача в реальності відображеного матеріалу та формувати погляди й сприйняття тих, хто їх переглядає.

Використання ШІ зі злочинною метою становить підвищений рівень суспільної небезпеки, оскільки таке використання здатне створювати віртуальну реальність для сторонніх осіб.

Крім того, ШІ стає джерелом висновків, які учасники кримінального провадження намагаються використати для обґрунтування своєї позиції та доведення обставин справи, що зумовлює питання про особливості дослідження

матеріалів, створених за допомогою штучного інтелекту, зокрема дипфейк-контенту, безпосередньо як доказів у кримінальному провадженні.

Принципове значення для окреслення позиції судової влади стосовно допустимості електронних матеріалів, які були створені або модифіковані засобами штучного інтелекту, має постанова Касаційного господарського суду у складі Верховного Суду від 8 липня 2025 року у справі № 925/496/24 [99].

У цій справі відповідач клопотав перед апеляційним судом про дослідження як електронних доказів відповідей двох систем генеративного штучного інтелекту Grok і ChatGPT з метою підтвердження тлумачення умов договору. Апеляційний суд відхилив клопотання, а касаційна інстанція підтримала цю позицію та сформувала такі правові висновки: штучний інтелект може бути корисним і допоміжним інформативним інструментом у сфері правосуддя, але не може замінити ні суддю, ні принципи належності, допустимості й достовірності доказів; технологію слід використовувати лише для підтримки та посилення верховенства права; відповіді штучного інтелекту не визнають як джерело достовірної науково доведеної інформації, тому відхилення судом клопотання про дослідження їх як доказу є правомірним.

Хоча правова позиція Верховного Суду була сформульована в господарському судочинстві, на нашу думку, її значення виходить за межі цієї юрисдикції та поширюється на інші сфери судочинства, зокрема й на кримінальний процес. Верховний Суд уперше провів межу між двома функціями ШІ: інструментальною (допомога правнику в роботі з текстами) і доказовою (як джерело відомостей про обставини справи). Друга функція була визнана процесуально неприпустимою.

Така позиція узгоджується зі ст. 16 Кодексу суддівської етики, затвердженого XVIII З’їздом суддів України 18 вересня 2024 року[68], і Висновком № 26 (2023) Консультативної ради європейських суддів [42], які безпосередньо визначають, що остаточне рішення у справі ухвалює суддя, а не алгоритм.

Слід зауважити, що цьому рішенню передувала ухвала Касаційного господарського суду у складі Верховного Суду від 8 лютого 2024 року у справі

№ 925/200/22 [134], у якій скаржник уперше на рівні касаційної інстанції посилався на ChatGPT для обґрунтування правової позиції. Суд розцінив апелювання до згенерованої ШІ «позиції» як зловживання процесуальними правами та виявом неповаги до суддів Верховного Суду.

Отже, протягом 2024–2025 років Верховний Суд почав формувати послідовну практику відхилення судом обґрунтувань і висновків, які були сформовані генеративним ШІ.

Інституційне реагування судової системи на розвиток алгоритмів ШІ засвідчує також і Положення про використання технологій штучного інтелекту працівниками Апарату Верховного Суду, затверджене наказом керівника Апарату Верховного Суду від 8 грудня 2025 року № 117 [93].

Зазначені нормативні акти в сукупності з правовими позиціями Верховного суду формують цілісну модель, що визнає ШІ виключно як допоміжний інструмент, але категорично виключає його з процесу оцінки доказів й ухвалення рішень.

Проблематику використання об’єктів, створених за допомогою ШІ, у доказовій діяльності активно розробляють як українські, так і закордонні науковці.

Технологію дипфейку (deepfake) у контексті кримінально-правового реагування досліджували С. Ф. Денисов і Ю. В. Філей [53], які, досліджуючи порнографічні фейки, схарактеризували дипфейк як аудіо- чи відеозапис, змінений так, що глядач сприймає як автентичний.

Кримінологічний вимір цього явища, правомірні сфери застосування технології, способи її створення та використання в кібершахрайствах і політичних маніпуляціях висвітлила К. В. Юртаєва [143].

Емпіричний зріз проблеми на основі рішень з Єдиного державного реєстру судових рішень здійснили К. С. Крамаренко та І. А. Тітко [74], запропонувавши розглядати ШІ в кримінальних провадженнях одночасно як елемент предмета доказування та як джерело аргументації сторін.

У дослідженні Н. С. Савенко й А. М. Лазебний [115] дипфейк включають до загальної системи сучасних форм фальсифікації доказів.

Увагу привертає праця І. В. Гловюк [44], присвячена проблемі «галюцинацій» ШІ в процесуальних документах, зокрема апеляційній скарзі з посиланнями на судові рішення, згенеровані штучним інтелектом, яких у реальності не було.

Кримінально-правові аспекти ШІ в традиційних категоріях національного кримінального права системно проаналізував О. Е. Радутний [111].

Серед іноземних дослідників на доказах, згенерованих за допомогою ШІ, увагу зосереджує R. A. Delfino [176; 177] У цих працях обґрунтовано розширення ролі судді як «воротаря» (gatekeeper) під час оцінки дипфейк-доказів, розроблено механізм перерозподілу тягаря доказування автентичності (burden-shifting framework).

Розмежування визнаних і невизнаних електронних доказів, створених за допомогою ШІ та відповідних процесуальних підходів до них, здійснили M. R. Grossman і P. W. Grimm [195], а комплексний аналіз допустимості електронних доказів, створених або модифікованих засобами штучного інтелекту, у загальному вигляді представили в спільній праці P. W. Grimm, M. R. Grossman та G. V. Cormack [194].

Вплив генеративного ШІ на кримінальне право ґрунтовно окреслив B. Panattoni [220], зауваживши, що ця технологія трансформує характер злочинних можливостей, здешевлює створення шкідливого контенту, масштабує коло потенційних жертв і дозволяє експлуатувати когнітивні вразливості людини. Технологічний та прикладний контекст явища висвітлено в працях M. Westerlund [241] щодо правомірних сфер застосування дипфейку та супутніх ризиків, а також E. Hurst [200], яка серед ключових чинників суспільної небезпеки цієї технології виокремила масштаб, широту застосування та ступінь довершеності згенерованого контенту.

Показовим прикладом небезпечності злочинного використання дипфейку є справа про подію, що сталася в січні 2024 року в середній школі Пайксвілла (штат Меріленд, США) [148; 221]. Працівник школи (керівник за напрямом атлетики) Дажон Дар’єн, дізнавшись про намір директора Еріка Ейсверта не подовжувати з

ним контракт через низькі показники роботи та внутрішню перевірку щодо можливого фінансового зловживання, скористався інструментами генеративного ШІ (зокрема OpenAI та Microsoft Bing Chat) і згенерував аудіозапис, що імітував голос Ейсверта з расистськими й антисемітськими висловлюваннями щодо учнів.

Поширення цього запису в соціальних мережах призвело до тимчасового відсторонення директора від роботи, хвилі публічного осуду, а також погроз на адресу Ейсверта та членів його родини. Висновками експертиз було встановлено сліди штучно згенерованого контенту з подальшим людським редагуванням. Цей кейс ілюструє, як синтезований штучним інтелектом аудіоматеріал здатний бути водночас знаряддям злочину (формування підробленого доказу) і предметом подальшої криміналістичної верифікації в кримінальному провадженні.

Українська судова практика вже містить окремі обвинувальні вироки, у яких штучний інтелект фігурує саме як знаряддя вчинення кримінального правопорушення.

Згідно з вироком Дніпровського районного суду м. Києва від 9 грудня 2025 року у справі № 755/23443/25 [19], обвинуваченого засуджено за ч. 4 ст. 190 КК України. Фактичні обставини справи зводилися до того, що засуджений, використовуючи інструменти генеративного ШІ для «оживлення» статичних зображень, виготовляв відео з накладеним голосовим супроводом і розповсюджував їх через персональні сторінки в соціальних мережах TikTok і Facebook.

Зміст таких відео імітував пропозиції «допомоги» у подоланні фінансових та побутових складнощів і був спрямований на введення в оману потерпілих. Предметом кримінально-правової оцінки суду була саме діяльність із виготовлення та поширення згенерованого ШІ контенту шахрайського спрямування.

Показовою є операція Національної поліції України з викриття організованої групи, що застосовувала дипфейк-технології для обходу біометричної фотоверифікації в банківських онлайн-системах [92].

Отримавши неправомірний доступ до електронних кабінетів громадян, учасники групи генерували відеоматеріали з підставлянням облич потерпілих на

власне зображення, що дало змогу відкрити рахунки від імені щонайменше 286 осіб й оформити кредити на суму понад 4 млн гривень.

Особливість таких посягань полягає в подвійному характері заподіяної шкоди, адже її зазнають як безпосередні потерпілі (клієнти банків), так й особи, чия зовнішність була протиправно використана для генерації підробленого контенту.

Аналіз цих справ засвідчує, що ШІ як знаряддя злочину якісно змінює характер посягання в декількох аспектах: сприйняття дипфейку як реальної інформації, низькі вимоги до спеціальних знань і матеріальних засобів, негативні наслідки для потерпілого й інших осіб (близьких, родичів та ін.).

Потерпілий сприймає дипфейк як оригінал, оскільки генеративні моделі «огортають» потерпілого штучним інформаційним середовищем, причому настільки переконливим, що людина перестає піддавати його критичному осмисленню.

Низькі вимоги до спеціальних знань і матеріальних засобів виявляються в технічній доступності, і порівняно низька вартість таких інструментів дає змогу тиражувати один і той самий метод на сотні епізодів, охоплюючи широке коло жертв.

Негативні наслідки як для потерпілого, так і для інших осіб виявляються в тому, що створена ШІ «віртуальна реальність» здатна провокувати потерпілого на дії, наслідки яких виходять далеко за межі безпосередньої шкоди як для нього, так і для його оточення.

Попри наявність кримінальних проваджень, у яких ШІ відіграє роль знаряддя злочину, станом на 2026 рік Кримінальний кодекс України не містить спеціальної норми, яка безпосередньо встановлювала б відповідальність за створення чи використання дипфейків або іншого штучно згенерованого контенту зі злочинною метою.

Часткову реакцію законодавця відображає законопроєкт № 14165 від 29 жовтня 2025 року [110], що знаходиться на розгляді Верховної Ради України та передбачає відповідальність у виді позбавлення волі на строк до десяти років за створення, модифікацію або поширення творів, відео-, фото- чи інших матеріалів

порнографічного й еротичного характеру, виготовлених з використанням інформаційних технологій і таких, що відтворюють зовнішність або голос особи без її добровільної згоди.

Порівняльно-правовий огляд іноземного досвіду дає підстави стверджувати, що низка держав уже випередила Україну в нормативному реагуванні на загрози штучного інтелекту.

У США 2025 року набув чинності федеральний TAKE IT DOWN Act [238], який запровадив кримінальну відповідальність (до трьох років позбавлення волі) за свідоме розповсюдження цифрових підробок інтимного характеру без згоди зображеної особи; законодавець застосовує технологічно нейтральне визначення «цифрової підробки», охоплюючи ним будь-які інтимні візуальні матеріали, отримані за допомогою програмного забезпечення, машинного навчання, ШІ або інших технологічних засобів за умови, що розумна особа не здатна відрізнити їх від справжнього зображення реальної людини.

Паралельно на розгляді Конгресу знаходиться AI Fraud Deterrence Act (H.R. 6306, 119-та сесія) [146], спрямований на посилення відповідальності за шахрайства з використанням ШІ.

Кримінальний кодекс Республіки Польщі 2023 року доповнено нормою про покарання у виді позбавлення волі на строк не менше ніж вісім років за поширення неправдивої чи оманливої інформації, що серйозно загрожує політичному устрою або економіці держави [209].

В Об’єднаних Арабських Еміратах Федеральний указ – закон № 34 від 2021 року «Про боротьбу з неправдивою інформацією та кіберзлочинами» [185] встановив за аналогічні діяння санкцію у виді штрафу до 27,4 тис. доларів США та позбавлення волі строком від одного року.

Такий досвід акцентує на можливості двох напрямів удосконалення КК України: запровадження кваліфікуючої ознаки «з використанням технологій штучного інтелекту» у відповідних складах злочинів; криміналізація як самостійного посягання створення, модифікації чи поширення дипфейків (зокрема інформаційного, новинного й аудіовізуального характеру), виготовлених без згоди

особи, зовнішність, голос або інші ідентифікаційні ознаки якої відтворено в такому контенті.

Зазначені пропозиції матеріально-правового характеру мають суміжний характер і потребують самостійного кримінально-правового дослідження. У межах цієї роботи їх сформульовано як концептуальні орієнтири, що випливають із виявлених у процесі дослідження прогалин процесуального реагування на загрози ШІ, натомість основну увагу зосереджено на процесуально-доказовому напрямі.

Слід зауважити, що поява електронних доказів, які були створені або модифіковані засобами штучного інтелекту, зумовила необхідність розроблення відповідної їх класифікації, вагомий внесок за цим напрямом зробили M. R. Grossman і P. W. Grimm [195].

Дослідники запропонували дихотомічну класифікацію електронних доказів, які були створені або модифіковані засобами штучного інтелекту, на «визнані» (acknowledged), стосовно яких сторона відкрито заявляє про використання штучного інтелекту під час створення чи обробки матеріалу, і «невизнані» (unacknowledged), стосовно яких факт застосування ШІ приховують або він є предметом спору.

Для кожної з категорій автори обґрунтовують необхідність окремого процесуального режиму та формулюють критерії, за якими суд визначає ступінь залучення ШІ до формування доказового матеріалу.

Подальший розвиток ця ідея дістала в праці R. A. Delfino «Deepfakes on Trial 2.0: A Revised Proposal for Authenticating AI-Manipulated Evidence» (2025) [176], у якій запропоновано механізм «перерозподілу тягаря доказування автентичності» (burden-shifting framework).

Його суть зводиться до того, що якщо опонент наводить достатні підстави вважати доказ таким, що створений або модифікований засобами ШІ, обов’язок довести його автентичність переходить до сторони, яка цей доказ подає. Відповідне питання має вирішувати суддя одноосібно на стадії попереднього розгляду, а не колегія присяжних під час розгляду справи по суті, оскільки потребує спеціальних технічних знань.

Адаптація зазначеної концепції до національної моделі кримінального провадження потребує врахування кількох принципових відмінностей.

В українському кримінальному процесі немає інституту присяжних у класичному розумінні, а отже, розмежування функцій судді та присяжних, на якому ґрунтується модель «перерозподілу тягаря доказування автентичності», має бути трансформоване в розмежування повноважень слідчого судді (на стадії досудового розслідування) і суду першої інстанції (на стадії судового розгляду).

Також чинний КПК України не передбачає стадії попереднього розгляду доказів як окремого процесуального етапу, тому питання перерозподілу тягаря доказування автентичності вирішують уже на стадії судового розгляду по суті.

Крім того, стандарт prima facie, який є обов'язковим для ініціювання перерозподілу тягаря, потребує конкретизації в умовах національного процесу: таким мінімальним фактологічним обґрунтуванням може слугувати висновок спеціаліста або попередній експертний висновок, що засвідчує наявність ознак штучного походження матеріалу.

Слід зазначити, що жодна із зарубіжних систем кримінального судочинства, зокрема й українська, дотепер не запровадила спеціального процесуального порядку дослідження електронних доказів, які були створені або модифіковані засобами штучного інтелекту.

В Україні такі об'єкти оцінюють за загальними правилами ст. 99 КПК України. Відповідно до ч. 1 цієї статті документом визнають спеціально створений з метою збереження інформації матеріальний об'єкт, що містить зафіксовані письмовими знаками, звуком, зображенням чи в інший спосіб відомості, придатні для використання як доказ обставин, які встановлюють у кримінальному провадженні, а згідно з ч. 2 до документів належать, зокрема, матеріали фотозйомки, звукозапису, відеозапису й інші носії інформації, зокрема електронні.

Унаслідок цього питання автентичного чи штучного походження електронного об'єкта вирішують у тому самому процесуальному режимі, що й стосовно будь-якого іншого електронного доказу, а ключовим інструментом перевірки достовірності залишається судова експертиза – процедура, яка є

витратною за часом і ресурсами та потребує дотримання процесуальних вимог на кожному етапі провадження.

В окремих категоріях справ сторона захисту використовує процесуальну тактику оспорювання доказів, побудовану на твердженні про їхнє штучне походження. Аналіз судової практики засвідчує, що такі доводи послідовно відхиляють суди, якщо вони мають характер припущень і не підкріплені належними й достовірними відомостями, зокрема у вироках Соснівського районного суду м. Черкаси від 23 січня 2026 року у справі № 712/11916/24 [31], Херсонського міського суду Херсонської області від 19 вересня 2025 року у справі № 766/10850/24 [37] і Первомайського міськрайонного суду Миколаївської області від 12 березня 2025 року у справі № 484/4660/24 [29]. Тягар обґрунтування версії про штучне створення доказу покладено на ту сторону, яка на цьому наполягає, і вимагає подання переконливих даних, а не абстрактного посилання на технологічну можливість підробки.

Американська модель регулювання, закладена у Федеральних правилах доказування США (Federal Rules of Evidence) [187], керується вимогою релевантності доказу як базового фільтра його допустимості (правило 401). Нині FRE не містять окремих положень, які стосувалися б електронних об’єктів, які були створені або модифіковані засобами штучного інтелекту, однак у доктрині та правозастосуванні вже сформульовано кілька варіантів їх адаптації.

W. M. Carlucci, K. E. Stone та N. A. Sarokhanian [157] запропонували доповнити правило 901 FRE новим розділом, який окремо регулює випадки, коли доказ підозрюють у повній чи частковій модифікації засобами ШІ, й уточнює розподіл тягаря доказування для таких ситуацій [157].

Паралельно 2025 року Комітет з правил практики та процедури Судової конференції Сполучених Штатів розглянув проєкт нового Правила 707 «Machine-Generated Evidence» [223], яке передбачає окремий (диференційований) підхід до оцінки доказів, створених алгоритмічними системами.

Запропоновану конструкцію допустимості електронних доказів, які були створені або модифіковані засобами штучного інтелекту, можна описати як

двоступеневу: спершу опонент має подати докази того, що відповідний електронний об’єкт може бути створений або модифікований засобами ШІ, і лише після цього обов’язок підтвердити автентичність переходить до сторони, яка доказ пред’явила.

Отже, правило ґрунтується на взаємопов’язаних принципах. Для ініціювання перевірки автентичності недостатньо простого твердження чи припущення, оскільки потрібне фактологічне обґрунтування з наданням доказів, висновків спеціалістів, сертифікованих програмних продуктів про наявність ознак об’єкта, який модифіковано засобами ШІ.

Якщо таке обґрунтування з доказами надано, то сторона-заявник повинна довести справжність доказу за підвищеним стандартом доказування.

Методологічним орієнтиром в оцінці допустимості матеріалів, створених ШІ, є доктрина, сформульована у справі Daubert v. Merrell Dow Pharmaceuticals, Inc. [174], яка встановила критерії допустимості експертних показань і наділила суддю функцією «воротаря» (gatekeeper), відповідального за відсіювання наукового матеріалу, що не відповідає стандартам надійності. До факторів, які підлягають оцінці, відносять проходження процедури рецензування, наявність відомих показників похибок й обґрунтованість методології.

Практичне застосування цих критеріїв до інструментів ШІ ілюструє рішення Верховного суду штату Вашингтон у справі State of Washington v. Puloka [235], якому суд відмовив у допуску як доказу відеозапису, «покращеного» засобами ШІ.

Сторона захисту в цій справі намагалася долучити покращений за допомогою засобами ШІ відеозапис зі смартфону, посилаючись на низьку якість оригіналу. Суд, кваліфікувавши відповідне програмне забезпечення як новаторську техніку, поклав на сторону, що його використовує, тягар доведення прийнятності такого методу в профільній спільноті.

У процесі розгляду суд констатував, що алгоритми машинного навчання продукту Topaz Video AI не пройшли рецензування спільноти судово-медичного відеоаналізу, не підлягають відтворенню її учасниками та не здобули загального визнання у фаховому середовищі.

Додатковим аргументом проти допустимості стало те, що захист не навів жодного прецеденту, у якому «покращене» відео за допомогою алгоритмів ШІ було б прийняте як доказ у кримінальному чи цивільному процесі.

Окреслені підходи дають змогу сформулювати тезу про те, що допустимість електронних доказів, які були створені або модифіковані засобами штучного інтелекту або науковою обґрунтованістю відповідного алгоритму чи сформованим прецедентом застосування відповідного алгоритму.

Якщо застосовуваний інструмент не пройшов відповідну сертифікацію, не має верифікованих показників похибки та не визнаний у профільній науковій спільноті, його не можна вважати таким, що забезпечує стандарт допустимості в кримінальному провадженні. Водночас можливість алгоритмів ШІ істотно змінювати доказовий матеріал як у бік посилення, так і в бік послаблення його пізнавальної цінності, робить необхідним формування спеціальних процесуальних механізмів їх перевірки.

У кримінальному процесі відомий прецедент визначення штучного створення засобами ШІ об’єктів, які стали доказами в кримінальному провадженні, який відображено в постанові Верховного Суду від 27 травня 2025 року у справі № 161/5016/21 [97], ухваленій у межах провадження про розповсюдження порнографічних зображень.

Сторона захисту обстоювала тезу про те, що частина інкримінованих матеріалів була згенерована засобами ШІ, а не отримана шляхом фотофіксації реальних об’єктів. Верховний Суд зазначив, що факт застосування технологій штучного інтелекту під час створення забороненого контенту не звільняє особу від кримінальної відповідальності: ключовим для кримінально-правової оцінки є факт виготовлення та поширення матеріалів відповідного змісту незалежно від того, створені вони людиною чи сформовані алгоритмічно. Питання природи походження зображень у цій справі не підлягало окремому дослідженню, адже юридично значущим визнавано результат, а не технічний спосіб його отримання.

Водночас штучний інтелект не слід розглядати виключно як загрозу системі доказування, оскільки ті самі технології та алгоритми здатні виконувати й

протилежну функцію, а саме слугувати інструментом верифікації автентичності електронних об’єктів.

Алгоритми здатні опрацьовувати значні обсяги даних, розпізнавати артефакти рендерингу, текстурні спотворення, аномалії освітлення й тіней та інші ознаки штучного походження, які залишаються поза межами людського зорового сприйняття.

На ринку вже є низка програмних рішень, здатних діагностувати ознаки генеративного походження контенту, зокрема Intel FakeCatcher, Microsoft Video Authenticator, Sensity AI, Reality Defender та Attestiv.

За умови розроблення стандартів сертифікації та методичних вимог до застосування таких продуктів вони потенційно могли б бути інтегровані в процесуальний інструментарій учасників кримінального провадження як для перевірки отриманих доказів, так і для обґрунтування тверджень щодо їхнього штучного походження.

Висновки до розділу 2

У другому розділі досліджено порядок збирання, оцінки та використання електронних доказів у кримінальному провадженні України, що надало можливість сформулювати такі висновки.

1. Запропоновано процесуально-правову концепцію трансформації електронного об’єкта на доказ через послідовний порядок дій: 1) відтворення електронної інформації засобами програмно-апаратного забезпечення; 2) аналіз її атрибутів і метаданих; 3) описове закріплення в процесуальному документі; 4) вилучення/копіювання з гарантією цілісності через хешування та фіксацію chain of custody.

2. На підставі узагальнення судової практики виокремлено правову позицію «презумпції допустимості електронного доказу», яка полягає в тому, що електронна форма доказу не є підставою для визнання його недопустимим, а

підстави для визнання недопустимим мають бути пов’язані з порушенням процесуального порядку отримання.

3. Обґрунтовано концепцію динамічної природи достовірності електронного доказу як категорії, що верифікується на кожному наступному етапі провадження через ланцюг поводження (chain of custody), на відміну від традиційного розуміння достовірності як властивості, що встановлюють одноразово.

4. Встановлено, що належність електронного доказу поширюється також на метадані («мовчазні свідки» електронних доказів), які можуть самостійно встановлювати обставини, що належать до предмета доказування за ст. 91 КПК України.

5. Розроблено класифікацію листування в месенджерах як окремого виду електронних доказів за вісьмома критеріями (за кількістю учасників, рівнем доступу, можливістю розміщення контенту, етапом створення, джерелом походження, форматом, змістово-інформаційною складовою, способом формування відповідей). Встановлено, що листування в месенджерах є найпоширенішим видом електронних доказів і набуло статусу основного джерела доказової інформації в провадженнях про злочини проти основ національної безпеки.

6. Запропоновано доповнити КПК України статтею 99-3 «Особливості оцінки електронних доказів, створених або модифікованих засобами штучного інтелекту», що передбачає три правила: обов’язок розкривати факт використання штучного інтелекту; перерозподіл тягаря доказування автентичності в разі обґрунтованих сумнівів; недопустимість нерозкритого штучно згенерованого доказу. Виокремлено критерії обґрунтованості сумнівів сторони щодо штучного походження доказу: висновок спеціаліста; попередній експертний висновок; інші фактологічні дані.

7. Обґрунтовано необхідність запровадження дієвого судового контролю під час отримання та дослідження електронної інформації, зокрема через функціональне розмежування повноважень, за якого технічний огляд значного

масиву даних здійснює незаінтересований спеціаліст, а використання відібраної інформації допускається лише після перевірки слідчим суддею.

8. Узагальнення опитування респондентів засвідчило домінування пропозицій щодо стандартизації процедур збирання, фіксації, дослідження та оцінки електронних доказів, закріплення критеріїв їх автентичності, внесення відповідних змін до КПК України (а саме щодо окремого регулювання електронних доказів і порядку фіксації листування в месенджерах), а також формування єдиної судової практики, зокрема шляхом узагальнень Верховного Суду.

РОЗДІЛ 3
АНАЛІЗ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ ІНШИХ КРАЇН

Порівняльно-правовий аналіз зарубіжного досвіду є необхідною передумовою для формулювання науково обґрунтованих пропозицій з удосконалення національного законодавства. Несформованість єдиного універсального підходу до регулювання електронних доказів у кримінальному процесі зумовлена різними правовими традиціями, рівнем цифровізації й історичними особливостями формування доказового права в кожній юрисдикції.

Для порівняльного аналізу обрано юрисдикції, що належать до різних правових сімей і демонструють принципово відмінні моделі регулювання електронних доказів. Англо-саксонська система представлена Сполученими Штатами Америки (як носієм формалізованої моделі з кодифікованими критеріями допустимості), Канадою (з унікальним інститутом презумпції цілісності електронних документів) і Великою Британією (з прагматичним підходом, ґрунтованим на суддівській дискреції). Континентальна система представлена Францією та Федеративною Республікою Німеччина, які демонструють відмінні підходи до інтеграції електронних доказів у традиційну класифікацію джерел доказів. Увагу зосереджено й на правових системах Китайської Народної Республіки (КНР) й Республіки Індія, які належать до змішаних правових моделей і цікаві тим, що КНР є однією з небагатьох країн, де електронні дані законодавчо закріплені як самостійний вид доказів, а Індія розробила специфічний механізм сертифікації електронних доказів.

Зазначений вибір країн доповнює дослідження І. Г. Каланчі (2025), сфокусоване на електронному сегменті кримінального процесу пострадянських держав (Республіка Молдова, Грузія, Естонська Республіка, Латвійська Республіка, Республіка Вірменія, Туркменістан, Азербайджанська Республіка), що забезпечує комплексний аналіз провідних світових моделей регулювання електронних доказів.

Порівняння буде здійснено за такими критеріями: наявність законодавчого визначення електронного доказу; процесуальний статус електронного доказу в системі джерел доказів; порядок автентифікації та вимоги до допустимості; розподіл тягаря доказування автентичності; наявність спеціалізованих інститутів (презумпція цілісності, сертифікація, стандарти збирання).

3.1. Електронні докази в англо-саксонській системі права (США, Канада, Велика Британія)

В англосаксонській правовій системі не сформовано чіткого поділу доказів на окремі види. Натомість доказове право ґрунтується на типових проблемних ситуаціях, що виникають у судовій практиці. Доказове право *США* фактично є результатом кодифікації ключових і прецедентних судових рішень, узагальнення напрацьованої практики та має переважно заборонний характер, оскільки визначає обставини, за яких певний доказ не може бути визнано допустимим. У зв'язку з цим для американських правників не має принципового значення питання про віднесення електронних доказів до самостійного виду доказів [230, с. 2].

Попри значну роль штатного законодавства, у Сполучених Штатах на федеральному рівні сформовано загальні принципи кримінального судочинства, обов'язкові для правоохоронних органів і судів штатів, джерелами яких є Конституція США, федеральні законодавчі акти та норми процесуального права. Правила поводження з електронними доказами в кримінальному процесі США ґрунтуються на загальних принципах доказового права, закріплених у Федеральних правилах доказування (Federal Rules of Evidence, FRE) [187], прийнятих 1975 року, а також на Федеральних правилах кримінального судочинства (Federal Rules of Criminal Procedure, FRCP) [3; 186].

Відповідно до Rule (Правила) 402 FRE [187], усі релевантні докази є допустимими, якщо інше не передбачено Конституцією США, федеральними законами або спеціальними правилами. Релевантність визначає правило 401 FRE за

наявності двох умов: (а) здатність доказу робити факт більш або менш імовірним, порівняно із ситуацією за його відсутності; (б) факт, що підтверджений доказом, повинен мати значення для встановлення обставин справи. Згідно з правилом 403 FRE, суд може відхилити навіть релевантний електронний доказ, якщо його доказова цінність суттєво переважає над небезпекою несправедливого упередження, уведення в оману присяжних або затягування процесу.

Наведена модель демонструє принципову схожість між американською категорією «релевантності» (relevance) та національною категорією «належності» доказів, передбаченою ст. 85 КПК України.

Автентифікація є ключовою умовою допустимості електронних доказів у кримінальному процесі США. Правило 901(a) FRE встановлює, що сторона, яка подає доказ, повинна надати достатні підтвердження для висновку про те, що доказ є саме тим, за що його подає. Поріг автентифікації є відносно невисоким, адже достатньо пред'явити такі обставини, за яких присяжні могли б визнати доказ справжнім. Правило 901(b) FRE передбачає різні способи автентифікації: прямі показання свідка, обізнаного з об'єктом (наприклад, слідчого, який отримав файл, або адресата електронного листа); експертне порівняння зі зразком; характерні ознаки контенту (метадані, унікальні деталі) у поєднанні з обставинами справи.

Учасник процесу, надаючи суду електронний доказ, має довести його автентичність за допомогою стандартної процедури автентифікації електронного документа, або сторона має надати опис процесу створення або систему, яку використовують для одержання результату, продемонструвати, що система або процес дає точний результат [190].

Здебільшого використовують такі методи автентифікації, як перевірка геш-значень, аналіз метаданих і використання цифрових підписів.

Відповідно до правила 41(a)(2)(A) FRCP, як інформацію, так й інші матеріальні об'єкти кваліфікують як «майно». Іноземні науковці зазначають, що цей підхід, поєднаний з положеннями Четвертої поправки до Конституції США, відіграє фундаментальну роль у процесі збирання електронних доказів.

Вагомими для застосування принципів використання електронних доказів є і судові рішення.

У справі *Lorraine v. Markel American Insurance Co.* суддя Пол Грімм Окружного суду США округу Меріленд запропонував докладні методичні рекомендації щодо допустимості інформації, яку зберігають в електронному вигляді (electronically stored information, ESI), у судових провадженнях [213]. Суддя визначив, що для визнання ESI допустимою необхідно дотримуватися низки ключових вимог:

1) релевантості (правила 401 і 402 FRE) – подана інформація має стосуватися предмета спору та сприяти встановленню істотних фактів;

2) автентичності (правило 901 FRE) – необхідно підтвердити, що електронний доказ є справжнім і відповідає заявленому змісту. Методи автентифікації можуть охоплювати перевірку метаданих, геш-значень або показань свідків;

3) дотримання правил щодо показань з чужих слів (правила 801, 803 і 804 FRE) – електронний доказ не визнається недопустимим як показання з чужих слів, якщо він охоплюється одним із установлених винятків — зокрема діловими записами (правило 803(6)) або заявами проти власних інтересів;

4) дотримання правила найкращого доказу (правила 1001–1008 FRE) – має бути подано оригінали або допустимі копії, за винятком випадків, коли оригінали недоступні з поважних причин;

5) відсутності несправедливого упередження (правило 403 FRE) – релевантні докази можуть бути виключені, якщо їх доказова цінність істотно поступається ризику несправедливого упередження, введення суду в оману або затягування процесу.

Суд також зауважив, що недотримання зазначених вимог може призвести до виключення електронних доказів із розгляду, що вкотре акцентує на важливості належної підготовки та коректного подання електронного доказу до судового процесу [214].

Позиція щодо стандарту автентифікації електронних доказів була сформульована американськими судами ще на початкових етапах появи справ з електронними доказами.

У справі *United States v. DeGeorgia,* (1969 р.), суд сформулював принципову позицію, відповідно до якої стандарт доведення автентичності електронного документа є тотожним стандарту автентифікації інших видів документів, а ступінь автентифікації не змінюється лише тому, що запис в електронній формі [239].

Цікавим є факт, що для того, щоб довести автентичність електронного доказу в судовому процесі, залучені особи, які мають підтверджувати автентичність, не завжди повинні мати спеціальну освіту або бути експертами.

У справі *U.S. v. Whitaker (1997 p.)* суд визнав, що автентичність роздрукованих комп'ютерних записів, вилучених під час обшуку в кримінальному провадженні, була належно підтверджена показаннями спеціального агента ФБР, який особисто був присутній під час вилучення комп'ютера та роздруковуванні електронних записів. Суд дійшов висновку, що свідчень, які ґрунтуються на безпосередніх знаннях свідка щодо процесу отримання електронних доказів, достатньо для їх автентифікації відповідно до правила 901(a) FRE доказів [240].

Принципово важливим у цьому рішенні є те, що для автентифікації немає вимоги щодо спеціальної технічної кваліфікації свідка, достатньо безпосереднього сприйняття процесу отримання доказу. Такий підхід ґрунтується на загальному принципі, що автентифікація є питанням мінімального стандарту prima facie.

Увагу привертає нормативна регламентація віддаленого обшуку інформаційних систем (remote search). Відповідно до правила 41 пункта (b)(6) FRCP, згідно з яким суддя-магістрат, що має юрисдикцію в будь-якому окрузі, де можуть бути вчинені дії, пов'язані зі злочином, має повноваження видавати ордер на дистанційний обшук у двох випадках: коли округ фізичного знаходження пристрою приховано шляхом застосування технологічних засобів й у разі розслідування правопорушень за 18 U.S.C. § 1030(a)(5), якщо вражено комп'ютерні системи в п'яти або більше округах. Тобто передбачено обов'язкову попередню судову санкцію, про що зазначає D. M. Adams [145, с. 380–381].

Правове регулювання електронних доказів у *Канаді* здійснюють на основі низки нормативних актів: Закону Канади про докази (Canada Evidence Act, R.S.C. 1985) [156], КК Канади (Criminal Code of Canada) [172], Закону про захист канадців від онлайн-злочинності (Protecting Canadians from Online Crime Act, S.C. 2014, c. 31) [224]. Також правову основу формують висновки Верховного суду Канади й апеляційних судів провінцій. Така багаторівнева модель забезпечує поєднання законодавчого регулювання з прецедентним розвитком стандартів допустимості електронних доказів.

Згідно зі ст. 31.8 Закону Канади про докази, електронний документ (electronic document) означає дані, записані або збережені на будь-якому носії в комп'ютерній системі чи іншому схожому пристрої, які можуть бути прочитані або сприйняті особою чи технічним засобом, водночас визначення прямо охоплює дисплей, роздруківку або інший вивід таких даних [156].

На нашу думку, законодавчо визначена дефініція електронного доказу, додаткового забезпечує єдність правозастосування та правового прогнозування.

Як і в моделі доказування США, у Канаді є вимога автентифікації електронного доказу (ст. 31.1 Закону Канади про докази), оскільки сторона, яка подає електронний документ як доказ, несе обов'язок довести його автентичність [156].

Ключовим інструментом доказування за канадським законодавством є презумпція цілісності системи електронних документів, закріплена в ст. 31.3 Закону Канади про докази.

Вона діє за відсутності доказів протилежного та може ґрунтуватися на одній із трьох альтернативних підстав: належному функціонуванні комп'ютерної системи в усі відповідні моменти часу; запису документа стороною, яка є опонуючою за інтересами стороні, що подає доказ; створенні документа у звичайному процесі діяльності особою, яка не є стороною провадження. Застосування цієї презумпції знижує доказове навантаження на сторону, що подає електронний доказ.

Презумпція цілісності є унікальним інститутом, оскільки полягає в зниженні процесуального навантаження на сторону, яка подає електронний доказ, оскільки замість позитивного доведення автентичності достатньо продемонструвати належне функціонування системи.

Проте, на нашу думку, цей механізм містить ризик, який набуває особливого проявлення в умовах ресурсної нерівності сторін. Якщо сторона захисту не має фінансових або технічних можливостей для залучення спеціаліста, здатного дослідити функціонування комп'ютерної системи та спростувати презумпцію, доказ фактично набуває статусу безспірного.

Крім того, презумпція цілісності сформована в контексті традиційних комп'ютерних систем і не враховує специфіку хмарних сервісів, де дані можуть обробляти на серверах у різних юрисдикціях, а контроль за цілісністю системи виходить за межі компетенції як сторін, так і суду.

У справі *R. v. M.S.A.* (2024 р.) суд розглянув питання дотримання правила найкращого доказу щодо електронних матеріалів, закріпленого в ст. 31.2 Закону Канади про докази. Сторона обвинувачення подала як електронні докази (аудіозаписи й текстові повідомлення), отримані від потерпілої. Сторона захисту наполягала на порушенні зазначеного правила з огляду на розбіжність між часовими позначками в метаданих записів і задекларованими датами їх створення.

Суд відхилив такі аргументи, зазначивши, що виявлену розбіжність пояснювали перенесенням записів з мобільного телефону потерпілої на її персональний комп'ютер, і підтвердив принцип низького порогу автентифікації електронних документів відповідно до ст. 31.1–31.2 Закону. Окрім того, суд визнав, що показань потерпілої про відповідність поданих цифрових матеріалів безпосередньо сприйнятим нею обставинам достатньо для задоволення вимог презумпції цілісності електронної системи [225].

У справі *R. v. S.M.* (2025 р.) Апеляційний суд провінції Онтаріо розглянув питання автентифікації знімків екрана (скріншотів) електронних зображень, переданих потерпілій у застосунку Snapchat третьою особою, яка в судовому розгляді показань не давала. Суд підтвердив, що низький поріг автентифікації,

закріплений у ст. 31.1 Закону Канади про докази, поєднаний із широким визначенням електронного документа в ст. 31.8, поширюється й на схожі опосередковані електронні матеріали [228].

Привертає увагу й судовий кейс *R. v. Jamali* (2017р.), які дослідили у своїй праці канадські вчені М. Берюбе, Л.-А. Больо, С. Алляр і В. Дено, щодо обвинувачень у тероризмі, яке розглядав Вищий суд Квебеку у 2017–2018 роках, що завершилося виправданням обвинувачених [155]. Особливість справи полягала в тому, що орган досудового розслідування зібрав доволі масивні об'єми електронних матеріалів, які потребували відбору, дослідження.

За результатами дослідження автори виявили три групи системних проблем, що безпосередньо впливають на доказову цінність електронних доказів:

– операційні, які пов'язані зі складнощами обробки великого обсягу даних (понад 8000 сторінок вмісту Facebook, 30 000 інтернет-посилань, 20 000 зображень), що в умовах обмежених ресурсів спонукало орган досудового розслідування до селективного відбору доказів, які підтверджували попередньо сформовану обвинувальну версію слідства, а виправдувальні докази не зберігалися в матеріалах слідства. Унаслідок цього під час перехресного допиту сторона захисту продемонструвала неповноту й тенденційність подання доказів, що поставило під сумнів їхню достовірність;

– технічні – щодо криміналістичного програмного забезпечення, яке застосовували для збирання доказів (Encase, IEF, Cellebrite UFED). Було встановлено, що алгоритми категоризації та фільтрації даних програмного забезпечення можуть вносити інтерпретаційне спотворення, не помітне для кінцевого користувача. Пояснення експертом технічних процесів й алгоритмів роботи програмного забезпечення стало викликом для суддів і присяжних через технічну термінологію та складність;

– управлінські (організаційні): в органі досудового розслідування не було визначено підрозділ — технічний, аналітичний чи слідчий, — відповідальний за формування повного й неупередженого масиву електронних доказів.. Унаслідок цього слідчий до матеріалів обвинувачення додав лише 330 зображень із 2730

фактично вилучених, що, на думку сторони захисту, сприяло «тунельному баченню» та формуванню упередженого сприйняття доказів [155].

Ми поділяємо висновки, що селективність відбору, відсутність контексту, непрозорість інструментів збору й обробки електронних доказів можуть впливати на об'єктивний та справедливий судовий кримінальний процес.

Крім того, виявлені додаткові ризики роботи з електронними доказами у випадку їх великого об'єму, а саме селективність відбору, деконтекстуалізація, непрозорість інструментів обробки, комунікаційний розрив між експертами й учасниками судового процесу.

Зазначена проблематика може слугувати окремим напрямом наукового дослідження та потребує урахування під час удосконалення національного кримінального процесуального законодавства в частині регламентації порядку збирання, дослідження та оцінки електронних доказів.

Окрім того, необхідність стандартизації контекстуалізації та валідації електронних доказів кореспондує з обґрунтованою в нашому дослідженні потребою формування в КПК України єдиних вимог до процесуального фіксації електронних доказів, що забезпечуватимуть їхню перевірку та відтворення.

Особливість канадської моделі полягає у відсутності окремих норм, яка прямо регулювала б віддалений негласний доступ до комп'ютерних систем. Стаття 487(2.1) Кримінального кодексу Канади (Criminal Code, R.S.C. 1985, c. 46) дозволяє лише пошук у системі, доступній з обшукуваного приміщення, натомість прихований дистанційний захід авторизується через інститут «загального ордера» (general warrant) за ст. 487.01 – як санкціонована суддею слідча дія[172].

Канадська модель правового регулювання електронних доказів вирізняється комплексним функціональним характером: вона поєднує законодавчо закріплені стандарти автентифікації, презумпцію цілісності й адаптоване правило найкращого доказу з розвиненим процесуальним інструментарієм отримання електронної інформації, передбаченим Законом про захист канадців від онлайн-злочинності (Protecting Canadians from Online Crime Act, S.C. 2014, c. 31) й активною роллю судової практики у формуванні правозастосовних стандартів.

Правовій системі *Великої Британії* притаманна відсутність кодифікованої дефініції електронного доказу, а електронні дані оцінюють на підставі Закону про поліцію та кримінальні докази 1984 року (Police and Criminal Evidence Act 1984, PACE) за загальними правилами доказування, сформованими в межах англійського права [222; 242].

Саме цей акт встановлює загальний критерій процесуальної справедливості, який застосовують і до цифрових доказів. Відповідно до ст. 78(1) PACE, суд може відмовити в допущенні доказу, на який посилається сторона обвинувачення, якщо з огляду на всі обставини, зокрема обставин його одержання, допущення такого доказу матиме настільки несприятливий вплив на справедливість провадження, що суд не повинен його приймати [222].

Показово, що зазначене дискреційне повноваження поширюється виключно на докази обвинувачення та може бути реалізоване лише до моменту допущення доказу.

Отже, для британського підходу визначальним є не лише питання формальної релевантності електронного доказу, а й насамперед його вплив на справедливість судового розгляду, що зумовлює потребу оцінки таких доказів крізь призму законності їх одержання, автентичності, цілісності та процесуальної добросовісності сторони, яка їх подає

Відповідно до ст. 19 PACE, поліцейський, який законно перебуває в приміщенні, наділений загальним повноваженням вилучати будь-який предмет, що знаходиться в приміщенні, за наявності обґрунтованих підстав вважати, що його одержано внаслідок вчинення злочину або він є доказом у справі про злочин, який розслідують, чи будь-який інший злочин.

Окремо ст. 19(4) встановлює спеціальне повноваження щодо електронної інформації: за наявності аналогічних підстав поліцейський може вимагати, щоб будь-яка інформація, збережена в електронній формі й доступна з приміщення, була надана у видимій і читабельній формі, придатній для вилучення, або у формі, з якої її можна легко відтворити в такому вигляді.

Важлива особливість британської моделі полягає в тому, що автентичність електронного доказу не зводиться до формально-технічної сертифікації. Судова практика керується тим, що електронний доказ повинен бути достатньо автентифікованим для того, щоб суд міг дійти висновку про його походження та надійність, однак спосіб такої автентифікації визначають з огляду на обставини конкретної справи.

Показовою в цьому контексті є справа *R v Mawji (Rizwan)* (2003 р.), у якій Апеляційний суд Англії та Уельсу визнав допустимим електронний лист із погрозою вбивством, відхиливши аргумент захисту про необхідність попереднього доведення технічної неможливості фальсифікації повідомлення [226].

Попри демонстрацію стороною захисту відносної простоти редагування (підробки) електронних листів, суд визнав, що зміст повідомлення у взаємозв'язку з іншими доказами справи був достатнім для обґрунтованого висновку про те, що лист був створений і надісланий саме обвинуваченим.

Це рішення демонструє, що в британському праві змістова оцінка доказу та його кореляція з іншими матеріалами справи можуть переважати над вимогою надмірної технічної формалізації процедури автентифікації.

Британська модель є найгнучкішою серед досліджених, проте ця гнучкість має зворотний бік. Відсутність кодифікованих критеріїв автентифікації електронних доказів означає, що рівень вимог до допустимості може суттєво варіюватися залежно від конкретного суду, складності справи та кваліфікації сторін.

Якщо у справі R v Mawji [226] суд прийняв електронний лист без технічної верифікації, то в іншій справі аналогічний доказ може бути відхилений на підставі тієї самої ст. 78 PACE. Така непередбачуваність, з одного боку, забезпечує індивідуалізацію правосуддя, а з іншого – ускладнює формування єдиної правозастосовної практики та створює ризик правової невизначеності для учасників провадження.

Прихований віддалений доступ до інформаційних систем у Сполученому Королівстві регламентований самостійним інститутом – втручанням в обладнання (equipment interference, EI) у ч. 5 Investigatory Powers Act 2016 (IPA)) [203].

Згідно зі ст. 99 IPA 2016, цільовий ордер на втручання в обладнання видає Державний секретар (Secretary of State) на підставі заяви правоохоронного органу або розвідувальної служби та набуває чинності лише після затвердження Судовим комісаром (Judicial Commissioner) у межах механізму «подвійного замка» (ст. 108–110 IPA 2016) [203].

3.2. Електронні докази в романо-германській системі права (Франція, Німеччина, нормативна база ЄС)

Сучасна правова структура регулювання електронних доказів у країнах Європейського Союзу формується сукупністю міжнародно-правових інструментів і національних особливостей, що в сукупності утворюють багаторівневу правову систему.

Низку актів Європейського Союзу у сфері електронних доказів спрямовано на забезпечення дієвого транскордонного співробітництва держав-членів у кримінальному процесі.

Конвенція про кіберзлочинність 2001 року (Будапештська конвенція) є міжнародним стандартом у сфері збирання електронних доказів і боротьби з кіберзлочинністю. Зазначений документ ратифікований усіма державами – членами ЄС, унаслідок чого положення Конвенції про процесуальні механізми оперативного збереження даних, виїмки комп’ютерних систем, перехоплення комунікацій та міжнародного співробітництва імплементовано до національного кримінально-процесуального законодавства держав Союзу [181, с. 1].

Також на рівні ЄС діють Регламент 2023/1543 про Європейські ордери на пред’явлення та Європейські ордери на збереження електронних доказів у кримінальному провадженні та для виконання покарань у вигляді позбавлення волі

після розгляду кримінальної справи [229] та (2) Директива 2023/1544, що встановлює правила збору електронних доказів у кримінальному провадженні [179].

Зазначені акти дають змогу судовому органу однієї держави – члена ЄС безпосередньо зобов'язати постачальника послуг в іншій державі-члені надати або зберегти електронні докази, незалежно від фізичного місцезнаходження даних. Регламент охоплює чотири категорії даних: інформацію про абонента, IP-адреси, дані трафіка та змістові дані (content data), до яких належать зміст листування, повідомлень, файлів тощо. Документ запроваджує диференційований підхід до процедурних гарантій: що чутливішими є дані, то суворішими є вимоги до видання наказу. Регламент застосовуватимуть з 18 серпня 2026 року [229].

Відповідно до п. 8 ст. 3 Регламенту (ЄС) 2023/1543, категорія електронних доказів охоплює три групи даних: дані абонента, дані трафіка й дані змісту, що зберігає постачальник послуг (або від його імені) в електронній формі, їх витребовують шляхом видачі Європейського наказу на надання або Європейського наказу на збереження.

Дані абонента охоплюють інформацію, яка дає змогу ідентифікувати особу як користувача послуги: зареєстроване ім'я, дату народження, поштову адресу, платіжні реквізити (зокрема банківські дані для оплати), номер телефону, адресу електронної пошти, а також відомості про вид наданої послуги та строк її надання.

Дані трафіка становлять відомості, що супроводжують надання послуги та характеризують процес електронної комунікації: джерело й адресата повідомлення або іншої взаємодії, місцезнаходження пристрою, дату, час, тривалість, обсяг, маршрут передачі, формат, використаний протокол і тип стиснення, а також інші метадані. Дані змісту становлять інформацію в цифровій формі, що відображає безпосередній зміст комунікації – текст, голосові повідомлення, відео, зображення та звукові записи [183].

Також важливим документом для правоохоронних органів є Рекомендації щодо роботи з електронними доказами [196]. На основі цих рекомендацій правоохоронні органи держав – членів ЄС розробили відомчі інструкції, що

регламентують технічні аспекти вилучення комп'ютерної техніки, її транспортування та забезпечення збереження електронних даних.

Інституційне забезпечення цифрових розслідувань реалізують через створення спеціалізованих національних підрозділів. Так, у Франції діє Центр боротьби з цифровою злочинністю (Centre de lutte contre les criminalités numériques, C3N) [188], а в Німеччині - Центральна служба боротьби з інтернет-злочинністю (Zentralstelle zur Bekämpfung der Internetkriminalität, ZIT), яка функціонує при Генеральній прокуратурі Франкфурта-на-Майні й тісно співпрацює з Федеральним відомством кримінальної поліції (Bundeskriminalamt, BKA) [154].

Детальний аналіз цих нормативних актів дає змогу дійти висновку, що сучасна модель правового регулювання електронних доказів у Європейському Союзі вирізняється багаторівневим механізмом, у якому органічно поєднано міжнародно-правові інструменти (конвенції, методики, стандарти), наднаціональне законодавство ЄС, національні імплементаційні акти держав-членів і відомчі методичні стандарти. Такий механізм забезпечує процесуальну ефективність використання електронних доказів у транскордонних кримінальних провадженнях за умови дотримання гарантій основоположних прав особи.

Зазначені акти спрямовані на ефективний транскордонний доступ до електронних доказів з одночасним забезпеченням дотримання основоположних прав людини й стандартів захисту персональних даних.

Попри активність процесів європейської інтеграції, законодавча гармонізація у сфері кримінального процесу залишається фрагментарною та не ґрунтується на єдиній універсальній правовій основі в межах Європейського Союзу. Кримінально-правові та кримінально-процесуальні системи держав – членів Союзу й надалі ґрунтуються на національних правових доктринах та історично сформованих правових традиціях [217]

У законодавстві *Федеративної Республіки Німеччини* немає легального визначення електронного доказу. Усі докази, зокрема ті, що існують в електронній формі, підпадають під дію принципу вільної оцінки доказів судом, закріпленого КПК Німеччини (Strafprozessordnung, StPO) [237].

Водночас німецький кримінальний процес поступово розвивається в напрямі цифровізації: до StPO імплементовано положення, що регламентують онлайн-перехоплення комунікацій та негласний віддалений пошук комп'ютерних даних.

Важливе значення в цьому контексті має рішення Федерального конституційного суду Німеччини від 27 лютого 2008 року у справі про онлайн-обшук (Online-Durchsuchung), прийняте за скаргою на законодавство федеральної землі Північний Рейн – Вестфалія.

Суд сформулював нове основоположне право – гарантію конфіденційності та цілісності інформаційно-технічних систем, що ґрунтується на загальному праві особистості (ст. 2 абз. 1 в поєднанні зі ст. 1 абз. 1 Основного закону ФРН).

Відповідно до правової позиції суду, негласне проникнення органів держави в комп'ютерну систему особи становить особливо серйозне втручання в приватність і є допустимим лише за сукупності умов: наявності конкретної загрози найвищим правовим благам (життю і фізичній цілісності особи, основам існування держави) та дотримання процесуальних гарантій, насамперед попередньої санкції незалежного суду [182, с. 1].

Такий механізм встановлює найвищий стандарт захисту права особи на приватність, однак з іншої сторони, процедура санкціонування (перелік злочинів, колегія трьох суддів, перевірка «права приватності») суттєво уповільнює отримання дозволу. Це робить його критичним для розслідування кіберзлочинів, де електронні докази є волатильними й можуть бути знищені протягом годин.

Такий механізм встановлює найвищий стандарт захисту, однак висока «вхідна» вимога (конкретна загроза найвищим правовим благам) і складна триступенева процедура санкціонування (перелік злочинів, колегія трьох суддів, перевірка «права приватності») суттєво уповільнюють отримання дозволу. Це робить його малопридатним для розслідування кіберзлочинів, де електронні докази є волатильними й можуть бути знищені протягом годин.

У німецькій кримінальній процесуальній доктрині питання допустимості електронних доказів традиційно розглядають у площині гарантування конституційних прав особи.

У разі коли електронний доказ отримано з порушенням права на приватність або за відсутності належної процесуальної підстави, сторона захисту може ініціювати визнання такого доказу недопустимим з посиланням на доктрину заборони використання доказів [191].

Зазначена доктрина, що сформувалася в німецькій кримінально-процесуальній науці та послідовно розвивається судовою практикою, передбачає виключення з доказової бази тих відомостей, отримання яких пов'язане з істотним порушенням процесуального закону або основоположних прав особи, наприклад, у випадку отримання даних із мобільного телефону без відповідної судової санкції. Спори стосовно допустимості таких доказів нерідко стають предметом розгляду Федерального конституційного суду Німеччини, який послідовно формує конституційно-правові стандарти втручання державних органів у сферу інформаційної приватності особи [237].

Стосовно процедури встановлення автентичності електронних доказів німецька кримінально-процесуальна традиція є менш формалізованою, порівняно з англо-американською моделлю.

Німецьке право не передбачає аналогів інституту самоавтентифікації доказів, притаманного системам загального права; натомість оцінку справжності електронного доказу здійснюють у межах загального принципу вільної оцінки доказів судом. У разі якщо сторона провадження заперечує автентичність електронного доказу, суд уповноважений призначити відповідну експертизу або безпосередньо дослідити доказ у судовому засіданні із залученням за необхідності спеціальних знань [236].

Порядок віддаленого негласного проникнення до інформаційних систем осіб (Online-Durchsuchung), закріпленого в §100b StPO, яке допустиме виключно в провадженнях про злочини з вичерпного переліку, що міститься в ч. 2 цієї статті.

Відповідно до §100e(2) StPO, такий захід санкціонує колегія в складі трьох суддів окружного суду, а в невідкладних випадках одноособово головою колегії з обов'язковим підтвердженням колегією протягом трьох робочих днів. Окрему гарантію встановлює § 100d(3) StPO: дані, що належать до «права приватного

життя», не підлягають збиранню, а в разі їх отримання негайно видаляють зі складанням відповідного протоколу.

Кодекс кримінального судочинства *Франції* (Code de procédure pénale, CPP) [165] не містить прямого нормативного визначення електронного доказу. Водночас французький законодавець передбачив низку спеціальних процесуальних інструментів, спрямованих на отримання електронних даних у межах кримінального провадження.

У межах французького кримінального процесуального законодавства можна виокремити дві самостійні групи норм, що регулюють відносини, пов'язані зі збиранням електронних доказів.

Першу групу становлять положення про негласне перехоплення комп'ютерних даних, закріплені в ст. 706-102-1 CPP. Зазначена норма спрямована на протидію кримінальним правопорушенням, учиненим з використанням інформаційних технологій, і надає слідчим органам повноваження здійснювати приховане отримання даних безпосередньо з пристрою користувача, зокрема шляхом дистанційного встановлення спеціальних технічних засобів.

З огляду на високий ступінь втручання в приватність, застосування цього інструменту обмежене: він допустимий виключно в провадженнях щодо тяжких кримінальних правопорушень і лише на підставі мотивованого рішення слідчого судді з питань свободи й тримання під вартою (juge des libertés et de la détention).

Другу групу утворюють положення ст. 706-95-1 і 706-95-2 CPP, які регламентують процедуру отримання вже збережених електронних даних від постачальників послуг електронних комунікацій. На відміну від першої групи норм, зорієнтованої на отримання даних у режимі реального часу безпосередньо з пристрою, ці положення стосуються даних, які постачальник послуг уже зберігає у своїх системах. У межах цієї процедури слідчий суддя уповноважений зобов'язати постачальника послуг надати наявні в його розпорядженні електронні дані, зокрема електронні листи та повідомлення.

Отже, французький законодавець розмежовує два принципово різні режими доступу до електронних даних – режим активного негласного перехоплення

(захоплення даних у динаміці) і режим витребування статичних збережених даних, кожен з яких має власні підстави, межі застосування та процесуальні гарантії.

Французька кримінально-процесуальна доктрина та правозастосовна практика традиційно ґрунтуються на принципі свободи доказів (principe de la liberté de la preuve), згідно з яким суд має право брати до уваги будь-які джерела фактичних даних за умови, що вони отримані законним шляхом і відповідають критерію достовірності [234].

Електронні докази не утворюють винятку із цього загального правила, оскільки судова практика послідовно визнає допустимими роздруківки електронної кореспонденції, текстових повідомлень (SMS), даних супутникових систем геолокації (GPS) та інших цифрових джерел інформації, оцінюючи їх за тими самими стандартами, що й традиційні докази [189].

Незалежно від порядку провадження та підслідності, електронні докази набули значення ключового інструменту встановлення обставин кримінального правопорушення у французькій системі кримінального судочинства.

Однією з гучних справ, яка засвідчує важливість електронних даних як ключових доказів, є справа «зґвалтувань у Мазані», розкрита саме завдяки криміналістичному аналізу мобільного телефону підозрюваного D. Pelicot [201].

Вагомість електронних доказів у кримінальному процесі Франції виявляється через особливий юридичний механізм щодо розкриття відомостей з мобільного телефону, а саме надання правоохоронним органам захисного коду до мобільного пристрою.

Судова практика сформувала прецедент, що суттєво обмежує право особи на мовчання та відмови в дачі пояснень. Відповідно до позиції Кримінальної палати [159], підтвердженої Пленумом Касаційного суду [158], за певних умов відмова підозрюваного повідомити код доступу до мобільного телефону може бути кваліфікована як самостійний злочин.

Стаття 434-15-2 КК Франції [149] передбачає покарання у вигляді трьох років позбавлення волі та штрафу 270 000 євро за відмову передати судовим органам

таємний ключ розшифрування засобу криптології, якщо цей засіб міг бути використаний для підготовки, полегшення або вчинення злочину.

Слід зауважити, що такий склад злочину було введено до КК Франції після терактів 11 вересня 2001 року, його спершу призначали для боротьби з тероризмом й організованою злочинністю. Отже, електронний доказ у французькому праві захищений не лише процесуально, а й кримінально-правовими засобами, що засвідчує його особливу доказову цінність у сучасному судочинстві.

Водночас така охорона не є абсолютною, оскільки рішення ССЄС від 4 жовтня 2024 року (справа C-548/21) обмежило цю практику, вимагаючи попереднього судового контролю, що означає, що охорона електронних доказів має бути збалансована із захистом основних прав особи [161].

Стаття 427 КПК Франції [165] проголошує лише свободу доказування в кримінальних справах, надаючи судді право ухвалювати рішення за своїм внутрішнім переконанням.

Доказ, окрім законності, має бути й отриманий з дотриманням принципу добросовісності (loi de loyauté de la preuve), який сформований виключно судовою практикою.

Зокрема, Пленум Касаційного суду в рішенні від 7 січня 2011 року визнав недопустимим прихований запис телефонної розмови, здійснений без відома автора висловлювань [175].

Принцип лояльності встановлює подвійний стандарт: правоохоронні органи (поліція, прокуратура) зобов’язані діяти добросовісно під час збирання доказів, натомість приватні особи цим принципом обмежені [166].

Показовою є «справа Короля Марокко», у якій адвокат, що діяв від імені Королівства Марокко, організував таємні зустрічі з особами, причетними до шантажу, і записав розмови на диктофон [170].

Ці записи були негайно передані поліції, яка була присутня поблизу під час зустрічей та підтримувала регулярні контакти з представником заявника. Кримінальна палата Касаційного суду визнала такі докази недопустимими,

констатувавши, що непряма участь органів влади в отриманні недобросовісного доказу приватною особою порушує принцип лояльності.

Пленум Касаційного суду підтвердив саме правовий принцип добросовісності, але не погодився з оцінкою фактів і не вбачив непрямої участі влади в цій конкретній справі [167].

Проте з плином часу цей принцип зазнав суттєвого коригування. Пленум Касаційного суду в рішенні від 9 грудня 2019 року закріпив, що застосування хитрощів представником правоохоронних органів з метою фіксації правопорушення або встановлення його виконавців не становить порушення принципу добросовісності [168]. Водночас суд визначив, що «хитрість» визнають недобросовісною лише у випадку, якщо вона призводить до порушення суттєвого права або основоположної гарантії особи, стосовно якої здійснюють розслідування [169].

На цій основі судова практика провела принципове розмежування між підбурюванням до вчинення правопорушення, що є абсолютно забороненим, і підбурюванням до надання доказів, що визнають допустимим.

У французькому кримінальному процесі визнають допустимими такі негласні методи збору електронних доказів, як створення фіктивних вебсайтів для ідентифікації підозрюваних, провадження розслідувань під псевдонімом та імітація ролі онлайн-покупця, за умови, що вони не спонукають до вчинення правопорушення, а лише виявляють уже наявну протиправну діяльність.

Аналіз принципу добросовісності доказу у французькому кримінальному судочинстві дає підстави для висновку, що відсутність прямого законодавчого закріплення цього принципу робить його гнучким відповідно до викликів, перед якими постає правова система, а з іншої сторони створює правову невизначеність, передусім у сфері електронних доказів, де технології розвиваються швидше, ніж юриспруденція [149 – 151].

3.3. Електронні докази в інших правових системах (КНР, Індія)

Допустимість цифрових доказів у *КНР* регламентована багаторічною структурою нормативних актів. До ключових нормативних актів у цій сфері належать:

– Кримінальний процесуальний закон КНР, що становить фундаментальну законодавчу основу здійснення кримінального провадження в КНР і містить ключові приписи щодо збирання та допустимості доказів у кримінальних справах. Кримінальний процесуальний кодекс КНР закріплює електронні дані як самостійний вид доказів у кримінальному провадженні (п. 8 ст. 50 КПК КНР);

– Положення про деякі питання збирання, вилучення, дослідження та оцінки електронних даних у кримінальних справах, яке було прийняте спільно Верховним Народним Судом, Верховною Народною Прокуратурою та Міністерством громадської безпеки КНР 2016 року;

– Правила збирання електронних доказів органами громадської безпеки у провадженнях щодо кримінальних справ, прийняті Міністерством громадської безпеки 2019 року на основі Положення від 2016 року, регламентує процедурний порядок роботи з електронними доказами [212; 231].

Відповідно до ст. 10 Правил Міністерства громадської безпеки КНР (МГБ КНР) 2019 року, вилучення оригінального носія інформації має найвищий пріоритет серед усіх методів збирання електронних доказів, а в разі неможливості застосовують копіювання. Правила передбачають також онлайн-екстракцію електронних даних, дистанційний онлайн-огляд та заморожування (блокування) електронних даних [231, с. 467–469].

Проблематика методу вилучення електронних доказів шляхом вилучення електронних носіїв виявилася у справі QvodPlayer [212, с. 471].. Компанія QvodPlayer орендувала чотири сервери в Beijing Wanglian Guangtong Technology Company. 2013 року в межах розслідування справи про розповсюдження порнографії з метою отримання прибутку всі сервери були цілком вилучені

поліцією, оскільки слідчі не могли на місці за стислий проміжок часу відокремити електронні дані, що стосувалися справи, від іншої інформації. Загальна місткість вилучених серверів становила 40 терабайтів.

Китайська модель є єдиною серед досліджених, яка визнає електронні дані самостійним видом доказів на рівні базового процесуального закону. Це забезпечує нормативну визначеність, якої бракує більшості інших юрисдикцій. Проте аналіз засвідчує, що цієї визначеності досягають ціною, яка, на нашу думку, є неприйнятною для правових систем, побудованих на принципі змагальності, оскільки нормативна система побудована на презумпції надійності електронних доказів, які зібрані органами досудового розслідування.

У змагальній системі сторона захисту має реальну можливість оспорити автентичність доказу, а у китайській моделі ця можливість формально є, але її обмежують інституційні умови, де обвинувачення та експертиза знаходяться в єдиній державній вертикалі.

Для порівняльного аналізу це означає, що механізм забезпечення перевірки автентичності може бути запозичений тільки за умови адаптації до змагальних стандартів.

Значну увагу законодавство спрямовує на забезпечення оперативного зберігання інформації в електронній формі, а також процедуру її надання правоохоронним органам у КНР. До ключових з них належать Закон КНР «Про кібербезпеку» від 6 січня 2017 року, Закон КНР «Про безпеку даних» від 9 січня 2021 року, Закон КНР «Про протидію відмиванню грошей» від 31 жовтня 2006 року та Закон КНР «Про контроль» від 20 березня 2018 року [173].

Зазначені нормативні акти в сукупності формують багаторівневий правовий режим, у межах якого визначають обов’язки операторів інформаційно-телекомунікаційних систем щодо збереження електронних даних, а також процесуальні підстави та процедурний порядок їх витребування вповноваженими державними органами.

Важливу роль відіграють рішення Верховного народного суду КНР, які дають орієнтири із широкого кола правових питань, зокрема щодо допустимості

електронних доказів. Такі роз'яснення слугують методологічним інструментом для судів в оцінці достовірності електронних доказів і водночас конкретизують процедурний порядок їх збирання та зберігання [204].

Однією з визначальних ознак електронних доказів, що підлягає верифікації, є їхня цілісність, яка полягає в тому, що файл має залишатися незмінним у різні часові періоди впродовж усього провадження, а всі його копії – відповідати оригіналу.

Для перевірки цілісності китайське законодавство передбачає різноманітні методи, серед яких – застосування цифрових підписів і сертифікатів, обчислення контрольних сум (геш-значень), відеофіксація процесу збирання доказів, допит свідків й інші процесуальні способи. Фіксацію шляхом гешування визнають одним із найпростіших і водночас найефективніших методів підтвердження цілісності електронного документа, оскільки збіг контрольних сум дає змогу встановити відповідність скопійованої інформації оригіналу [204].

Показовим прикладом ваги та порядку оцінки електронних доказів у КНР може слугувати кримінальне провадження за фактом убивства Чжан Сяожун, учиненого в Шанхаї (КНР) [204]. Ідентифікацію особи правопорушника та відтворення хронології події було здійснено передусім на підставі матеріалів, отриманих із систем зовнішнього відеоспостереження, розміщених у безпосередній близькості до місця події [211]. Самостійне доказове значення в цьому провадженні мали цифрові дані, вилучені з персонального комп'ютера підозрюваного, зокрема історія пошукових інтернет-запитів й активність у соціальних мережах, на підставі яких вдалося встановити мотив учинення злочину й виявити ознаки попередньої підготовки до його реалізації.

Визнання судом допустимості зазначених цифрових джерел й обрання їх за основу обвинувального вироку свідчать про сприйняття правовою системою Китайської Народної Республіки практичної цінності електронної доказової бази в кримінальному судочинстві.

Унікальна особливість китайської моделі збирання електронних доказів полягає у відсутності вимоги судового дозволу для застосування слідчих заходів,

що пов’язані з перехопленням комунікацій, які ідентичні українським негласним розшуковим діям, для яких потрібна ухвала слідчого судді.

Затвердження проведення таких заходів здійснюють у межах органу досудового розслідування. Так технічні слідчі заходи (моніторинг записів, відстеження переміщень, перехоплення комунікацій) здійснюють органи громадської безпеки на рівні міста або вище (ст. 150 Кримінального процесуального закону КНР), заморожування електронних даних і вилучення електронної пошти – органи громадської безпеки на рівні повіту або вище, а запит на надання електронних даних – керівник підрозділу, що розслідує справу [212, с. 478].

Ця модель діаметрально протилежна європейським стандартам, за якими попередній контроль незалежного органу за доступом до даних електронних комунікацій є однією з ключових гарантій захисту прав особи.

Це підтверджує практика Суду Європейського Союзу, зокрема рішення у справі H. K. (Prokuratuur) від 2 березня 2021 р. (C-746/18). Суд визнав, що доступ до збережених даних про трафік і місцезнаходження є серйозним втручанням у права, гарантовані статтями 7 і 8 Хартії основоположних прав ЄС, а тому виправданий лише для боротьби з тяжкою злочинністю. Водночас такий доступ має підлягати попередньому контролю суду або незалежного органу, який, за позицією Суду, є «третьою стороною» щодо органу, що запитує дані, не бере участі в розслідуванні та зберігає нейтральність до сторін. Принципово, що прокуратура не є таким незалежним органом, оскільки керує досудовим розслідуванням і за потреби підтримує публічне обвинувачення [197].

Аналіз національних моделей правового регулювання дає підстави для висновку, що, попри істотні відмінності між правовими системами, міжнародна практика виявляє стійку тенденцію до визнання електронних доказів повноцінними й самостійно значущими джерелами інформації в кримінальному провадженні. У всіх досліджених юрисдикціях формуються спільні принципові вимоги, що становлять загальновизнаний міжнародний стандарт допустимості: законність

отримання, автентичність, цілісність і належне забезпечення збереження електронних доказів.

Узагальнюючи, можна констатувати, що Китай демонструє одну з найбільш технологічно розвинених моделей правового регулювання електронних доказів у сучасному світі. Водночас ця модель ґрунтується на засадах посиленого державного контролю, обмеженій ролі незалежних експертів і високому рівні довіри судів до даних, отриманих від великих корпоративних провайдерів.

На відміну від держав із розвиненою змагальною моделлю кримінального процесу (зокрема США й Німеччини), де процедура автентифікації цифрових доказів передбачає активну роль сторони захисту та незалежної експертизи, китайські суди схильні презюмувати достовірність електронних матеріалів за умови дотримання формальної процедури їх збирання та посвідчення державними органами.

В Індії ключовим нормативним положенням стосовно допустимості електронних доказів став розділ 65B Закону Індії про докази 1872 року (Indian Evidence Act, 1872) [202], який встановлює, що інформація, яка міститься в електронному записі, може бути визнана допустимим доказом за умови дотримання сукупності вимог щодо цілісності та автентичності даних. Зокрема, обов’язковою передумовою допустимості є надання сертифіката, який ідентифікує електронний запис й описує спосіб його створення, що має забезпечити надійність поданих доказів.

Судова практика Індії послідовно наполягає на суворому дотриманні вимог розділу 65B.

Принциповим у цьому контексті стало рішення Верховного суду Індії у справі *Anvar P.V. v. P.K. Basheer* (2014), у якому встановлено, що електронні докази, подані без обов’язкового сертифіката відповідно до розділу 65B Закону про докази, є недопустимими [147].

Суд акцентував на безумовній обов’язковості процесуальних вимог, передбачених зазначеним розділом, включаючи надання сертифіката, що підтверджує автентичність і цілісність даних.

Це рішення змінило попередню практику, за якої електронні докази міг приймати суд без такого сертифіката, й утвердило обов'язковість дотримання формалізованих процедур як необхідної гарантії достовірності цифрових доказів у судовому провадженні.

Позицію щодо безумовної обов'язковості сертифіката за розділом 65B(4) остаточно підтвердив Верховний суд Індії у справі *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020 p.)* [152]. Зокрема, Суд роз'яснив, що якщо оригінальний електронний пристрій подають безпосередньо до суду, потреби в сертифікаті немає. В усіх інших випадках, коли електронний доказ подають як вторинний, сертифікат за розділом 65B(4) є обов'язковою передумовою допустимості. Це рішення усунуло правову невизначеність й остаточно закріпило формалізований підхід Індії до допустимості електронних доказів [152].

Зіставлення індійської моделі з іншими досліджуваними юрисдикціями дає змогу констатувати, що вона посідає крайню позицію на шкалі формалізації. Якщо британський суд у справі *R v Mawji* [226] прийняв електронний доказ на підставі змістовної оцінки без технічної верифікації, а канадська презумпція цілісності взагалі звільняє сторону від обов'язку доводити автентичність за відсутності доказів протилежного, то індійська модель вимагає формального сертифіката навіть тоді, коли автентичність доказу не оспорюється жодною зі сторін.

Для вітчизняного законодавця індійський досвід є цінним як ілюстрація ризиків надмірної формалізації, оскільки запроваджуючи вимоги до автентифікації електронних доказів у КПК України, необхідно уникнути ситуації, коли процесуальна форма превалює над змістовою достовірністю доказу.

Розділ 65B(4) Закону про докази встановлює чотири кумулятивні вимоги до змісту сертифіката: ідентифікація електронного запису й опис способу його створення; зазначення пристрою, який створив запис; підтвердження того, що протягом усього відповідного періоду пристрій функціонував належно або що неналежне функціонування не вплинуло на зміст електронного запису; зазначення того, що інформація в електронному записі відтворює дані, які вносили до пристрою у звичайному порядку.

Сертифікат підписує особа, яка обіймає відповідальну посаду стосовно функціонування пристрою або управління відповідною діяльністю. Отже, індійська модель покладає на сторону, яка подає електронний доказ, не лише обов'язок підтвердити його походження, а й обов'язок засвідчити надійність усього технологічного ланцюга створення доказу.

Саме ця особливість робить індійську модель найбільш формалізованою серед досліджених і водночас найвразливішою до критики за надмірний формалізм: достовірний електронний доказ може бути відхилений судом виключно через відсутність сертифіката, навіть якщо його автентичність не викликає сумнівів.

3.4. Порівняльний аналіз зарубіжного досвіду та перспективи вдосконалення правового регулювання електронних доказів у кримінальному процесі України

Здійснений аналіз правового регулювання електронних доказів в інших країнах дає змогу здійснити системне порівняння досліджених моделей та визначити ті елементи іноземного досвіду, які можуть бути адаптовані до національного кримінального процесуального законодавства. Порівняння здійснюють за п'ятьма критеріями, визначеними на початку цього розділу: наявність законодавчого визначення електронного доказу; процесуальний статус у системі джерел доказів; порядок автентифікації та вимоги до допустимості; розподіл тягаря доказування автентичності, а також віддаленого доступу до даних.

Аналіз законодавчого визначення електронного доказу в інших країнах засвідчує принципово різний рівень нормативної визначеності. Китайська Народна Республіка є однією з небагатьох держав, де електронні дані прямо визнані самостійним видом доказів у Законі про кримінальне судочинство КНР (2012, зі змінами 2018 року).

Канада законодавчо визначила поняття «електронний документ» у ст. 31.8 Закону Канади про докази (Canada Evidence Act). Індія закріпила правовий режим електронних записів через розділ 65B Закону про докази (Indian Evidence Act). Натомість у США, Великій Британії, Франції та Німеччині спеціального легального визначення електронного доказу немає: електронна інформація підпадає під загальні правила доказування.

Щодо процесуального статусу електронного доказу в системі джерел доказів прослідковують три підходи до визначення місця електронних доказів у кримінальному процесі:

1) визнання електронних доказів самостійним видом доказів (КНР);

2) включення електронних доказів до наявних категорій без виокремлення в самостійний вид (США, де електронний доказ підпадає під загальні правила FRE; Велика Британія; Франція; Німеччина);

3) гібридний підхід, за якого електронні записи отримують спеціальний правовий режим, залишаючись у межах загальної системи доказів (Канада з презумпцією цілісності; Індія з вимогою сертифікації за розділом 65B).

У цій системі Україна формально належить до другого підходу (електронні докази кваліфікують як документи за ст. 99 КПК), проте судова практика фактично рухається в напрямі першого, оскільки Верховний Суд у справі № 569/1908/23 прямо назвав електронні (цифрові) докази основними доказами в провадженнях про злочини проти основ національної безпеки [96].

Розрив між нормою і практикою є непритаманним українській правовій доктрині, і на нашу думку, потребує усунення шляхом імплементації пропозиції І. А. Смаль та І. Г. Каланчі стосовно доповнення ч. 2 ст. 84 КПК України електронними доказами як самостійним джерелом доказів.

У контексті здійсненого нами порівняльного аналізу зарубіжних моделей зазначена пропозиція потребує доповнення положеннями про функціональні ознаки електронного доказу (запропонований у підрозділі 1.1 функціональний підхід до дефініції) та про особливості оцінки електронних доказів, створених або

модифікованих засобами штучного інтелекту (запропонована ст. 99-3 КПК України).

Порядок автентифікації та вимоги до допустимості виявляє найсуттєвіші розбіжності між досліджуваними правовими системами. Американська модель побудована як каскад послідовних перевірок: релевантність, автентифікація, перевірка, правило найкращого доказу, баланс доказової цінності й упередженості.

Така архітектура забезпечує високий стандарт надійності, однак створює значне процесуальне навантаження на сторону, яка подає доказ, і залежить від рівня підготовки суду до роботи з електронними доказами.

Крім того, з 2017 року правила 902(13)–(14) FRE запровадили механізм самоавтентифікації електронних записів за умови наявності сертифікації кваліфікованого спеціаліста, що суттєво спрощує процедуру для певних категорій доказів.

Канадська модель, навпаки, знижує поріг автентифікації завдяки презумпції цілісності системи електронних документів (ст. 31.3 Canada Evidence Act). Ця презумпція діє за відсутності доказів протилежного й може ґрунтуватися на належному функціонуванні комп'ютерної системи, створенні документа стороною-опонентом або створенні документа у звичайному процесі діяльності третьою особою.

Такий підхід є прагматичним, проте містить ризик недостатньої перевірки автентичності у випадках, коли сторона захисту не має ресурсів для спростування презумпції.

Індійська модель є найбільш формалізованою в частині вимог до допустимості. Розділ 65B(4) Закону про докази вимагає обов'язкового сертифіката, що ідентифікує електронний запис й описує спосіб його створення. Судова практика Верховного суду Індії послідовно дотримується позиції про безумовну обов'язковість такого сертифіката. Перевагою цього підходу є правова визначеність; недоліком – ризик виключення достовірних доказів за формальними підставами.

Британський підхід є найгнучкішим: суд за ст. 78 PACE має дискреційне повноваження відхилити будь-який доказ, допущення якого матиме несприятливий вплив на справедливість провадження. Відповідно до справи R v Mawji [226], змістова оцінка доказу та його кореляція з іншими матеріалами справи переважають над вимогою формалізованої автентифікації.

Франція та Німеччина, які належать до континентальної правової традиції, не передбачають окремих процедур автентифікації електронних доказів. У Франції діє принцип свободи доказів, обмежений доктриною добросовісності (loyauté de la preuve), яка не має прямого законодавчого закріплення та розвивається виключно через судову практику Касаційного суду.

У Німеччині принцип вільної оцінки доказів судом доповнюється доктриною заборон використання доказів, що створює систему негативних обмежень: суд оцінює доказ вільно, але має виключити його в разі порушення конституційних гарантій, зокрема права на конфіденційність інформаційно-технічних систем, сформульованого Федеральним конституційним судом у рішенні від 27 лютого 2008 року.

Україна наразі не має жодного із зазначених механізмів автентифікації електронних доказів на рівні КПК України. Це означає, що суди вирішують питання автентичності без законодавчих орієнтирів, що призводить до непослідовності судової практики, виявленої під час аналізу судової практики в попередніх підрозділах.

Доцільним видається закріплення в КПК України вимог до автентифікації електронних доказів, що передбачали б обов’язковість фіксації геш-суми під час вилучення (за аналогією з ДСТУ ISO/IEC 27037:2017, який вже імплементовано в Україні), процедуру підтвердження ланцюга збереження (chain of custody) і можливість залучення спеціаліста для верифікації цілісності.

Також виявлено два підходи щодо розподілу тягаря доказування автентичності. Порівняння дало змогу виокремити два принципово відмінні підходи. У системах загального права (США, Канада, Велика Британія) тягар первинного доведення автентичності покладається на сторону, яка подає доказ. У

континентальних системах (Франція, Німеччина) це питання вирішують у межах загальної суддівської оцінки. КНР та Індія представляють проміжний варіант, оскільки в Індії формалізована вимога сертифікації фактично покладає тягар на сторону, яка подає доказ, а в КНР державні органи забезпечують достовірність через процедуру посвідчення. В Україні це питання не врегульовано, що створює невизначеність стосовно того, хто саме – сторона обвинувачення, сторона захисту чи суд – має ініціювати перевірку автентичності електронного доказу.

Актуальності набуває проблема розподілу тягаря доказування в контексті доказів, створених або модифікованих засобами штучного інтелекту. У підрозділі 2.4 встановлено, що в доктрині та правозастосуванні США вже формується двоступеневий підхід, коли спершу опонент повинен подати докази того, що електронний об’єкт може бути дипфейком, і лише після цього обов’язок підтвердити автентичність переходить до сторони, яка доказ пред’явила, що свідчить про нові стандарти тягаря доказування.

На підставі узагальнення здійсненого порівняльного аналізу констатуємо, що для України найперспективнішою є комбінована модель регулювання електронних доказів, яка поєднує елементи формалізованого (чіткі законодавчі критерії допустимості й автентифікації) і прагматичного (суддівська дискреція в оцінці доказу) підходів у межах наднаціонального нормативного каркаса транскордонного доступу.

Такий вибір зумовлений не лише стратегічним курсом України на набуття повноправного членства в Європейському Союзі й необхідністю узгодження національного законодавства із законодавством ЄС у галузі кримінального судочинства, а й об’єктивними потребами правозастосування в умовах збройного конфлікту, коли електронні докази (дані з месенджерів, супутникові зображення, відеозаписи з безпілотних літальних апаратів) набувають вирішального значення для документування злочинів.

Порівняльний аналіз засвідчує, що в усіх досліджених юрисдикціях дистанційний доступ до інформаційних систем сформувався як самостійний процесуальний інститут. Його поява зумовлена широким використанням

шифрування, хмарного зберігання та анонімізувальних технологій, які роблять традиційне вилучення фізичних носіїв недостатнім. Водночас дистанційне проникнення до інформаційної системи є одним із найінтрузивніших втручань у право на приватність, що зумовило диференціацію моделей його санкціонування.

У США дистанційний обшук за Rule 41(b)(6) санкціонує суддя-магістрат у двох випадках: приховування місцезнаходження пристрою технологічними засобами й ураження комп'ютерних систем у п'яти або більше округах.

Німеччина встановила найвищий стандарт: Online-Durchsuchung за § 100b StPO допускається лише щодо злочинів із вичерпного каталогу, за санкцією колегії трьох суддів й абсолютною забороною збирання даних «ядра приватного життя» – на підставі нового основоположного права, сформульованого Федеральним конституційним судом у рішенні від 27 лютого 2008 року. Франція обмежила captation des données informatiques (ст. 706-102-1 CPP) провадженнями щодо організованої злочинності й тероризму із санкцією слідчого судді; без судового підтвердження протягом двадцяти чотирьох годин здобуті дані не можуть бути використані. Велика Британія застосовує механізм «подвійного замка»: ордер на equipment interference видає Державний секретар, він набуває чинності лише після затвердження Судовим комісаром. Канада залишається єдиною юрисдикцією без окремого інституту: віддалений доступ авторизується через «загальний ордер».

Зіставлення цих моделей з українським законодавством виявляє суттєву прогалину в національному законодавстві. КПК України передбачає НСРД, зокрема зняття інформації з транспортних телекомунікаційних мереж (ст. 263), зняття інформації з електронних інформаційних систем (ст. 264) й обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267), проте не містить окремого інституту дистанційного проникнення до інформаційних систем.

Вважаємо, що запровадження такого інституту в національному законодавстві має ґрунтуватися на трьох принципах, серед яких: обов'язковість попередньої судової санкції; обмеження кола злочинів, щодо яких захід допускається; заборона або обов'язок негайного видалення даних, що належать до сфери приватного життя і не пов'язані з предметом розслідування. Ці принципи

мають бути враховані під час удосконалення відповідних положень КПК України, зокрема шляхом конкретизації процесуальних гарантій під час проведення НСРД, пов'язаних із доступом до електронних інформаційних систем.

Уваги потребує проблематика транскордонного доступу до електронних доказів. Регламент (ЄС) 2023/1543, що починають застосовувати із 18 серпня 2026 року, запроваджує European Production Order – механізм прямого звернення судового органу однієї держави-члена до постачальника послуг в іншій державі-члені зі строком виконання 10 днів, а в невідкладних випадках – 8 годин.

Україна, не маючи доступу до цього механізму та не завершивши ратифікацію Другого додаткового протоколу до Будапештської конвенції (підписаного 2022 року), вимушена використовувати традиційний механізм міжнародної правової допомоги, строки виконання якого інколи вимірюються місяцями. Подолання цього розриву потребує не лише завершення ратифікаційних процедур, а й імплементації в КПК України процесуального механізму прямого звернення до іноземних постачальників послуг електронних комунікацій.

Висновки до розділу 3

У третьому розділі здійснено порівняльно-правовий аналіз регулювання електронних доказів у кримінальному процесі країн англо-саксонської, романо-германської та інших правових систем, що дає змогу сформулювати такі висновки.

1. Встановлено, що в англо-саксонській правовій системі сформовано три відмінні моделі регулювання електронних доказів: формалізована американська, канадська з презумпцією цілісності та прагматична британська. Кожна з них має самостійну цінність для рецепції в українському законодавстві. Водночас аналіз практики цих юрисдикцій виявив додаткові ризики електронних доказів, зокрема селективність відбору, деконтекстуалізація, непрозорість інструментів обробки та комунікаційний розрив між технічними експертами й учасниками судового процесу.

2. Здійснено порівняльну систематизацію моделей санкціонування дистанційного доступу до інформаційних систем у країнах романо-германської правової системи: триступенева німецька модель (з обов'язковою колегією суддів й абсолютною забороною збирання даних «ядра приватного життя»); французька модель (з обмеженням до тяжких злочинів та обов'язковою санкцією слідчого судді). Виокремлено наднаціональний рівень регулювання електронних доказів на рівні ЄС (механізми European Production Order і European Preservation Order для транскордонного збирання електронних доказів). Обґрунтовано, що для України найпридатнішими є німецький принцип захисту «ядра приватного життя» та французький принцип обмеження дистанційного доступу виключно тяжкими злочинами, натомість механізми ЄС є зразком для майбутньої гармонізації після набуття членства в Європейському Союзі.

3. Аргументовано позицію неможливості рецепції правових систем правових механізмів Китайської Народної Республіки та Республіки Індія. Китайський механізм забезпечення достовірності електронних доказів побудований на презумпції надійності, що ґрунтується на довірі до державних органів, і функціонує в принципово відмінному конституційно-правовому контексті — без притаманних національному та європейському кримінальному процесу гарантій змагальності й незалежного судового контролю. З огляду на це китайська модель не може слугувати джерелом рецепції для України, правопорядок якої орієнтований на європейські стандарти захисту прав особи; її вивчення зберігає лише порівняльно-аналітичну цінність як приклад принципово іншого підходу. Натомість індійська модель обов'язкової сертифікації електронних доказів демонструє ризики надмірної формалізації: достовірний електронний доказ може бути відхилений судом виключно через відсутність формального сертифіката, навіть якщо його автентичність не оспорюють. Ці ризики слід ураховувати під час запровадження вимог до автентифікації електронних доказів у КПК України.

4. Обґрунтовано комбіновану модель регулювання електронних доказів для України, що поєднує: формалізований елемент (чіткі законодавчі критерії допустимості й автентифікації за зразком США та Канади); прагматичний елемент

(суддівська дискреція в оцінці доказу за сутністю за зразком Великої Британії); наднаціональний каркас транскордонного доступу (механізми European Production Order і European Preservation Order за зразком ЄС). Засвідчено доцільність запровадження в КПК України інституту дистанційного проникнення до інформаційних систем на трьох спільних принципах: 1) обов'язковість попередньої судової санкції; 2) обмеження кола злочинів вичерпним переліком тяжких й особливо тяжких кримінальних правопорушень; 3) заборона збирання даних «ядра приватного життя». Виявлено критичний розрив між інструментарієм транскордонного доступу, доступним державам – членам ЄС, і можливостями України, подолання якого потребує ратифікації Другого додаткового протоколу до Будапештської конвенції 2022 року й імплементації в КПК України процесуального механізму прямого звернення до іноземних провайдерів послуг електронних комунікацій.

ВИСНОВКИ

У дисертації здійснено комплексне дослідження теоретичних, правових і прикладних аспектів використання електронних доказів у кримінальному провадженні, що дало змогу сформулювати науково обґрунтовані пропозиції з удосконалення відповідного процесуального регулювання. За результатами здійсненого дослідження сформовано такі висновки.

1. Сформульовано авторське функціональне визначення електронного доказу як інформації в електронній формі, що створена, збережена, передана або відображена за допомогою електронних пристроїв, систем чи мереж, містить відомості про обставини, що мають значення для кримінального провадження, і може бути використана як доказ за умови її отримання та перевірки в порядку, передбаченому КПК України. Обґрунтовано необхідність виокремлення електронного доказу як самостійного джерела доказів і запропоновано доповнити ч. 2 ст. 84 КПК України електронними доказами як самостійним процесуальним джерелом.

2. Виокремлено й систематизовано шість специфічних ознак електронних доказів, що відрізняють їх від традиційних джерел: нематеріальність (зміст доказу не тотожний матеріальному носієві та не зникає з його знищенням); динамічність (здатність змінюватися без видимих слідів, що вимагає невідкладної фіксації); відтворюваність (необмежене копіювання без втрати змісту, що знімає проблему «єдиного оригіналу»); залежність від технічних засобів (сприйняття доказу неможливе без програмно-апаратного забезпечення та спеціальних знань); відсутність жорсткої прив’язки до матеріального носія (одна й та сама інформація може одночасно існувати на кількох носіях або у хмарному середовищі); наявність метаданих (супутні технічні дані про час, джерело й історію змін). Доведено, що сукупність цих ознак унеможливлює повне зведення електронного доказу до документа чи речового доказу й зумовлює потребу в окремому процесуальному режимі його збирання, фіксації та оцінки. Окремо обґрунтовано виокремлення

метаданих як ознаки із самостійним доказовим значенням («мовчазних свідків» електронного доказу).

3. Запропоновано координатну авторську класифікацію електронних доказів за п’ятьма взаємодоповнюваними критеріями, кожен з яких поділено на види: за способом створення інформації (створені людиною; створені комп’ютером; комбіновані; створені штучним інтелектом); за процесуальним режимом отримання (безпосередньо вилучені; отримані через тимчасовий доступ до речей і документів; отримані через негласні слідчі (розшукові) дії; отримані через міжнародне співробітництво); за процесуальним статусом носія (локальні; мережеві; локально-мережеві; транзитні); за рівнем процесуальної верифікованості (самоверифіковані; технічно верифіковані; експертно підтверджені; презумптивно верифіковані); за рівнем втручання в право на повагу до приватного життя (без втручання; з мінімальним, середнім і високим рівнями втручання). На відміну від наявних одновимірних класифікацій, координатний характер запропонованої моделі дає змогу одночасно схарактеризувати кожен електронний доказ за всіма п’ятьма критеріями, а їх комбінація визначає процесуальний маршрут роботи з доказом – від виявлення до представлення суду – і слугує орієнтиром у виборі способу збирання, перевірки автентичності й оцінки допустимості.

4. Встановлено, що КПК України, на відміну від ЦПК (ст. 100), ГПК (ст. 96) та Кодексу адміністративного судочинства (ст. 99), не містить ані визначення поняття «електронний доказ», ані спеціальних норм щодо порядку його збирання, фіксації та оцінки, унаслідок чого електронні докази на практиці відносять до категорії документів (ч. 2 ст. 99 КПК). Доведено, що судова практика об’єктивно випередила нормотворення: Верховний Суд фактично вдається до розширювального тлумачення, визнавши, зокрема, електронні (цифрові) докази основними в провадженнях про злочини проти основ національної безпеки (справа № 569/1908/23), і тим самим легітимізує вид доказів, якого чинний процесуальний закон не знає. Аналіз міжнародних актів (Конвенції Ради Європи про кіберзлочинність з Другим додатковим протоколом 2022 року, Регламенту (ЄС) 2023/1543 і Директиви (ЄС) 2023/1544, стандарту ISO/IEC 27037:2016,

імплементованого в Україні як ДСТУ ISO/IEC 27037:2017) засвідчив наявність розвинутої багаторівневої міжнародної нормативної бази, орієнтири якої (диференціація процесуальних гарантій залежно від категорії даних, єдині стандарти поводження з доказами, механізми транскордонного доступу) доцільно врахувати під час формування національної моделі регулювання.

5. Запропоновано процесуально-правову концепцію трансформації електронного об'єкта на доказ через чотири послідовні технологічно зумовлені операції: 1) відтворення електронної інформації засобами програмно-апаратного забезпечення; 2) аналіз її атрибутів і метаданих; 3) описове закріплення в процесуальному документі; 4) вилучення або копіювання з гарантією цілісності через хешування та фіксацію ланцюга поводження (chain of custody). На відміну від криміналістично-технічних моделей збирання електронних доказів, запропонована модель має процесуально-правову природу й визначає мінімальний стандарт належної фіксації, недотримання якого тягне недопустимість доказу за ч. 1 ст. 87 КПК України.

6. На підставі узагальнення правових позицій ККС ВС обґрунтовано доктринальне положення про презумпцію допустимості електронної форми доказу, згідно з яким електронна форма не є самостійною підставою для визнання доказу недопустимим, а тягар доведення підстав недопустимості (порушення процесуального порядку отримання) покладено на сторону, яка оспорює доказ. Зазначена презумпція ґрунтується на позиціях Верховного Суду, відповідно до яких допустимість електронного документа не можна заперечувати лише через його електронну форму, а всі ідентичні за змістом примірники електронного документа розглядають як оригінали (постанови Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к та від 25 вересня 2023 року у справі № 208/2160/18).

7. Обґрунтовано концепцію динамічної природи достовірності електронного доказу: на відміну від традиційного розуміння достовірності як властивості, яку встановлюють одноразово в момент отримання доказу, доведено, що достовірність електронного доказу верифікують на кожному наступному етапі провадження

через ланцюг поводження (chain of custody) – від виявлення до дослідження в суді, що корелює з нормами статей 87, 91, 95 КПК України. Встановлено також, що належність електронного доказу поширюється не лише на його змістову складову, а й на метадані («мовчазні свідки» електронного доказу), які можуть самостійно встановлювати обставини, що належать до предмета доказування за ст. 91 КПК України (зокрема час, місце й обстановку вчинення кримінального правопорушення); тож доцільною видається практична вимога фіксувати під час збирання не лише зміст електронного об’єкта, а й повний масив його метаданих.

8. Розроблено класифікацію листування в месенджерах як окремого виду електронних доказів за вісьмома критеріями: кількістю учасників; рівнем доступу; можливістю розміщення контенту; етапом створення; джерелом походження; форматом; змістово-інформаційною складовою; способом формування відповідей. На відміну від класифікацій цифрових слідів, орієнтованих переважно на технічні характеристики, запропонована класифікація має процесуальне спрямування і безпосередньо впливає на вибір способу збирання, методу фіксації та критеріїв оцінки допустимості конкретного виду листування. Доведено, що листування в месенджерах є найпоширенішим видом електронних доказів (засвідчили 78,5 % опитаних працівників прокуратури), а в кримінальних провадженнях про злочини проти основ національної безпеки воно набуло статусу основного джерела доказової інформації, що підтверджує правова позиція Верховного Суду у справі № 569/1908/23.

9. Запропоновано доповнити КПК України статтею 99-3 «Особливості оцінки електронних доказів, створених або модифікованих засобами штучного інтелекту», що передбачає три взаємопов’язані правила: 1) обов’язок учасника провадження розкривати факт використання технологій штучного інтелекту під час створення чи обробки доказу; 2) перерозподіл тягаря доказування автентичності на сторону, що подала доказ, у разі заявлення іншою стороною обґрунтованих сумнівів; 3) недопустимість електронного доказу штучного походження, не розкритого стороною, що його подала. Необхідність такого регулювання підтверджують результати анкетування: 77,7 % опитаних працівників прокуратури сприймають

докази, згенеровані штучним інтелектом, як актуальну загрозу, а 63,1 % констатують, що тягар доказування автентичності де-факто вже покладено на сторону, яка подає доказ.

10. На підставі дослідження англо-саксонської правової системи (Сполучені Штати Америки, Канада, Велика Британія) виокремлено три відмінні моделі регулювання електронних доказів: формалізовану американську, у якій автентифікацію здійснюють за кодифікованими Федеральними правилами доказування (правило 901) з можливістю самоавтентифікації електронних записів (правила 902(13)–(14)); канадську, що ґрунтується на законодавчо закріпленій презумпції цілісності системи електронних документів (ст. 31.3 Canada Evidence Act) і знижує доказове навантаження на сторону, яка подає доказ; прагматичну британську, у якій допустимість визначають дискреційним повноваженням суду за критерієм справедливості провадження (ст. 78 PACE). Аналіз практики цих юрисдикцій (зокрема справи R. v. Jamali) додатково виявив ризики електронних доказів – селективність відбору, деконтекстуалізацію, непрозорість інструментів обробки та комунікаційний розрив між технічними експертами й учасниками процесу, які слід ураховувати в національному регулюванні.

11. На підставі дослідження романо-германської правової системи (Франція, Німеччина) та нормативної бази Європейського Союзу здійснено порівняльну систематизацію моделей санкціонування дистанційного доступу до інформаційних систем: німецької (Online-Durchsuchung за § 100b StPO – за санкцією колегії трьох суддів з абсолютною забороною збирання даних «ядра приватного життя»), французької (захоплення даних за ст. 706-102-1 CPP – лише щодо тяжких злочинів і тероризму, за санкцією слідчого судді) та наднаціональної (механізми European Production Order і European Preservation Order Регламенту (ЄС) 2023/1543). Обґрунтовано, що для України найпридатнішими є німецький принцип захисту «ядра приватного життя» та французький принцип обмеження дистанційного доступу виключно тяжкими злочинами, натомість механізми ЄС є зразком для гармонізації після набуття членства в Європейському Союзі.

12. На підставі дослідження правових систем Китайської Народної Республіки та Республіки Індія аргументовано межі рецепції закордонного досвіду. Встановлено, що китайська модель забезпечення достовірності електронних доказів, побудована на презумпції надійності, що ґрунтується на довірі до державних органів, функціонує в принципово відмінному конституційно-правовому контексті - без властивих національному та європейському кримінальному процесу гарантій змагальності й незалежного судового контролю - і тому не може слугувати джерелом рецепції для України. Індійська модель обов'язкової сертифікації демонструє ризики надмірної формалізації: достовірний доказ може бути відхилено лише через відсутність сертифіката, навіть якщо автентичність не оспорюють, чого слід уникати під час запровадження вимог до автентифікації в КПК України

13. Обґрунтовано комбіновану модель регулювання електронних доказів для України, що поєднує формалізований елемент (чіткі законодавчі критерії допустимості й автентифікації за зразком США та Канади), прагматичний елемент (суддівська дискреція в оцінці доказу за сутністю за зразком Великої Британії) і наднаціональний каркас транскордонного доступу (механізми European Production Order і European Preservation Order за зразком ЄС). Запропоновано запровадити в КПК України інститут дистанційного проникнення до інформаційних систем на трьох принципах: обов’язковість попередньої судової санкції; обмеження кола злочинів вичерпним переліком тяжких та особливо тяжких кримінальних правопорушень; заборона збирання даних «ядра приватного життя». Виявлено критичний розрив між інструментарієм транскордонного доступу держав – членів ЄС і можливостями України, подолання якого потребує ратифікації Другого додаткового протоколу до Будапештської конвенції 2022 року й імплементації в КПК України механізму прямого звернення до іноземних провайдерів послуг електронних комунікацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алєксєєва-Процюк Д. О., Брисковська 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.

2. Ахтирська Н. М., Костюченко О. Ю. Процесуальні та організаційні аспекти збору електронних доказів під час міжнародного співробітництва. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2022. Вип. 72 (2). С. 192–198. URL: http://nbuv.gov.ua/UJRN/nvuzhpr_2022_72(2)__33

3. Бернхем В. Вступ до права та правової системи США / пер. з англ. Київ : Україна, 1999. 554 с.

4. Біленчук П. Д., Гель А. П., Семаков Г. С. Криміналістична тактика і методика розслідування окремих видів злочинів : навч. посіб. для студ. вищ. навч. закл. Київ : МАУП, 2007. 512 с.

5. Боннер О. Т. Науково-технічний прогрес і розвиток російського процесуального законодавства та судової практики. *Право України.* 2011. № 10. С. 45–62.

6. Вапнярчук В. В. Загальна характеристика властивостей доказів та їх розмежування між собою. *Держава і право. Серія «Юридичні науки».* 2015. Вип. 67. С. 361–375.

7. Великий тлумачний словник сучасної української мови : 250000 / уклад. та голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. Т. VIII. 1728 с.

8. Вернидубов І., Белікова С. Електронні докази: поняття, особливості та проблеми щодо дослідження їх судом. *European Political and Law Discourse.* 2018. Vol. 5. Issue 2. С. 299–305.

9. 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.

10. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів : метод. рек. / [авт. кол.: А. В. Захарко, А. Г. Гаркуша, В. В. Рогальська та ін.]. Дніпро : Дніпр. держ. ун-т внутр. справ, 2019. 73 с.

11. Вирок Бердичівського міськрайонного суду Житомирської області від 24 лют. 2025 р. у справі № 274/6556/23, провадження № 1-кп/0274/331/25. URL: https://reyestr.court.gov.ua/Review/125349423

12. Вирок Болградського районного суду Одеської області від 2 берез. 2026 р. у справі № 497/430/26, провадження № 1-кп/497/125/26. URL: https://reyestr.court.gov.ua/Review/134463371

13. Вирок Вознесенівського районного суду м. Запоріжжя від 12 берез. 2025 р. у справі № 335/2022/25, провадження № 1-кп/335/569/2025. URL: https://reyestr.court.gov.ua/Review/125757379

14. Вирок Дніпровського районного суду м. Запоріжжя від 10 груд. 2024 р. у справі № 334/4126/24, провадження № 1-кп/334/554/24. URL: https://reyestr.court.gov.ua/Review/123645637

15. Вирок Дніпровського районного суду м. Запоріжжя від 13 груд. 2024 р. у справі № 334/2045/24, провадження № 1-кп/334/476/24. URL: https://reyestr.court.gov.ua/Review/123773129

16. Вирок Дніпровського районного суду м. Запоріжжя від 16 серп. 2024 р. у справі № 334/9999/23, провадження № 1-кп/334/368/24. URL: https://reyestr.court.gov.ua/Review/121038824

17. Вирок Дніпровського районного суду м. Запоріжжя від 29 листоп. 2024 р. у справі № 334/5278/24, провадження № 1-кп/334/588/24. URL: https://reyestr.court.gov.ua/Review/123523319

18. Вирок Дніпровського районного суду м. Києва від 25 лип. 2024 р. у справі № 755/2508/23., провадження № 1-кп/755/92/24. URL: https://reyestr.court.gov.ua/Review/120590672

19. Вирок Дніпровського районного суду м. Києва від 9 груд. 2025 р. у справі № 755/23443/25, провадження № 1-кп/755/1959/25. URL: https://reyestr.court.gov.ua/Review/132712305

20. Вирок Жовківського районного суду Львівської області від 8 берез. 2024 р. у справі № 461/3477/22, провадження № 1-кп/444/44/2024. URL: https://reyestr.court.gov.ua/Review/117517325

21. Вирок Івано-Франківського міського суду Івано-Франківської області від 11 черв. 2024 р. у справі № 344/8521/23, провадження № 1-кп/344/414/24. URL: https://reyestr.court.gov.ua/Review/119672102

22. Вирок Івано-Франківського міського суду Івано-Франківської області від 29 квіт. 2025 р. у справі № 344/7425/16-к, провадження № 1-кп/344/41/25. URL: https://reyestr.court.gov.ua/Review/126963183

23. Вирок Івано-Франківського міського суду Івано-Франківської області від 23 груд. 2025 р. у справі № 344/19190/25, провадження № 1-кп/344/1443/25. URL: https://reyestr.court.gov.ua/Review/132833459

24. Вирок Ізяславського районного суду Хмельницької області від 18 верес. 2025 р. у справі № 685/1189/23, провадження № 1-кп/675/13/2025. URL: https://reyestr.court.gov.ua/Review/130297064

25. Вирок Ковельського міськрайонного суду Волинської області від 5 квіт. 2024 р. у справі № 159/4835/19, провадження № 1-кп/159/103/24. URL: https://reyestr.court.gov.ua/Review/118179256

26. Вирок Коломийського міськрайонного суду Івано-Франківської області від 19 трав. 2025 р. у справі № 346/1275/25, провадження № 1-кп/346/504/25. URL: https://reyestr.court.gov.ua/Review/127481243

27. Вирок Нововоронцовського районного суду Херсонської області від 24 берез. 2026 р. у справі № 954/674/25, провадження № 1-кп/954/46/26. URL: https://reyestr.court.gov.ua/Review/135081498

28. Вирок Охтирського міськрайонного суду Сумської області від 25 груд. 2023 р. у справі № 583/2443/23, провадження № 1-кп/583/245/23. URL: https://reyestr.court.gov.ua/Review/115896439

29. Вирок Первомайського міськрайонного суду Миколаївської області від 12 берез. 2025 р. у справі № 484/4660/24, провадження № 1-кп/484/123/25. URL: https://reyestr.court.gov.ua/Review/125772125

30. Вирок Роздільнянського районного суду Одеської області від 29 лют. 2024 р. у справі № 511/563/19, провадження № 1-кп/511/11/24. URL: https://reyestr.court.gov.ua/Review/117324337

31. Вирок Соснівського районного суду м. Черкаси від 23 січ. 2026 р. у справі № 712/11916/24, провадження № 1-кп/712/291/26. URL: https://reyestr.court.gov.ua/Review/133807590

32. Вирок Тернопільського міськрайонного суду Тернопільської області від 11 верес. 2023 р. у справі № 607/4566/23, провадження № 1-кп/607/1256/2023. URL: https://reyestr.court.gov.ua/Review/113441939

33. Вирок Тернопільського міськрайонного суду Тернопільської області від 20 жовт. 2023 р. у справі № 607/18811/23, провадження № 1-кп/607/2194/2023. URL: https://reyestr.court.gov.ua/Review/114602814

34. Вирок Турківського районного суду Львівської області від 18 лип. 2024 р. у справі № 458/465/22, провадження № 1-кп/458/7/2024. URL: https://reyestr.court.gov.ua/Review/120455406

35. Вирок Тисменицького районного суду Івано-Франківської області від 5 квіт. 2023 р. у справі № 352/1477/21, провадження № 1-кп/352/52/23. URL: https://reyestr.court.gov.ua/Review/110016374

36. Вирок Золотоніського міськрайонного суду Черкаської області від 28 лют. 2023 р. у справі № 711/4173/22, провадження № 1-кп/695/190/23. URL: https://reyestr.court.gov.ua/Review/109268371

37. Вирок Херсонського міського суду Херсонської області від 19 верес. 2025 р. у справі № 766/10850/24, провадження № 1-кп/766/50/25. URL: https://reyestr.court.gov.ua/Review/130398458

38. Вирок Хмельницького міськрайонного суду Хмельницької області від 7 груд. 2023 р. у справі № 686/32668/23, провадження № 1-кп/686/1668/23. URL: https://reyestr.court.gov.ua/Review/115472985

39. Вирок Холодногірського районного суду м. Харкова від 25 листоп. 2025 р. у справі № 642/5920/25, провадження № 1кп/642/594/25. URL: https://reyestr.court.gov.ua/Review/132039938

40. Вирок Хортицького районного суду м. Запоріжжя від 14 серп. 2024 р. у справі № 337/862/23, провадження № 3/335/1916/2024. URL: https://reyestr.court.gov.ua/Review/121038828

41. Вирок Шевченківського районного суду м. Полтави від 24 жовт. 2024 р. у справі № 554/7727/24, провадження № 1-кп/554/1218/2024. URL: https://reyestr.court.gov.ua/Review/122564892

42. Висновок № 26 (2023) Консультативної ради європейських суддів «Рух уперед: використання допоміжних технологій у судочинстві» від 1 груд. 2023 р. URL: https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7

43. Гаран О. В. Спеціальні ознаки електронних доказів у площині когнітивного консонансу. *Вісник Одеського національного університету. Серія «Правознавство».* 2019. Т. 24. Вип. 1. С. 125–136. URL: http://nbuv.gov.ua/UJRN/Vonu_prav_2019_24_1_16

44. Главюк І. В. Апеляційна скарга з галюцинаціями штучного інтелекту: висновки на майбутнє з одного кейсу у кримінальному провадженні. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2026. Т. 5. № 93. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/355844

45. Гонгало С. Й. Електронні документи як об’єкти судової техніко-криміналістичної експертизи та їх класифікація. *Адвокат.* 2013. № 1 (148). С. 33–36. URL: http://nbuv.gov.ua/UJRN/adv_2013_1_8

46. Гора І. В., Колесник В. А., Попович І. І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2024. Вип. 85. Т. 4. С. 63–70. DOI: https://doi.org/10.24144/2307-3322.2024.85.4.9

47. Господарський процесуальний кодекс України : Закон України від 6 листоп. 1991 р. № 1798-XII. URL: https://zakon.rada.gov.ua/go/1798-12

48. Гусєв О. Ю. «Електронні» чи «цифрові»: термінологічні аспекти впровадження досягнень науково-технічного прогресу у законодавство України. ІТ-право: проблеми та перспективи розвитку в Україні : матеріали ІІ Міжнар. наук.-практ. конф. (Львів, 17 листоп. 2017 р.). Львів, 2017. С. 61–65.

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

50. 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. DOI: 10.37025/1992-4437/2020-33-1-37

51. Гуцалюк М. В., Хахановський В. Г. Використання електронних (цифрових) доказів у кримінальному провадженні : навч.-метод. посіб. Київ : НАВС, 2020. 10 с.

52. Дзерин М. М. Узагальнення судової практики розгляду клопотань про тимчасовий доступ до речей і документів за 2023 рік. Ямпіль, 24 квіт. 2024 р. URL: https://yam.vn.court.gov.ua/sud0231/an/122

53. Денисов С. Ф., Філей Ю. В. Порнографічні фейки: проблеми протидії. *Вісник Пенітенціарної асоціації України.* 2020. № 2. С. 94–102. URL: https://www.researchgate.net/publication/343637479_Pornograficni_fejki_problemi_protidii

54. Дєєв М. В. Достатність доказів у кримінальному процесі України : дис. … канд. юрид. наук : 12.00.09. Київ, 2008. 218 с.

55. Докази та доказування у кримінальному провадженні : навч. посіб. / [Р. І. Благута, Ю. В. Гуцуляк, О. М. Дуфенюк та ін.]. Львів : ЛьвДУВС, 2018. 272 с.

56. Докази і доказування в кримінальному судочинстві / за заг. ред. В. П. Пєткова. Київ : Професіонал, 2024. 406 с.

57. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT). Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Чинний від 2019-01-01. Вид. офіц. Київ : УкрНДНЦ, 2018. VI. 31 с.

58. Електронні докази в кримінальному процесі: перспективи та практичні аспекти. *Прес-центр Верховного Суду*. 2025. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1838651/

59. Запотоцький А. П. Документи як процесуальні джерела доказів у кримінальному судочинстві : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 26 с.

60. Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. *Українське право*. 2018. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazyudoskonalennya_zmin_do_protsesualnogo_zakonodavstva

61. Каламайко А. Ю. Місце електронних засобів доказування та окремі питання їх використання в цивільному процесі. *Право та інновації.* 2015. № 2 (10). С. 127–132.

62. 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.

63. Кіберзлочинність та електронні докази: суддя ВС розповіла про оцінку електронних доказів у кримінальному провадженні. *Прес-центр Верховного Суду*. 2024. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1594957/

64. Кіберполіція припинила незаконну діяльність 20 онлайн-обмінників. *Департамент Кіберполіції Національної поліції України.* URL: https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-nezakonnu-diyalnist--onlajn-obminnykiv-8653/

65. Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. Вип. 161. С. 202–214. DOI: https://doi.org/10.21564/2414-990X.161.278117

66. Ковальчук С. О. Умови допустимості речових доказів у кримінальному провадженні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2015. Вип. 35. Ч. ІІ. Т. 3. С. 132–135.

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

68. Кодекс суддівської етики : затвердж. XVIII З'їздом суддів України 18 верес. 2024 р. URL:

https://court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Kodeks_suddivskoji_etyky_18_09_2024.pdf

69. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : міжнар. док. від 28 січ. 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

70. Конвенція про захист прав людини і основоположних свобод : міжнар. док. від 4 листоп. 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004

71. Конвенція про кіберзлочинність : міжнар. док. від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575

72. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н. В. Глинської. Харків : Право, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139

73. Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології та захист інформації.* 1998. № 2. С. 70–79.

74. Крамаренко К. С., Тітко І. А. Напрями використання штучного інтелекту в кримінальних провадженнях (за матеріалами судової практики). *Аналітично-порівняльне правознавство.* 2026. Ч. 3. № 1. С. 75–81. URL: https://journal-app.uzhnu.edu.ua/article/view/353208

75. Кримінальний процес : підручник / [Ю. М. Грошевий, В. Я. Тацій, А. Р. Туман та ін.] ; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 824 с.

76. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: http://zakon3.rada.gov.ua/laws/show/4651-17

77. Лобойко Л. М. Кримінальний процес : підручник. Київ : Істина, 2014. 432 с.

78. Лоскутов Т. О. Щодо критеріїв визначення допустимості доказів у кримінальному провадженні. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки. 2021. Т. 32 (71), № 1. С. 106–110.

79. Матвєєв П. С. Особливості встановлення достовірності електронних доказів у господарському судочинстві України. *Правова позиція.* 2022. № 4 (37). С. 236–240. DOI: 10.32782/2521-6473.2022-4.44

80. Машталяр О. М., Петрик В. В. Персональні дані як електронний доказ у кримінальному процесі. *Юридичний науковий електронний журнал.* 2026. № 5. С. 218–221. DOI: https://doi.org/10.32782/2524-0374/2026-5/49

81. Метелев О. П. Гносеологічна і правова природа цифрових доказів у кримінальному процесі. *Правова позиція.* 2018. № 1 (20). С. 75–86. URL: http://biblio.umsf.dp.ua.jspui

82. Метелев О. П. Цифрові докази як окремий вид доказів у кримінальному процесі. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення.* 2018. Вип. 10. С. 100–104.

83. Михайленко В. Практичні аспекти тимчасового доступу до речей і документів за клопотаннями захисту і потерпілого. *Юридична газета.* URL: https://yur-gazeta.com/publications/practice/sudova-praktika/praktichni-aspekti-timchasovogo-dostupu-do-rechey-i-dokumentiv-za-klopotannyami-zahistu-i-poterpilog.html

84. Орлов Ю. Ю. Електронне відображення як криміналістичний об’єкт. *Науковий вісник Національної академії внутрішніх справ.* 2019. № 4 (113). С. 15–23.

85. Орлов Ю. Ю., Чернявський С. С. Використання електронних відображень як доказів у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 3 (104). С. 13–24.

86. Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 1 (13). С. 12–24.

87. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. № 87. С. 119–123. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/325327/315277

88. Петрик В. В. Електронні об’єкти, згенеровані штучним інтелектом, як докази у кримінальному провадженні: проблеми правового регулювання в Україні та зарубіжний досвід. *Юридичний науковий електронний журнал.* 2026. № 4. С. 217–222. URL: https://www.lsej.org.ua/4_2026/48.pdf

89. Петрик В. В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. № 90. Ч. 4. С. 324–328. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/340185/328228

90. Петрик В. В., Ментинська І. Б. Відтворення англомовних назв програмних продуктів у кримінальному процесі: проблеми уніфікування. *Інтернаука.* 2026. № 1 (95). С. 161–168. URL: https://humanitarian.com.ua/index.php/juridical/article/view/79/98

91. Погорецький М. А. Цифрові (електронні) докази та цифрова (електронна) форма доказів: розмежування понять і його значення для кримінального процесуального доказування. *Аналітично-порівняльне правознавство.* 2026. Ч. 3. № 1. С. 115–125. URL: https://journal-app.uzhnu.edu.ua/article/view/353257.

92. Поліція викрила злочинну групу, яка за допомогою штучного інтелекту оформлювала кредити на громадян. *РБК-Україна.* 2025. URL: https://www.rbc.ua/rus/news/zlochintsi-dopomogoyu-shtuchnogo-intelektu-1760430030.html

93. Положення про використання технологій штучного інтелекту працівниками Апарату Верховного Суду : наказ керівника Апарату Верховного Суду від 8 груд. 2025 р. № 117. URL: https://court.gov.ua/storage/portal/supreme/rizne/Polozhennya_SHI.pdf

94. Постанова Верховного Суду у складі колегії суддів Першої судової палати Касаційного кримінального суду від 29 верес. 2020 р. у справі № 601/1143/16, провадження № 51-2996км19. URL: https://reyestr.court.gov.ua/Review/92335214

95. Постанова Великої Палати Верховного Суду від 21 черв. 2023 р. у справі № 916/3027/21, провадження № 12-8гс23. URL: https://reyestr.court.gov.ua/Review/112088045

96. Постанова Верховного Суду у складі колегії суддів Третьої судової палати Касаційного кримінального суду від 12 черв. 2024 року у справі № 569/1908/23. провадження № 51-1430 км 24. URL: https://reyestr.court.gov.ua/Review/119741340

97. Постанова Верховного Суду у складі колегії суддів Першої судової палати Касаційного кримінального суду від 27 трав. 2025 р. у справі № 161/5016/21, провадження № 51-5933км23. URL: https://reyestr.court.gov.ua/Review/127826090

98. Постанова Верховного Суду у складі колегії суддів Третьої судової палати Касаційного кримінального суду від 21 лип. 2025 р. у справі № 201/11849/23, провадження № 51-584км25. URL: https://reyestr.court.gov.ua/Review/129086893

99. Постанова Верховного Суду у складі колегії суддів Касаційного господарського суду від 8 лип. 2025 р. у справі № 925/496/24. URL: http://reyestr.court.gov.ua/Review/128775966

100. Постанова Касаційного кримінального суду у складі Верховного Суду від 26 січ. 2021 р. у справі № 236/4268/18. URL: https://reyestr.court.gov.ua/Review/94905297

101. Постанова Касаційного кримінального суду у складі Верховного Суду від 10 верес. 2020 р. у справі № 751/6069/19. URL: https://reyestr.court.gov.ua/Review/91722819

102. Постанова Верховного Суду у складі колегії суддів Першої палати Касаційного кримінального суду від 31 берез. 2026 р. у справі № 175/10123/23, провадження № 51-1985км25. URL: https://reyestr.court.gov.ua/Review/135443439

103. Постанова Верховного Суду у складі колегії суддів Першої палати Касаційного кримінального суду від 30 верес. 2021 р. у справі № 498/582/18, провадження № 51-2926км2. URL: https://reyestr.court.gov.ua/Review/100109348

104. Постанова Верховного Суду у складі колегії суддів Першої судової палати Касаційного кримінального суду від 9 лип. 2024 р. у справі № 463/11851/21, провадження № 51-508км24. URL: https://reyestr.court.gov.ua/Review/120314115

105. Постанова Верховного Суду у складі колегії суддів Першої судової палати Касаційного кримінального суду від 3 груд. 2024 р. у справі № 331/451/22, провадження № 51-1952км24. URL: https://reyestr.court.gov.ua/Review/123602962

106. Постанова об'єднаної палати Касаційного кримінального суду у складі Верховного Суду від 25 верес. 2023 року у справі № 208/2160/18. URL: https://reyestr.court.gov.ua/Review/113817314

107. Постанова об'єднаної палати Касаційного кримінального суду у складі Верховного Суду від 29 берез. 2021 р. у справі № 554/5090/16-к, провадження № 51-1878кмо20. URL: https://reyestr.court.gov.ua/Review/96074938

108. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовт. 2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

109. 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

110. Проект Закону України «Про внесення змін до Кримінального кодексу України щодо кримінальних правопорушень проти безпеки особи» від 29 жовт. 2025 р. № 14165. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/58611

111. Радутний О. Е. Штучний інтелект в традиційних категоріях кримінального права України. *Вісник Асоціації кримінального права України.* 2023. Т. 1. № 19. URL: https://vakp.nlu.edu.ua/article/view/281123.

112. Ратнова А. В. Класифікація електронних документів, як джерел доказів, у кримінальному провадженні. *Журнал східноєвропейського права.* 2021. № 84. С. 42–47. URL: https://easternlaw.com.ua/wp-content/uploads/2021/01/ratnova_84.pdf

113. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказувані : дис. … д-ра філософії : 081 «Право». Львів, 2021. 248 с.

114. Рішення Конституційного Суду України у справі за конституційним поданням Служби безпеки України щодо офіційного тлумачення положення частини третьої статті 62 Конституції України від 20 жовт. 2011 р. № 12-рп/2011. URL: https://zakon.rada.gov.ua/laws/show/v012p710-11210

115. Савенко Н. С., Лазебний А. М. Проблеми фальсифікації криміналістичних доказів. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2026. Т. 5. № 93. С. 181–186. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/356002

116. Салтевський М. В. Криміналістика у сучасному викладі : підручник. Київ : Кондор, 2005. 588 с.

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

118. Сергєєва Д. Б. Проблеми визначення достовірності доказу як його властивості за новим Кримінальним процесуальним кодексом України. *Юрист України.* 2013. № 4 (25). С. 106–111.

119. Смаль І. А. Теоретичні засади формування та практика застосування електронних доказів у кримінальному процесі : дис. … д-ра філософії : 081 «Право». Чернігів, 2025. 344 с.

120. Стахівський С. М. Кримінально-процесуальні засоби доказування : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 32 с.

121. Степанов О. С. Належність та допустимість доказів у кримінальному процесі України : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 19 с.

122. Стефанів Н. Судова практика ККС Верховного Суду щодо допустимості електронних доказів : презентація. *Верховний Суд.* URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf

123. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. *Прес-центр Верховного Суду.* 2021. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/

124. Суддя ВС у ККС Наталія Марчук: електронні докази належать до категорії документів, а їхня допустимість визначається порядком отримання. *Прес-центр Верховного Суду*. 2025. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1838189/

125. Стоянов М. М. Система правил допустимості доказів у кримінальному провадженні України. *Актуальні проблеми держави і права.* 2013. Вип. 70. С. 245–250. URL: http://nbuv.gov.ua/UJRN/apdp_2013_70_39

126. Стоянов М. М. Властивості доказів у кримінальному процесі України : автореф. дис. ... канд. юрид. наук : 12.00.09. Одеса, 2010. 20 с.

127. Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2019. № 4. С. 208–214. URL: http://nbuv.gov.ua/UJRN/muvnudp_2019_14_24

128. Тализіна Я. Автентичні та редаговані відео-, аудіозаписи НСРД: правова позиція ВС щодо перевірки доказів на достовірність. *Вища школа адвокатури НААУ*. 2025. URL: https://www.hsa.org.ua/blog/avtenticni-ta-redagovani-video-audiozapisi-nsrd-pravova-poziciia-vs-shhodo-perevirki-dokaziv-na-dostovirnist

129. Толочко О. Гуманізація доказування у кримінальному провадженні. *Науковий часопис Національної академії прокуратури України.* 2014. № 4. С. 187–196.

130. Тренери цифрової доби: як працювати з електронними доказами ефективно. *Національна школа суддів України.* URL: https://www.nsj.gov.ua/ua/news/treneri-tsifrovoi-dobi-yak-pratsuvati-z-elektronnimi-dokazami-efektivno/

131. Тренінг «Цифрові докази у кримінальному провадженні». *Тренінговий центр прокурорів України*. 2023. URL: https://ptcu.gp.gov.ua/uk/2023/05/trening-czyfrovi-dokazy-u-kryminalnomu-provadzhenni/

132. Удалова Л. Д., Хабло О. Ю. Забезпечення державних, суспільних та особистих інтересів під час кримінального провадження в умовах воєнного чи

надзвичайного стану. Юридичний часопис Національної академії внутрішніх справ. 2022. Т. 12, № 4. С. 17–27. DOI: 10.56215/04221204.17.

133. Ухвала Апеляційної палати Вищого антикорупційного суду від 1 лют. 2022 р. у справі № 991/492/19, провадження №11-кп/991/3/22. URL: https://reyestr.court.gov.ua/Review/103002653

134. Ухвала Касаційного господарського суду у складі Верховного Суду від 8 лют. 2024 р. у справі № 925/200/22. URL: https://reyestr.court.gov.ua/Review/116984639

135. Ухвала слідчої судді Вищого антикорупційного суду від 25 черв. 2025 р. у справі № 991/6722/25, провадження № 1-кс/991/6791/25. URL: https://reyestr.court.gov.ua/Review/128751608

136. Хахановський В. Г., Петрик В. В. Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект). *Європейський правничий часопис.* 2025. Вип. 8. С. 161–165. URL: https://cms.legal-journal.e-u.edu.ua/uploads/8_23_2ebc56f1c6.pdf

137. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшукові діяльності органі внутрішніх справ : монографія. Одеса, 2011. 216 с.

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

139. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства.* 2017. № 2. С. 112–124. URL: http://nbuv.gov.ua/ UJRN/vkc_2017_2_16

140. Чигрина Г. Л. Джерела доказів у кримінальних справах про ухилення від сплати податків, зборів, інших обов’язкових платежів : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2004. 21 с.

141. Чупрікова І. Л. Належне джерело отримання доказів як гарантія допустимості. *Юридичний науковий електронний журнал.* 2015. Вип. 4. С. 266–269.

142. Шведова О. В. Комплексне криміналістичне дослідження документів, виконаних за допомогою комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2006. 19 с.

143. Юртаєва К. В. Кримінологічний аналіз використання технології Deepfake: коли фейк стає злочином. *Вісник Кримінологічної асоціації України.* 2021. № 1 (24). С. 31–42. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/10400

144. Wi-Fi-слід: маловідомий, але критичний демаскуючий фактор у цій війні. *Мілітарний.* URL: https://militarnyi.com/uk/blogs/wi-fi-slid-malovidomyj-ale-krytychnyj-demaskuyuchyj-faktor-u-tsij-vijni/

145. Adams D. M. The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, «Particularly» Speaking. *University of Richmond Law Review.* 2017. Vol. 51. P. 343–385. URL: https://scholarship.richmond.edu/law-student-publications/146/

146. AI Fraud Deterrence Act, H.R. 6306, 119th Congress. 2025. URL: https://www.congress.gov/bill/119th-congress/house-bill/6306/text

147. Anvar P. V. v P. K. Basheer & Ors, 18 September 2014. Supreme Court of India. *Civil Appellate Jurisdiction.* 2012. Civil Appeal No. 4226.

148. Athletic Director Charged in Pikesville High School AI Case. Baltimore County Police Department Press Release. URL: https://www.baltimorecountymd.gov/departments/police/news/2024/04/25/athletic-director-charged-in-pikesville-high-school-ai-case

149. Audibert M. La preuve numérique au cœur des enquêtes judiciaires, quels enjeux et quelles perspectives en procédure pénale ? *Les notes du Centre de Recherche de la Gendarmerie Nationale.* 2025. No. 114. P. 2. URL: https://hal.science/hal-05023029v1/document

150. Audibert M. Le recueil de la preuve numérique : enjeux et perspectives en procédure pénale : thèse de doctorat. Paris : Université Paris Nanterre, 2024. DOI: 10.70675/b32d1be5z447fz4b71z8a50z69881440c0a8

151. Audibert M. Refuser de communiquer le code de déverrouillage de son téléphone peut être une infraction. *Actualité juridique Pénal.* 2022. No.°21-83.146 P. 577.

152. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors., Civil Appeal Nos. 20825–20826 of 2017, (2020) 7 SCC 1 (Supreme Court of India, 14 July 2020). URL: https://indiankanoon.org/doc/172105947/

153. Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. New York and Geneva, 2022. 102 p. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

154. Bundeskriminalamt (BKA). Pressestelle der Generalstaatsanwaltschaft Hessen. URL: https://www.bka.de/SharedDocs/Kontaktdaten/DE/Inland/Gsta_Justiz_Hessen_Pressestelle.html

155. Bérubé M., Beaulieu L.-A., Allard S., Denault V. From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice.* 2025. Vol. 65. Issue 5. DOI: https://doi.org/10.1016/j.scijus.2025.101306

156. Canada Evidence Act, R.S.C., 1985, c. C-5. Department of Justice Canada. URL: https://laws-lois.justice.gc.ca/eng/acts/C-5/

157. Carlucci W. M., Stone K. E., Sarokhanian N. A. Changes Proposed to the Federal Rules of Evidence to Address AI Usage. *Barnes & Thornburg*. Nov. 15, 2024. URL: https://btlaw.com/en/insights/alerts/2024/changes-proposed-to-the-federal-rules-of-evidence-to-address-ai-usage

158. Cass. Ass. Plén., 7 Novembre 2022, No. 21-83.146. URL: https://www.legifrance.gouv.fr/juri/id/JURITEXT000042579789

159. Cass. Crim., 13 Octobre 2020, No.°20-80.150. URL: https://www.legifrance.gouv.fr/juri/id/JURITEXT000046583035

160. Case Georgia v. Russia (II) (Application No. 38263/08) : Decision of the European Court of Human Rights of 21 January 2021. URL: https://hudoc.echr.coe.int/eng?i=001-207757

161. CJUE, gr. ch., 4 Octobre 2024, aff. C-548/21. *Bezirkshauptmannschaft Landeck.* URL: https://infocuria.curia.europa.eu/tabs/document?source=document&docid=290675&doclang=FR

162. Case of Big Brother Watch and Others v. the United Kingdom (Applications Nos. 58170/13, 62322/14 and 24960/15) : Judgment of the European Court of Human Rights of 25 May 2021. URL: https://hudoc.echr.coe.int/eng?i=001-210077

163. Case of Benedik v. Slovenia (Application No. 62357/14) : Judgment of the European Court of Human Rights of 24 April 2018. URL: https://hudoc.echr.coe.int/eng?i=001-182455

164. Casey E. Digital evidence and computer crime: forensic science, computers and the internet. 3rd ed. Academic Press, 2011. 770 p.

165. Code de procédure pénale. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/

166. Cour de cassation, Assemblée plénière, 7 Janvier 2011, No. 09-14.316. *Bull. Ass. Plén.* 2011. No. 1. URL: https://www.legifrance.gouv.fr/juri/id/JURITEXT000023382684

167. Cour de cassation, Assemblée plénière, 10 Novembre 2017, No.°17-82.028. *Bull. crim.* 2017. No. 2. URL: https://www.legifrance.gouv.fr/juri/id/JURITEXT000036017648

168. Cour de cassation, Assemblée plénière, 9 Décembre 2019, No.°18-86.767. *Bull. crim.* 2019. URL: https://www.legifrance.gouv.fr/juri/id/JURITEXT000039536885

169. Cour de cassation, Assemblée plénière, 22 Décembre 2023, No. 20-20.648. *Bull.* 2023. URL: https://www.legifrance.gouv.fr/juri/id/JURITEXT000048769030

170. Cour de cassation, chambre criminelle, 20 Septembre 2016, No. 16-80.820. *Bull. crim.* 2016. URL: https://www.legifrance.gouv.fr/juri/id/JURITEXT000033147857

171. Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 2018 : H.R. 4943, 115th Cong. URL: https://www.congress.gov/bill/115th-congress/house-bill/4943

172. Criminal Code (Canada), R.S.C. 1985, c. C-46. *Justice Laws Website.* URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/

173. Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective by June 1, 2017), CLI.1.283838(EN) (China), Art. 24.

174. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). URL: https://supreme.justia.com/cases/federal/us/509/579/

175. Delage P.-J., Jeanne N., Parizot R. Procédure pénale. *Revue de science criminelle et de droit pénal comparé.* 2018. No. 1. P. 117–152. DOI: 10.3917/rsc.1801.0117

176. Delfino R. A. Deepfakes on Trial 2.0: A Revised Proposal for Authenticating AI-Manipulated Evidence. 2025. URL: https://www.uscourts.gov/sites/default/files/2025-04/25-ev-a_suggestion_from_prof._rebecca_delfino_-_rule_901.pdf

177. Delfino R. A. Deepfakes on Trial: A Call To Expand the Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery. *Hastings Law Journal.* 2023. Vol. 74. P. 293. URL: https://repository.uclawsf.edu/hastings_law_journal/vol74/iss2/3/

178. Digital 2025 Global Overview Report. *DataReportal.* URL: https://datareportal.com/reports/digital-2025-global-overview-report

179. 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. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj

180. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

181. Décret No. 2006-580 du 23 Mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 Novembre 2001 (1). URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000788820

182. Duncker & Humblot – Berlin: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme? *Duncker & Humblot – Berlin: Home*. URL: https://elibrary.duncker-humblot.com/article/5428/grundrecht-auf-gewaumlhrleistung-der-vertraulichkeit-und-integritaumlt-informationstechnischer-systeme

183. Electronic evidence guide. A basic guide for police officers, prosecutors and judges. Version 2.1. Strasbourg, 2020. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf

184. EN ISO/IEC 27037:2016. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://standards.iteh.ai/catalog/standards/cen/ff19a638-8301-45c0-8bb4-92965b0296ab/en-iso-iec-27037-2016

185. Federal Decree-Law No. (34) of 2021 on Combatting Rumours and Cybercrimes. *United Arab Emirates.* URL: https://uaelegislation.gov.ae

186. Federal Rules of Criminal Procedure. *United States Courts.* URL: https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-criminal-procedure

187. Federal Rules of Evidence. *United States Courts.* URL: https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence

188. France. Cybercrime policies/strategies. *Council of Europe.* URL: https://www.coe.int/en/web/octopus/-/france

189. Féral. La jurisprudence de la Cour de cassation en matière de preuve électronique. *Féral.* 2018. URL: https://feral.law/archives/la-jurisprudence-de-la-courde-cassation-en-matiere-de-preuve-electronique

190. General Principles for Digital Evidence. 2021. URL: https://www.ciinvestigators.org/wp-content/uploads/2021/11/CII-General-Principles-for-Digital-Evidence-21stCII.pdf

191. Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG). § 51. *Gesetze im Internet.* URL: https://www.gesetze-im-internet.de/bzrg/__51.html

192. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings : adopted by the Committee of Ministers on 30 January 2019 at the 1335th meeting of the Ministers' Deputies. URL:

https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

193. Goodison S. E., Davis R. C., Jackson B. A. Digital evidence and the U.S. criminal justice system. *RAND Corporation*. 2015. URL: https://www.rand.org/pubs/research_reports/RR890.html

194. Grimm P. W., Grossman M. R., Cormack G. V. Artificial Intelligence as Evidence. *Northwestern Journal of Technology and Intellectual Property.* 2021. Vol. 19. No. 1. URL: https://scholarlycommons.law.northwestern.edu/njtip/vol19/iss1/2/

195. Grossman M. R., Grimm P. W. Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence. *Science and Technology Law Review (Columbia).* 2025. Vol. 26 (2). DOI: https://doi.org/10.52214/stlr.v26i2.13890

196. Guidelines for digital forensics first responders. Best practices for search and seizure of electronic and digital evidence. March 2021. *INTERPOL*. URL: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf

197. H.K. v Prokuratuur : Judgment of the Court (Grand Chamber) of 2 March 2021, Case C-746/18, ECLI:EU:C:2021:152. URL: https://curia.europa.eu/juris/liste.jsf?num=C-746/18

198. Hargreaves C., van Beek H., Casey E. SOLVE-IT: A proposed digital forensic knowledge base inspired by MITRE ATT&CK. *Forensic Science International: Digital Investigation.* 2025. Vol. 52. DOI: 10.1016/j.fsidi.2025.301864

199. How a fake AI-generated audio clip framed a Baltimore principal. *The Baltimore Banner.* URL: https://www.thebaltimorebanner.com/education/k-12-schools/eric-eiswert-ai-audio-baltimore-county-YBJNJAS6OZEE5OQVF5LFOFYN6M/

200. Hurst E. How can the law deal with Deepfake? *All About Law.* URL: https://www.allaboutlaw.co.uk/commercial-awareness/legal-spotlight/how-can-the-law-deal-with-deepfake-

201. Jaussent V. Procès des viols de Mazan : la «personnalité à double facette» de Dominique Pelicot, jugé pour avoir drogué et livré sa femme à des hommes. *Franceinfo*.

9 Septembre 2024. URL: https://www.franceinfo.fr/faits-divers/affaire-des-viols-de-mazan/proces-des-viols-de-mazan-la-personnalite-a-double-facette-de-dominique-pelicot-juge-pour-avoir-drogue-et-livre-sa-femme-a-des-hommes_6682488.html

202. Indian Evidence Act, 1872 (Act No. 1 of 1872), as amended by the Information Technology Act, 2000 (Act No. 21 of 2000). URL: https://www.indiacode.nic.in/handle/123456789/2188

203. Investigatory Powers Act 2016 (UK), c. 25, ss. 99, 108–110. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents

204. Jiahong H. Back from the dead: Wrongful convictions and criminal justice in China. Honolulu,University of Hawai'i Press,2016. XXVI. 236 p.URL: https://journals.openedition.org/chinaperspectives/7150

205. Judgment of the Court of Justice of the European Union of 30 April 2024 in Case C-670/22 (M.N. – EncroChat). URL: https://curia.europa.eu/juris/liste.jsf?num=C-670/22

206. Judgment of the Court (Grand Chamber) of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238. *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

207. Khakhanovsky V., Petryk V. Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad. *Scientific Journal of the National Academy of Internal Affairs*. 2026. Vol. 31. No. 2. P. 9–19.

208. Kessler G. C. Judges' Awareness, Understanding, and Application of Digital Evidence : Doctoral dissertation. Fort Lauderdale, FL, 2010. URL: https://nsuworks.nova.edu/gscis_etd/196/

209. Kodeks karny Rzeczypospolitej Polskiej. Art. 132. URL: https://sip.lex.pl/akty-prawne/dz-u-dziennik-ustaw/kodeks-karny-16798683/art-132

210. Korshunov P., Marcel S. Subjective and Objective Evaluation of Deepfake Videos. *ICASSP 2021 – IEEE International Conference on Acoustics, Speech and Signal Processing*. 2021. P. 2510–2514.

211. Liang L. Between emotion, politics and law: narrative transformation and authoritarian deliberation in a land dispute-triggered social drama in China. *The China Quarterly.* 2021. Vol. 245. P. 94–121. URL: https://scholars.cityu.edu.hk/en/publications/between-emotion-politics-and-law-narrative-transformation-and-aut/

212. Li Zhe, Jin Zhenan. Digital Evidence and Cooperation of Service Providers in China. *The Cambridge Handbook of Digital Evidence in Criminal Investigations* / ed. by L. Bachmaier Winter. Cambridge University Press, 2025. P. 457–484.

213. Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007). URL: https://casetext.com/case/lorraine-v-markel-american-ins-co

214. Lorraine v. Markel American Insurance Company. *CourtListener.* URL: https://www.courtlistener.com/docket/4512526/27/lorraine-v-markel-american-insurance-company/

215. Mason S. The use of evidence generated by software in criminal proceedings. Institute of Advanced Legal Studies, University of London. 2025. URL: https://law.nus.edu.sg/trail/wp-content/uploads/sites/9/2025/08/The-use-of-evidence-generated-by-software-in-criminal-proceedings-Mason-for-TRAIL.pdf.

216. Mason S., Seng D. Electronic Evidence and Electronic Signatures. 5th edn. London : University of London Press, 2021. Chapter 2 : The foundations of evidence in electronic form. P. 51–84.

217. Mifsud Bonnici J. P., Tudorica M., Cannataci J. A. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. *Handling and Exchanging Electronic Evidence Across Europe (Law, Governance and Technology Series)*. 2018. Vol. 39. P. 189–235.

218. Novak M. Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law.* 2020. Vol. 14. No. 4. URL: https://commons.erau.edu/jdfsl/vol14/iss4/3

219. Number of internet users worldwide. *Statista.* URL: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

220. Panattoni B. Generative AI and criminal law. *Cambridge Forum on AI: Law and Governance.* 2025. Vol. 1. DOI: 10.1017/cfl.2024.9

221. Pikesville High School's principal was accused of offensive language on a recording. Authorities now say it was a deepfake. *CNN.* 2024. URL: https://www.cnn.com/2024/04/26/us/pikesville-principal-maryland-deepfake-cec/index.html

222. Police and Criminal Evidence Act 1984. URL: https://www.legislation.gov.uk/ukpga/1984/60/contents

223. Proposed Federal Rule of Evidence 707: Machine-Generated Evidence. *Committee on Rules of Practice and Procedure :* Judicial Conference of the United States. 2025. URL: https://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/agenda-books

224. Protecting Canadians from Online Crime Act, S.C. 2014, c. 31. Government of Canada. *Justice Laws.* URL: https://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/fulltext.html

225. R. v. M.S.A., 2024 ONCA 477. Court of Appeal for Ontario. URL: https://www.canlii.org/en/on/onca/doc/2024/2024onca477/2024onca477.html

226. R. v. Mawji (Rizwan) [2003] EWCA Crim 3067. England and Wales Court of Appeal (Criminal Division). URL: https://www.bailii.org/ew/cases/EWCA/Crim/2003/3067.html

227. R. v. Mills. Supreme Court of Canada. No. 26358. URL: https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1751/index.do

228. R. v. S.M., 2025 ONCA 18. Court of Appeal for Ontario. URL: https://www.canlii.org/en/on/onca/doc/2025/2025onca18/2025onca18.html

229. 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. *OJ L 191*. 2023. P. 118–180. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj

230. Rothstein P. F. Evidence: State and Federal Rules. St. Paul, 1991. 669 p.

231. Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases, 2 January 2019. URL: https://app.mps.gov.cn/gdnps/pc/content.jsp?id=7449892

232. Scientific Working Group on Digital Evidence. Electronic data (1 file). URL: http://www.swgde.org/

233. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. *Council of Europe Treaty Series.* Strasbourg, 2022. No. 224. URL: https://rm.coe.int/1680a49dab

234. Service-public.fr. Preuve d'un fait ou d'un acte juridique (21 October 2019). URL: https://www.service-public.fr/particuliers/vosdroits/F1800

235. State of Washington v. Puloka. AI on trial: How courts are litigating the GenAI boom. Thomson Reuters. URL: https://fingfx.thomsonreuters.com/gfx/legaldocs/zgvokxekavd/04192024ai_wash.pdf

236. Strafprozessordnung (StPO). § 261. Grundsatz der freien richterlichen Beweiswürdigung. *Dejure.org.* URL: https://dejure.org/gesetze/StPO/261.html

237. StPO – nichtamtliches Inhaltsverzeichnis. *Gesetze im Internet*. URL: https://www.gesetze-im-internet.de/stpo/

238. Take it Down Act: Pub. L. No. 119-12. *Congress.gov.* 2025. URL: https://www.congress.gov/crs-product/LSB11314

239. United States v. De Georgia, 420 F.2d 889 (9th Cir. 1969). *United States Court of Appeals for the Ninth Circuit.* URL: https://openjurist.org/420/f2d/889/united-states-v-de-georgia

240. United States v. Whitaker, 127 F.3d 595 (7th Cir. 1997). *United States Court of Appeals for the Seventh Circuit.* URL: https://openjurist.org/127/f3d/595/united-states-v-r-whitaker-d

241. Westerlund M. The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review.* 2019. Vol. 9. Issue 11. P. 39–52. URL: https://timreview.ca/article/1282

242. Youth Justice and Criminal Evidence Act 1999. URL: https://www.legislation.gov.uk/ukpga/1999/23/contents

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких відображено основні результати дослідження:

1. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. № 87. С. 119–123. DOI: 10.24144/2307-3322.2025.87.4.17

2. Хахановський В. Г., Петрик В. В. Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект). *Європейський правничий часопис.* 2025. Вип. 8. С. 161–165. DOI: 10.36919/3041-1149(Print).8.2025.161-165

3. Петрик В. В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. *Науковий вісник Ужгородського національного університету. Серія «Право».* № 90, ч. 4. 2025. С. 324–328. DOI: 10.24144/2307-3322.2025.90.4.46

4. Петрик В. В., Ментинська І. Б. Відтворення англомовних назв програмних продуктів у кримінальному процесі: проблеми уніфікування. *Інтернаука*. 2026. № 1 (95). С. 161–168. DOI: 10.25313/2520-2308-2026-1-11840

5. Петрик В. В. Електронні об’єкти, згенеровані штучним інтелектом, як докази у кримінальному провадженні: проблеми правового регулювання в Україні та зарубіжний досвід. *Юридичний науковий електронний журнал.* 2026. № 4. С. 217–222. DOI: 10.32782/2524-0374/2026-4/46

6. Машталяр О. М., Петрик В. В. Персональні дані як електронний доказ у кримінальному процесі. *Юридичний науковий електронний журнал.* 2026. № 5. С. 218–221. DOI: 10.32782/2524-0374/2026-5/49

7. Khakhanovsky V., Petryk V. Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad. *Scientific Journal of the*

National Academy of Internal Affairs. 2026. № 31 (2). P. 9–19. DOI: 10.63341/naia-herald/2.2026.09

Наукові праці, у яких засвідчено апробацію матеріалів праці:

1. Петрик В. В. Електронні докази в судочинстві України та зарубіжних країн: поняття, правове регулювання та проблеми використання. *Global trends in science and education* : матеріали III Міжнар. наук.-практ. конф. (Київ, 7–9 квіт. 2025 р.). Київ, 2025. С. 921–926.

2. Петрик В. В. Поняття та правова природа електронних доказів у кримінальному процесі України. *Future of science: innovations and perspectives* : . Proceedings of the 9th International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2025. Pp. 224–228 .

Додаток Б

Акти впровадження

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор
полковник поліції
Сергій ЧЕРНЯВСЬКИЙ
_____ 2026 року

АКТ

20 . 05 . 2026 м. Київ № 126-ОП

Впровадження результатів дисертації Петрика Віталія Віталійовича на тему: «Особливості використання електронних доказів у кримінальному процесів в Україні та світі» в освітній процес НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– начальника відділу організації освітнього процесу, старшого лейтенанта поліції Бойчук Вікторії Олександрівни;

– т.в.о. начальника відділу організації наукової діяльності, кандидата юридичних наук, капітана поліції Горбенко Дар'ї Андріївни;

– завідувача кафедри інформаційних технологій Навчально-наукового інституту права та психології, кандидата фізико-математичних наук, доцента Кудінова Вадима Анатолійовича;

– завідувача кафедри кримінології та інформаційних технологій, доктора філософії права, доцента, капітана поліції Школьнікова Владислава Ігоровича;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора, підполковника поліції Тихонової Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила матеріали дисертації, поданої на здобуття ступеня доктора філософії зі спеціальності 081 «Право», та наукові праці аспіранта денної форми навчання кафедри інформаційних технологій Навчально-наукового інституту права та психології Національної академії внутрішніх справ Петрика Віталія Віталійовича на тему: «Особливості використання електронних доказів у кримінальному процесів в Україні та світі» та на основі проведеного аналізу зробила висновок, що надана робота містить низку обґрунтованих теоретичних положень і пропозицій, спрямованих на удосконалення процесуального порядку збирання, фіксації, перевірки та оцінки електронних доказів у кримінальному процесі, а також на запровадження

сучасних підходів до роботи з окремими видами електронних доказів, зокрема, створеними засобами штучного інтелекту).

Проаналізовано основні результати дослідження Петрика В.В., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Петрик, В. В. Електронні докази в судочинстві України та зарубіжних країн: поняття, правове регулювання та проблеми використання. *III Міжнародна науково-практична конференція " Global trends in science and education "*, 7–9 квітня 2025 р. Київ, Україна. С. 921 – 926;

2. Петрик В. В. Поняття та правова природа електронних доказів у кримінальному процесі України. IX Міжнародна науково-практична конференція "Future of Science: Innovations and Perspectives", 14–16 липня 2025 р. Стокгольм, Швеція. С. 224–228;

3. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. Науковий вісник Ужгородського національного університету. Серія: Право. № 87. 2025. С. 119–123. DOI: 10.24144/2307-3322.2025.87.4.17;

4. Хахановський В. Г., Петрик В. В. Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект). Європейський правничий часопис. 2025. Вип. 8. С. 161–165. DOI: 10.36919/3041-1149(Print).8.2025.161-165;

5. Петрик В. В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. Науковий вісник Ужгородського національного університету. Серія: Право. № 90, ч. 4. 2025. С. 324–328; DOI: 10.24144/2307-3322.2025.90.4.46;

6. Петрик В. В., Ментинська І. Б. Відтворення англомовних назв програмних продуктів у кримінальному процесі: проблеми уніфікування. Міжнародний науковий журнал «Інтернаука». 2026. № 1 (95). С. 161–168. DOI: 10.25313/2520-2308-2026-1-11840;

7. Петрик В. В. Електронні об'єкти, згенеровані штучним інтелектом, як докази у кримінальному провадженні: проблеми правового регулювання в Україні та зарубіжний досвід. Юридичний науковий електронний журнал. №4/2026. С. 217-222. DOI: 10.32782/2524-0374/2026-4/46;

8. Машталяр О. М., Петрик В. В. Персональні дані як електронний доказ у кримінальному процесі. Юридичний науковий електронний журнал. №5/2026. С. 218-221. DOI: 10.32782/2524-0374/2026-5/49;

9. Khakhanovsky, V., & Petryk, V. (2026). Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad. Scientific Journal of the National Academy of Internal Affairs, 31(2), 9-19. DOI: 10.63341/naia-herald/2.2026.09.

На основі проведеного аналізу комісія зробила висновок, що праці Петрика В.В., 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 «Інформаційні технології та системи», «Застосування інформаційних технологій в правоохоронній діяльності», «Аналіз та прогнозування злочинності» під час підготовки навчально-методичних та дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

Вікторія БОЙЧУК

Дар'я ГОРБЕНКО

Вадим КУДІНОВ

Владислав ШКОЛЬНІКОВ

Олена ТИХОНОВА

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор
Національної академії
внутрішніх справ,
доктор юридичних наук, професор
полковник поліції
Олег ТАРАСЕНКО
_____ 2026 року

АКТ

20 . 05 . 2026 м. Київ № 122-110

Впровадження результатів дисертації Петрика Віталія Віталійовича на тему: «Особливості використання електронних доказів у кримінальному процесі в Україні та світі» 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 кафедри інформаційних технологій Навчально-наукового інституту права та психології, кандидата фізико-математичних наук, доцента Кудінова Вадима Анатолійовича;

– завідувача кафедри кримінології та інформаційних технологій, доктора філософії права, доцента капітана поліції Школьнікова Владислава Ігоровича;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила матеріали дисертації, поданої на здобуття ступеня доктора філософії зі спеціальності 081 «Право», наукові праці аспіранта денної форми навчання кафедри інформаційних технологій Навчально-наукового інституту права та психології Національної академії внутрішніх справ Петрика Віталія Віталійовича на тему: «Особливості використання електронних доказів у кримінальному процесі в Україні та світі» та на основі проведеного аналізу зробила висновок, що надана робота містить низку обґрунтованих теоретичних положень і пропозицій спрямованих на удосконалення кримінального процесуального регулювання використання електронних доказів, підвищення ефективності їх збирання, фіксації, перевірки та оцінки у кримінальному провадженні, а також на запровадження дієвих механізмів забезпечення допустимості й автентичності електронних доказів, зокрема створених або модифікованих засобами штучного інтелекту.

Проаналізовано основні результати дослідження Петрика В.В., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Петрик, В. В. Електронні докази в судочинстві України та зарубіжних країн: поняття, правове регулювання та проблеми використання. *III Міжнародна науково-практична конференція " Global trends in science and education "*, 7–9 квітня 2025 р. Київ, Україна. С. 921 – 926.

2. Петрик В.В. Поняття та правова природа електронних доказів у кримінальному процесі України. IX Міжнародна науково-практична конференція "Future of Science: Innovations and Perspectives", 14–16 липня 2025 р. Стокгольм, Швеція. С. 224–228.
3. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. Науковий вісник Ужгородського національного університету. Серія: Право. № 87. 2025. С. 119–123. DOI: 10.24144/2307-3322.2025.87.4.17.
4. Хахановський В. Г., Петрик В. В. Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект). Європейський правничий часопис. 2025. Вип. 8. С. 161–165. DOI: 10.36919/3041-1149(Print).8.2025.161-165
5. Петрик В. В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. Науковий вісник Ужгородського національного університету. Серія: Право. № 90, ч. 4. 2025. С. 324–328; DOI: 10.24144/2307-3322.2025.90.4.46
6. Петрик В. В., Ментинська І. Б. Відтворення англомовних назв програмних продуктів у кримінальному процесі: проблеми уніфікування. Міжнародний науковий журнал «Інтернаука». 2026. № 1 (95). С. 161–168. DOI: 10.25313/2520-2308-2026-1-11840
7. Петрик В.В. Електронні об'єкти, згенеровані штучним інтелектом, як докази у кримінальному провадженні: проблеми правового регулювання в Україні та зарубіжний досвід. Юридичний науковий електронний журнал. №4/2026. С. 217-222. DOI: 10.32782/2524-0374/2026-4/46
8. Машталяр О.М., Петрик В.В. Персональні дані як електронний доказ у кримінальному процесі. Юридичний науковий електронний журнал. №5/2026. С. 218-221. DOI: 10.32782/2524-0374/2026-5/49
9. Khakhanovsky, V., & Petryk, V. (2026). Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad. Scientific Journal of the National Academy of Internal Affairs, 31(2), 9-19. DOI: 10.63341/naia-herald/2.2026.09

На основі проведеного аналізу комісія зробила висновок про те, що вищезазначені матеріали дисертаційного дослідження Петрика В.В. на тему: «ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В КРИМІНАЛЬНОМУ ПРОЦЕСІ В УКРАЇНІ ТА СВІТІ» застосовуються 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

Вадим КУДІНОВ

Владислав ШКОЛЬНІКОВ

Олена ТИХОНОВА

Людмила ГАЙДАР

info@uaa.org.ua
www.uaa.org.ua

+38 067 501 5610
ЄДРПОУ 34294645



ВСЕУКРАЇНСЬКА ГРОМАДСЬКА ОРГАНІЗАЦІЯ
"АСОЦІАЦІЯ АДВОКАТІВ УКРАЇНИ"

вул. Дніпровська набережна, 3
м. Київ, 02098

Вих. від «08» червня 2026 р. № 364

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Петрика Віталія Віталійовича

«Особливості використання електронних доказів в кримінальному процесі в Україні та світі»

на здобуття наукового ступеня доктора філософії

за спеціальністю 081 «Право»

Результати дисертаційного дослідження «Особливості використання електронних доказів в кримінальному процесі в Україні та світі» Петрика Віталія Віталійовича опубліковані у наведених нижче фахових наукових статтях:

1. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. Науковий вісник Ужгородського національного університету. Серія: Право. № 87. 2025. С. 119–123. DOI https://doi.org/10.24144/2307-3322.2025.87.4.17.
2. Хахановський В. Г., Петрик В. В. Штучний інтелект і електронні докази: проблеми автентичності (юридичний аспект). Європейський правничий часопис. 2025. Вип. 8. С. 161–165; DOI 10.36919/3041-1149(Print).8.2025.161-165
3. Петрик В. В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. Науковий вісник Ужгородського національного університету. Серія: Право. № 90, ч. 4. 2025. С. 324–328; DOI https://doi.org/10.24144/2307-3322.2025.90.4.46
4. Петрик В. В., Ментинська І. Б. Відтворення англомовних назв програмних продуктів у кримінальному процесі: проблеми уніфікування. Міжнародний науковий журнал «Інтернаука». 2026. № 1 (95). С. 161–168. DOI: https://doi.org/10.25313/2520-2308-2026-1-11840
5. Петрик В.В. Електронні об'єкти, згенеровані штучним інтелектом, як докази у кримінальному провадженні: проблеми правового регулювання в Україні та зарубіжний досвід. Юридичний науковий електронний журнал. №4/2026. С. 217-222 DOI https://doi.org/10.32782/2524-0374/2026-4/46

info@uaa.org.ua
www.uaa.org.ua

+38 067 501 5610
ЄДРПОУ 34294645



ВСЕУКРАЇНСЬКА ГРОМАДСЬКА ОРГАНІЗАЦІЯ
"АСОЦІАЦІЯ АДВОКАТІВ УКРАЇНИ"

вул. Дніпровська набережна, 3
м. Київ, 02098

6. Машталяр О.М., Петрик В.В. Персональні дані як електронний доказ у кримінальному процесі. Юридичний науковий електронний журнал. №5/2026. С. 218-221. DOI https://doi.org/10.32782/2524-0374/2026-5/49

7. Khakhanovsky, V., & Petryk, V. (2026). Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad. Scientific Journal of the National Academy of Internal Affairs, 31(2), 9-19. doi: 10.63341/naia-herald/2.2026.09

Результати дисертаційного дослідження вивчено, отримано відповідні рекомендації та прийнято до уваги для подальшого використання в діяльності Всеукраїнської громадської організації «Асоціація адвокатів України». Практичну цінність для адвокатської діяльності становлять обґрунтовані здобувачем підходи до перевірки автентичності, допустимості та цілісності електронних доказів, оцінки окремих їх видів (листування в месенджерах, електронних об'єктів, створених за допомогою штучного інтелекту), а також до перевірки належного суб'єкта, способу та джерела отримання електронних доказів, що сприяє забезпеченню ефективного захисту прав і законних інтересів учасників кримінального провадження. Напрацювання цієї роботи за потреби будуть використовуватись Асоціацією під час організації та проведення вебінарів, круглих столів тощо.

Президент ВГО «Асоціація адвокатів України»
Дмитрієва О.Л.

Додаток В

АНКЕТА ТА ЗВЕДЕНІ РЕЗУЛЬТАТИ АНКЕТУВАННЯ

Анкетування «Особливості використання електронних доказів у кримінальному процесі України» проведено автором за допомогою онлайн-форми. Отримано та опрацьовано відповіді 130 працівників прокуратури. Географія опитування охоплює прокурорів більшості регіонів України, зокрема Вінницької, Волинської, Дніпропетровської, Житомирської, Закарпатської, Запорізької, Івано-Франківської, Київської, Кіровоградської, Львівської, Миколаївської, Одеської, Полтавської, Рівненської, Сумської, Тернопільської, Харківської, Херсонської, Хмельницької, Черкаської, Чернівецької та Чернігівської областей.. Анкета містила чотири блоки запитань. Нижче наведено текст анкети та зведені результати за кожним запитанням (кількість відповідей та їх частка від загальної кількості респондентів, N = 130).

А. Текст анкети

БЛОК І. Загальні відомості про респондента

1. Стаж практичної роботи: до 1 року; від 1 до 3 років; від 3 до 5 років; від 5 до 10 років; понад 10 років.

2. Чи мали Ви досвід роботи з електронними доказами (ЕД) у кримінальному провадженні: так, неодноразово; так, поодинокі випадки; ні, не доводилось.

БЛОК ІІ. Правове регулювання та класифікація електронних доказів

3. Який термін найбільш точно відображає правову природу інформації в електронній формі, що використовується як доказ: електронний доказ; цифровий доказ; електронний документ (як підвид документа); електронне відображення; важко відповісти.

4. Чи достатньо чинне кримінальне процесуальне законодавство України регулює порядок використання ЕД: так; частково, існують окремі прогалини; ні, потребує суттєвого доопрацювання; важко відповісти.

5. Чи потребує КПК України окремої статті, яка визначала б поняття «електронний доказ» та встановлювала його як самостійне джерело доказів: так; ні (достатньо ч. 3 ст. 99 КПК); потрібно вдосконалити існуючі норми без окремої статті; важко відповісти.

6. З якими різновидами ЕД Ви найчастіше стикались (кілька варіантів): листування у месенджерах; електронна пошта; відео-/аудіозаписи, фотографії; дані соцмереж; дані геолокації; бази даних і реєстри; хмарні сховища; вміст інтернет-сайтів; матеріали, згенеровані ШІ.

7. Чи достатнє регулювання отримання ЕД з-за кордону (Конвенція про кіберзлочинність, Другий додатковий протокол): достатнім; потребує вдосконалення механізмів; потребує суттєвої реформи; важко відповісти.

БЛОК ІІІ. Збирання, дослідження та оцінка електронних доказів

8. Основні проблеми збирання та використання ЕД (кілька варіантів): відсутність єдиної методики; складність автентичності/цілісності; брак кваліфікації спеціалістів; обмеженість технічних засобів; складність отримання даних від провайдерів.

9. Найпроблемніші елементи допустимості ЕД: належний суб’єкт; належний спосіб; належне джерело.

10. Найпоширеніший спосіб фіксації листування в месенджерах (кілька варіантів): скриншоти; протокол огляду пристрою з фотофіксацією; експорт файлів переписки; КТЕ пристрою; резервні копії з хмари; запит до адміністратора месенджера.

11. Найсерйозніші проблеми листування як доказу (кілька варіантів): ідентифікація відправника; «зникаючі» повідомлення; наскрізне шифрування; відмова провайдерів; підробка скриншотів; відсутність метаданих; міжюрисдикційність серверів.

12. Чи стикались Ви із запереченням автентичності листування: так, неодноразово, і це вплинуло на оцінку; так, але суд переважно визнавав допустимими; так, і доказ визнано недопустимим; ні.

13. Інструменти забезпечення автентичності/цілісності ЕД (кілька варіантів): хеш-суми; спеціалізоване ПЗ (UFED, FTK, Encase); ЕЦП/КЕП; фіксація метаданих окремим протоколом; нотаріальне посвідчення; не застосовую.

14. Чи призначали Ви КТЕ або іншу експертизу ЕД: так, неодноразово; так, поодинокі випадки; ні, не було потреби.

15. Роль ЕД порівняно з іншими доказами: превалюють; рівнозначні; допоміжна (другорядна) роль.

16. Категорії правопорушень, де ЕД найважливіші (кілька варіантів): проти життя/здоров'я; проти волі, честі, гідності; проти власності; обіг наркотиків; кіберзлочини; громадська безпека; службова діяльність (корупція); основи національної безпеки.

БЛОК IV. Сучасні виклики та перспективи

17. Чи стикались Ви з доказами, згенерованими ШІ: так; ні, але вважаю це актуальною загрозою; ні, і не вважаю це проблемою.

18. Чи стикались Ви з аудіо-/відео-/фотоматеріалами, автентичність яких ставилася під сумнів через ШІ (deepfake): так, у власних провадженнях; так, чув від колег; ні; важко відповісти.

19. Чи використовуєте інструменти ШІ для оцінки ЕД: так, регулярно; ні, але вважаю перспективним; ні, не вбачаю необхідності.

20. На кого має покладатися тягар доказування автентичності цифрових аудіо-/відео: на сторону, що подає доказ (де-факто); на сторону, що оспорює; механізм перерозподілу; обов'язкова експертиза за рахунок держави; важко відповісти.

21. Чи потрібна обов'язкова експертиза на ШІ-генерацію для всіх цифрових аудіовізуальних доказів: так, для всіх; так, лише за клопотанням сторони; ні, лише за рішенням слідчого/суду; важко відповісти.

22. Чи доцільно запровадити єдиний стандарт збирання, фіксації та зберігання ЕД: так, вкрай необхідно; бажано, але не першочергово; ні; важко відповісти.

23. Ваші пропозиції щодо вдосконалення правового регулювання та практики використання ЕД (відкрите запитання).

Б. Зведені результати за запитаннями

Рис. 1. Стаж практичної роботи

Варіант відповіді	К-ть	%
до 1 року	9	6,9
від 1 до 3 років	5	3,8
від 3 до 5 років	2	1,5
від 5 до 10 років	12	9,2
понад 10 років	102	78,5

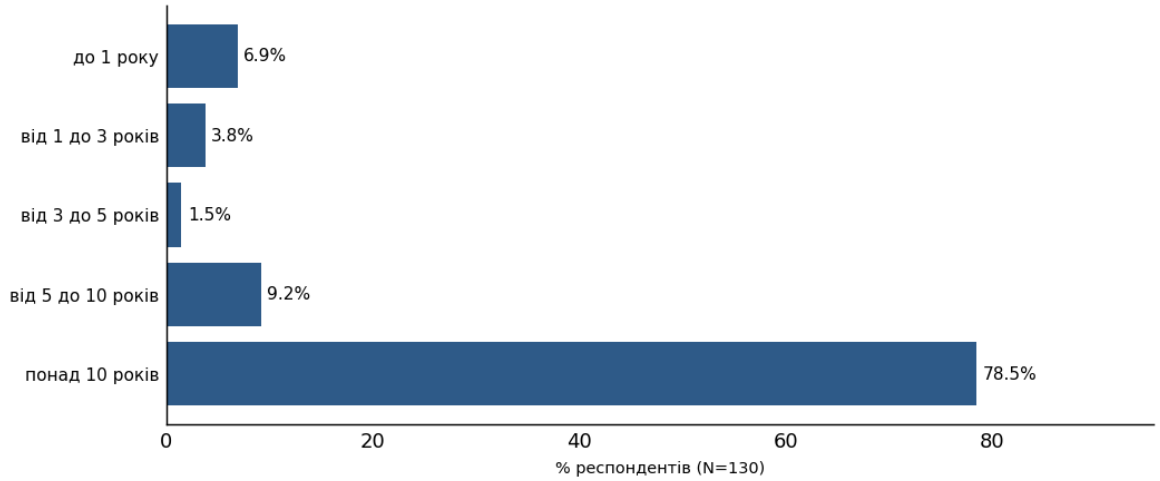


Рис. 2. Досвід роботи з електронними доказами

Варіант відповіді	К-ть	%
так, неодноразово	46	35,4
так, поодинокі випадки	47	36,2
ні, не доводилось	37	28,5

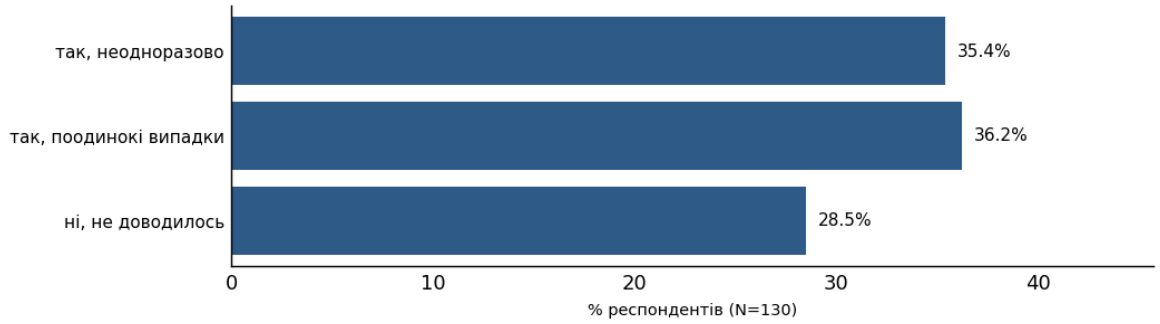


Рис. 3. Найточніший термін для інформації в електронній формі

Варіант відповіді	К-ть	%
електронний доказ	64	49,2
цифровий доказ	23	17,7
електронний документ (як підвид документа)	32	24,6
електронне відображення	3	2,3
важко відповісти	8	6,2

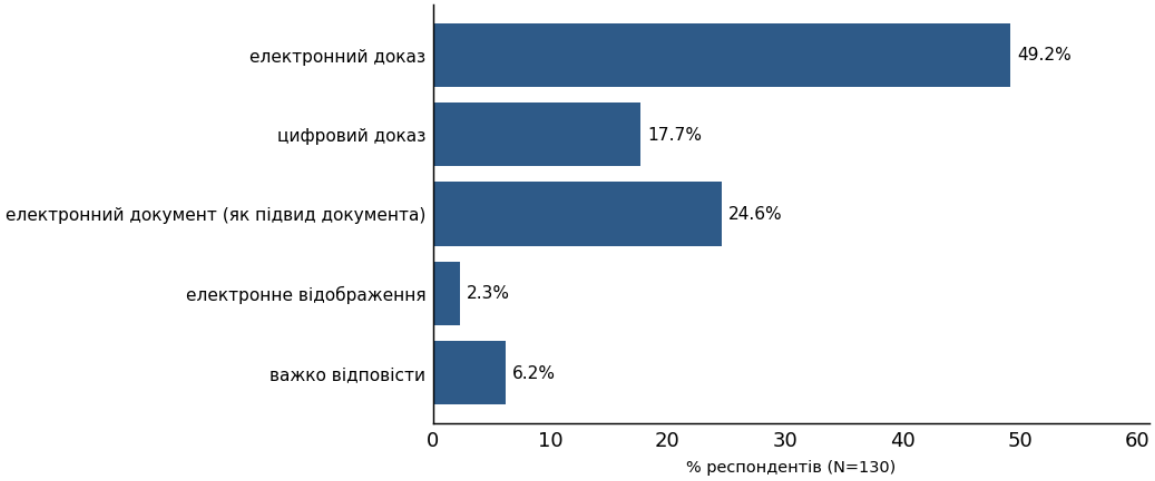


Рис. 4. Достатність чинного регулювання використання ЕД

Варіант відповіді	К-ть	%
так, законодавство є достатнім	15	11,5
частково, існують окремі прогалини	64	49,2
ні, потребує суттєвого доопрацювання	38	29,2
важко відповісти	13	10,0

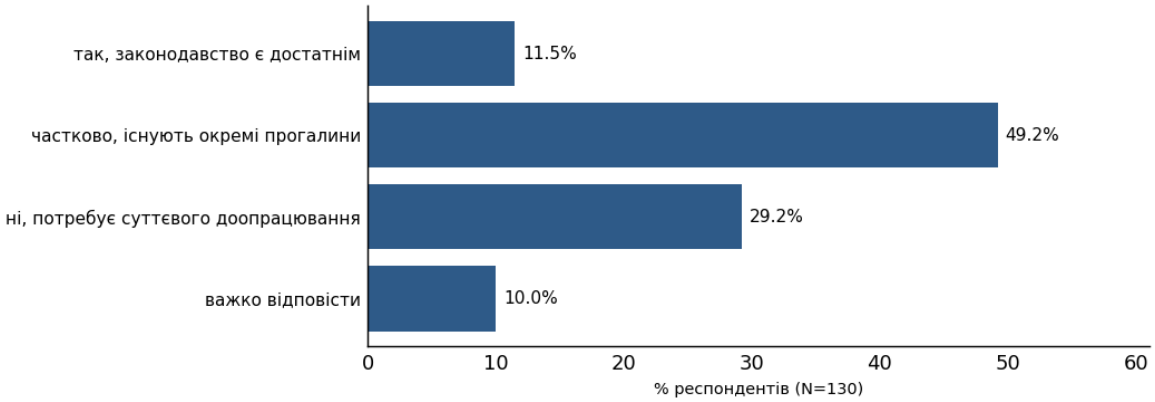


Рис. 5. Необхідність окремої статті КПК про «електронний доказ»

Варіант відповіді	К-ть	%
так, це необхідно	71	54,6
ні, достатньо чинного регулювання через поняття «електронний документ» (ч. 3 ст. 99 КПК)	17	13,1
потрібно вдосконалити існуючі норми без створення окремої статті	33	25,4
важко відповісти	9	6,9

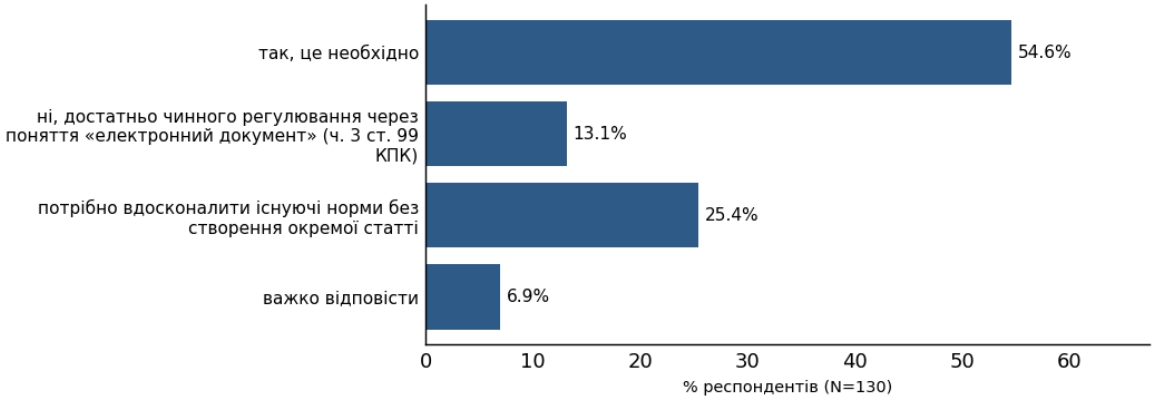


Рис. 6. Різновиди ЕД у практиці (можливо декілька варіантів; сума часток перевищує 100 %)

Варіант відповіді	К-ть	%
листування у месенджерах	102	78,5
електронна пошта	36	27,7
відео- та аудіозаписи, фотографії	99	76,2
дані з соціальних мереж	60	46,2
дані геолокації	39	30,0
інформація з електронних баз даних та реєстрів	50	38,5
дані з хмарних сховищ	9	6,9
вміст Інтернет-сайтів та веб-сторінок	62	47,7
матеріали, згенеровані штучним інтелектом	1	0,8
інші / уточнені відповіді	2	1,5

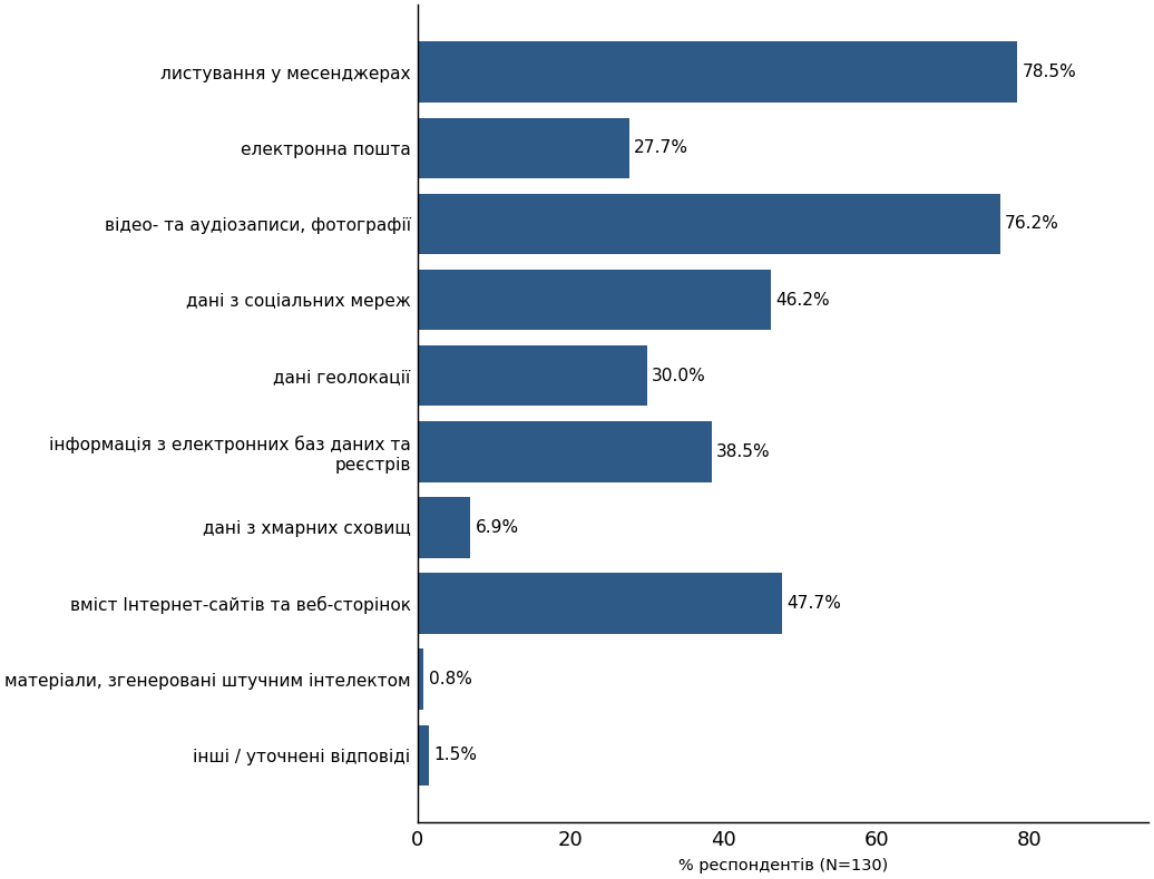


Рис. 7. Регулювання отримання ЕД з-за кордону

Варіант відповіді	К-ть	%
достатнім	13	10,0
потребує вдосконалення механізмів практичного застосування	63	48,5
потребує суттєвої законодавчої реформи	17	13,1
важко відповісти	37	28,5

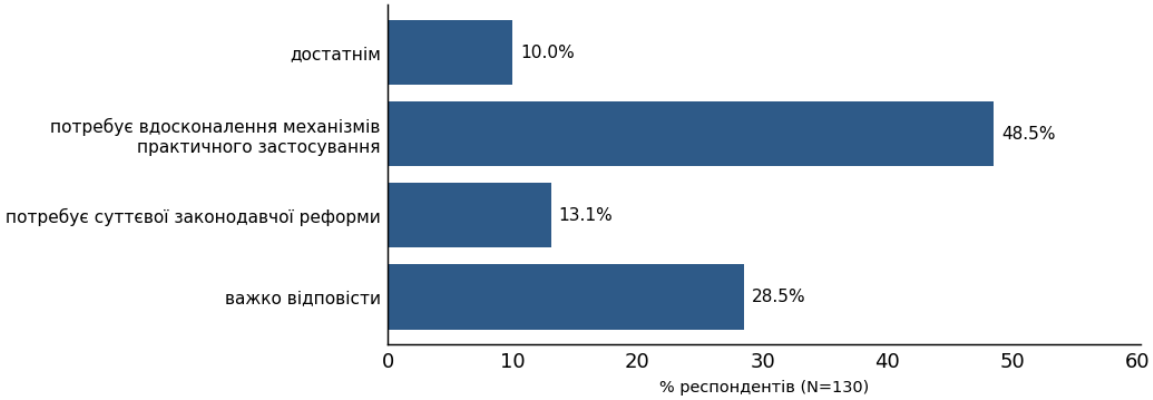


Рис. 8. Основні проблеми збирання та використання ЕД (можливо декілька варіантів; сума часток перевищує 100 %)

Варіант відповіді	К-ть	%
відсутність єдиної методики збирання та фіксації	78	60,0
складність забезпечення автентичності та цілісності даних	56	43,1
відсутність або недостатня кваліфікація спеціалістів	39	30,0
відсутність або обмеженість технічних засобів	48	36,9
складність отримання даних від постачальників послуг	52	40,0
інші / уточнені відповіді	4	3,1

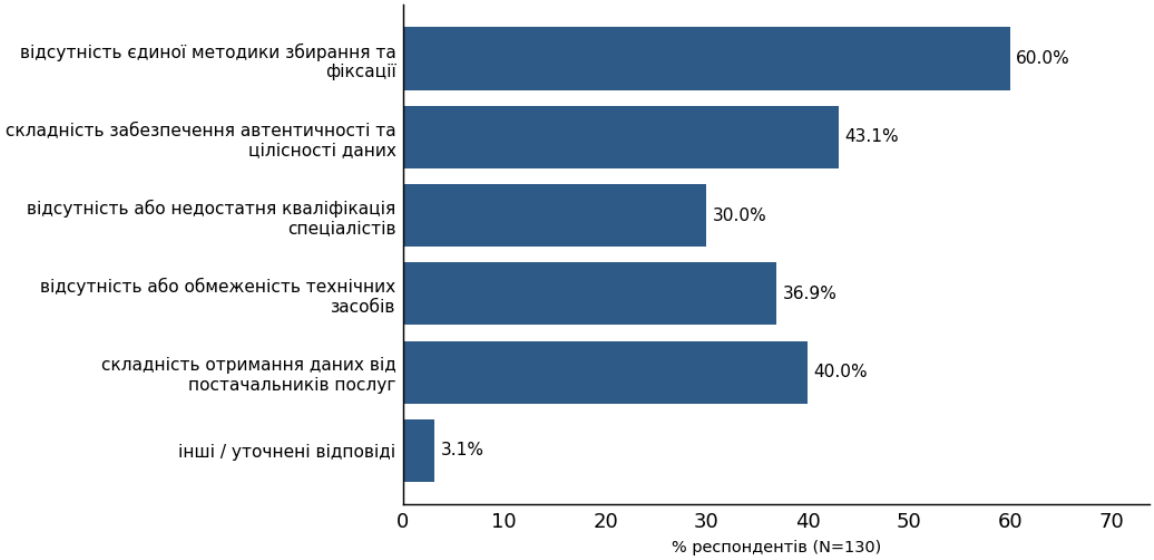


Рис. 9. Найпроблемніші елементи допустимості ЕД (можливо декілька варіантів; сума часток перевищує 100 %)

Варіант відповіді	К-ть	%
належний суб’єкт збирання доказу	6	4,6
належний спосіб збирання доказу	60	46,2
належне джерело отримання доказу	63	48,5
інші / уточнені відповіді	1	0,8

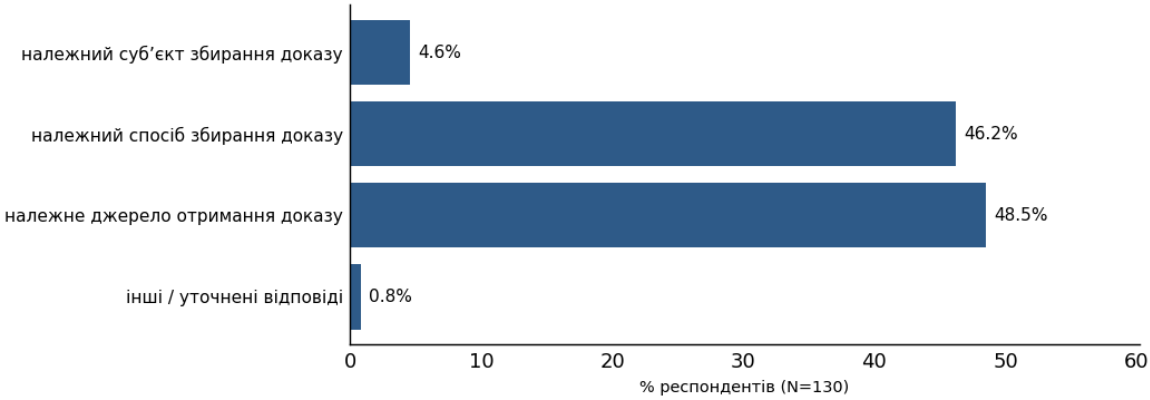


Рис. 10. Спосіб фіксації листування в месенджерах (можливо декілька варіантів; сума часток перевищує 100 %)

Варіант відповіді	К-ть	%
скриншоти екрану пристрою	77	59,2
протокол огляду мобільного пристрою з фотофіксацією екрана	103	79,2
експортовані файли переписки	20	15,4
судова комп'ютерно-технічна експертиза мобільного пристрою	52	40,0
отримання резервних копій з хмарних сховищ	9	6,9
запит до адміністратора месенджера	4	3,1
інші / уточнені відповіді	1	0,8

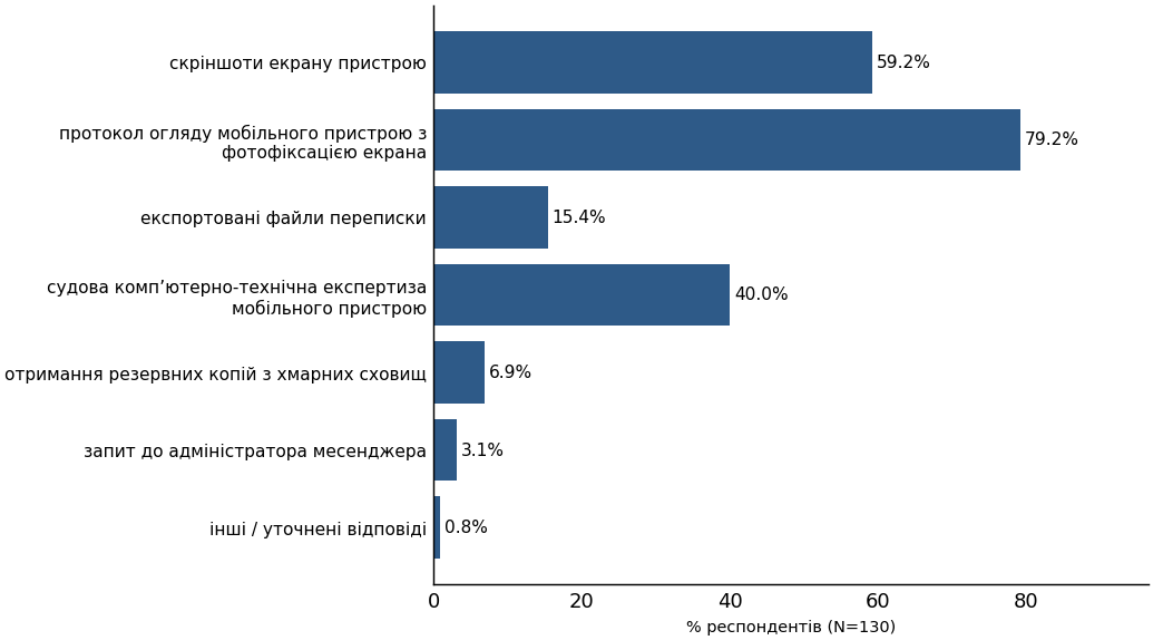


Рис. 11. Найсерйозніші проблеми листування як доказу (можливо декілька варіантів; сума часток перевищує 100 %)

Варіант відповіді	К-ть	%
ідентифікація особи, яка фактично надсилала повідомлення	96	73,8
функції «зникаючих» повідомлень	77	59,2
наскрізне шифрування	55	42,3
відмова провайдерів передавати дані за запитом	34	26,2
можливість підробки скриншотів та редагування переписки	30	23,1
відсутність метаданих у скриншотах	32	24,6
міжюрисдикційний характер серверів месенджерів	14	10,8

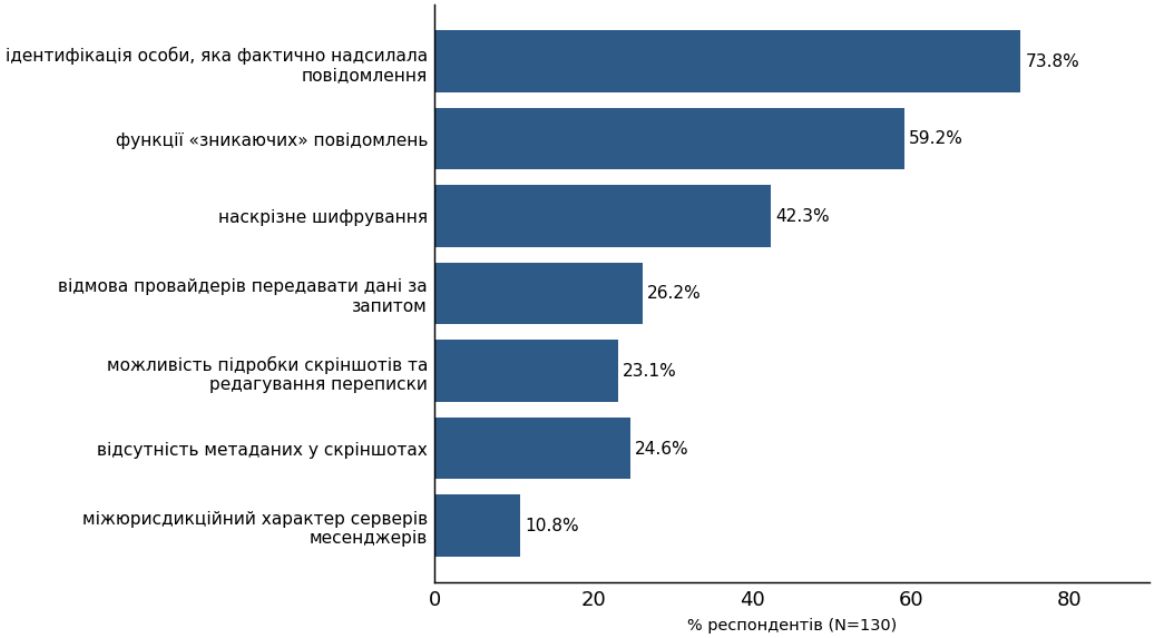


Рис. 12. Заперечення автентичності листування на практиці

Варіант відповіді	К-ть	%
так, неодноразово, і це вплинуло на оцінку доказу судом	14	10,8
так, але суд переважно визнавав докази допустимими	39	30,0
так, і доказ було визнано недопустимим	2	1,5
ні, такі ситуації не траплялись	75	57,7

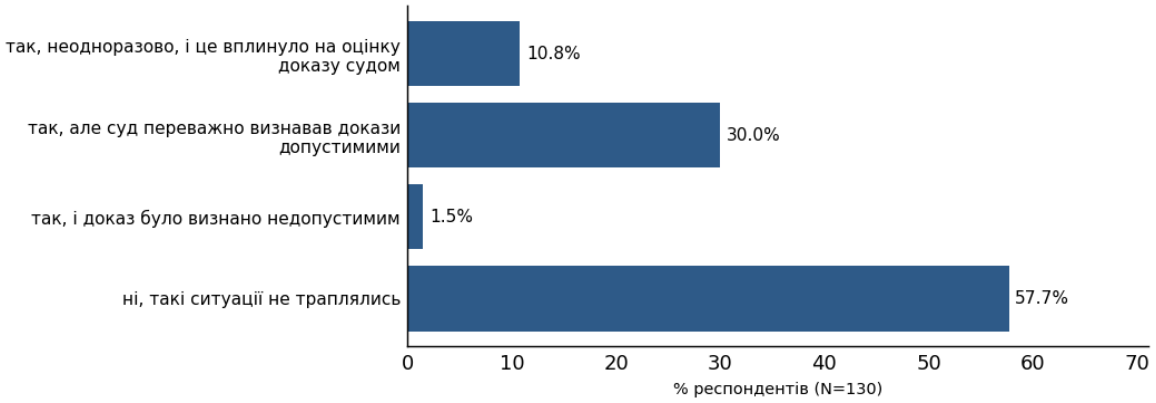


Рис. 13. Інструменти забезпечення автентичності та цілісності (можливо декілька варіантів; сума часток перевищує 100 %)

Варіант відповіді	К-ть	%
обчислення та фіксація хеш-сум	32	24,6
використання спеціалізованого ПЗ для криміналістичного копіювання	17	13,1
електронний / кваліфікований електронний підпис	37	28,5
фіксація метаданих окремим протоколом	24	18,5
нотаріальне посвідчення електронного доказу	2	1,5
не застосовую жодних спеціальних інструментів	45	34,6
інші / уточнені відповіді	2	1,5



Рис. 14. Призначення експертизи ЕД

Варіант відповіді	К-ть	%
так, неодноразово	18	13,8
так, поодинокі випадки	45	34,6
ні, не було потреби	67	51,5

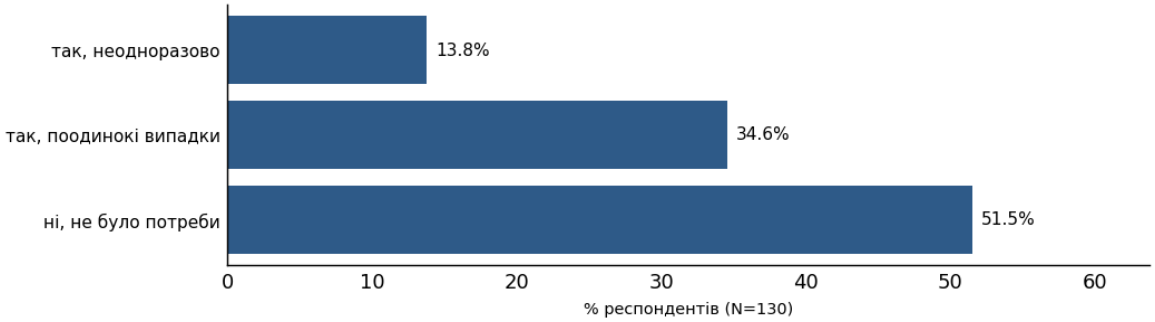


Рис. 15. Роль ЕД порівняно з іншими доказами

Варіант відповіді	К-ть	%
електронні докази превалюють серед інших видів доказів	8	6,2
електронні докази мають рівнозначне значення порівняно з іншими видами доказів	72	55,4
електронні докази відіграють допоміжну (другорядну) роль	48	36,9
інші / уточнені відповіді	2	1,5

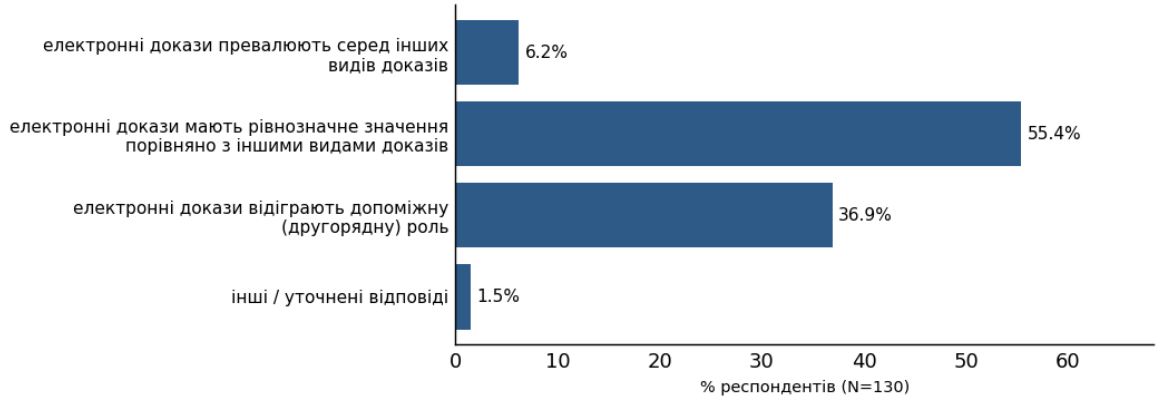


Рис. 16. Категорії правопорушень, де ЕД найважливіші (можливо декілька варіантів; сума часток перевищує 100 %)

Варіант відповіді	К-ть	%
проти життя та здоров'я особи	24	18,5
проти волі, честі та гідності особи	15	11,5
проти власності	65	50,0
у сфері обігу наркотичних засобів	52	40,0
у сфері використання комп'ютерів та комп'ютерних мереж (кіберзлочини)	84	64,6
проти громадської безпеки	11	8,5
у сфері службової діяльності (корупційні правопорушення)	51	39,2
проти основ національної безпеки	63	48,5
інші / уточнені відповіді	3	2,3

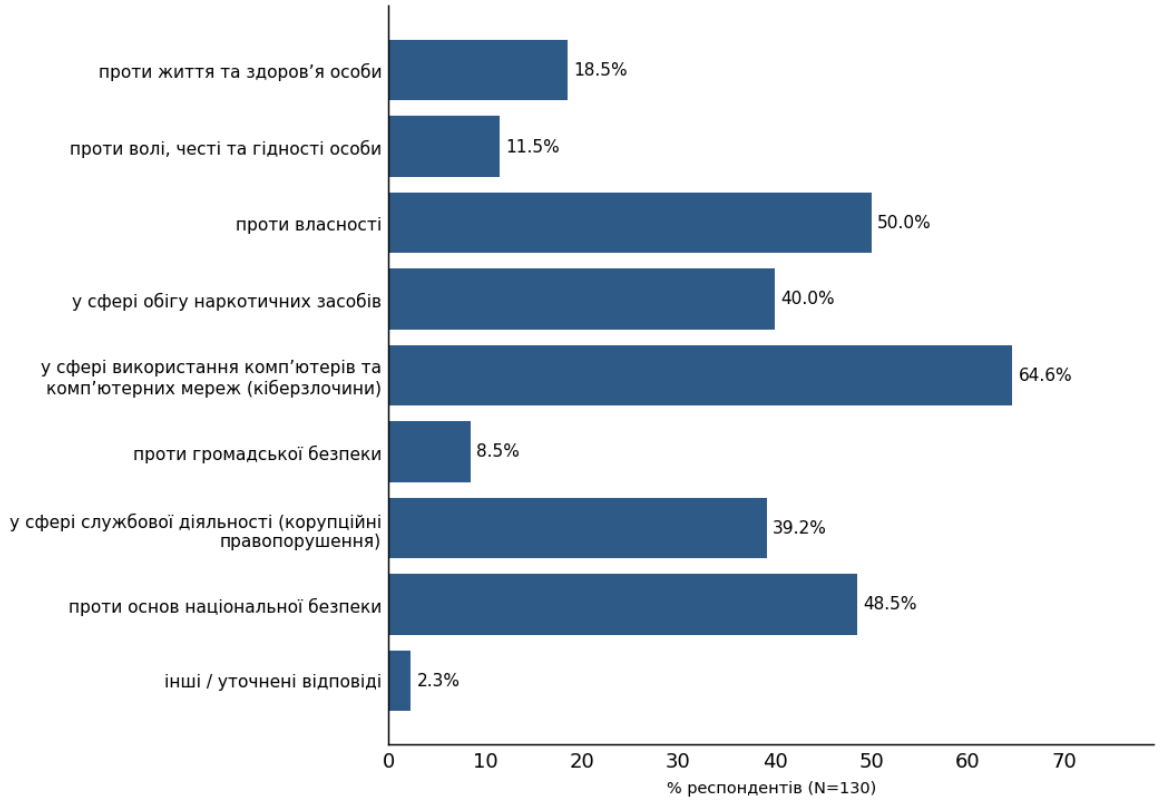


Рис. 17. Випадки доказів, згенерованих ШІ

Варіант відповіді	К-ть	%
так, такі випадки траплялись	6	4,6

ні, але вважаю це актуальною загрозою	101	77,7
ні, і не вважаю це суттєвою проблемою	19	14,6
інші / уточнені відповіді	4	3,1

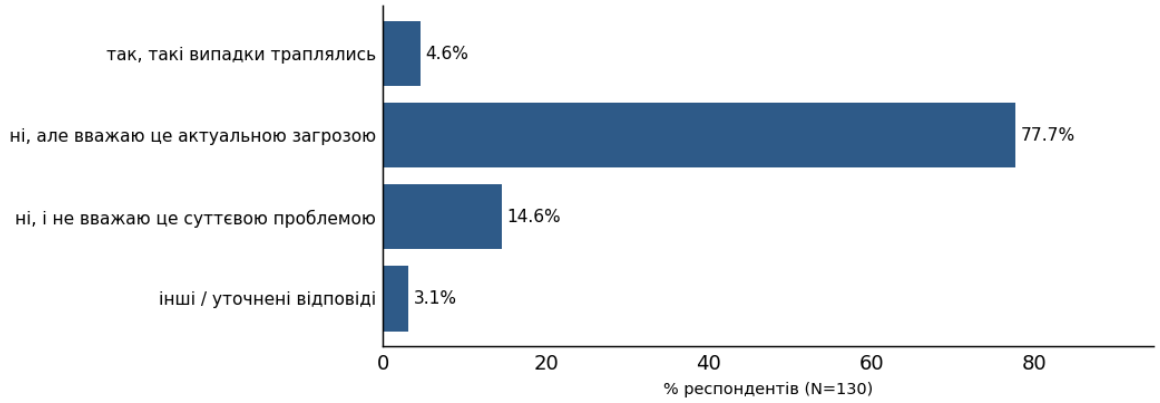


Рис. 18. Сумніви в автентичності через ШІ (deepfake)

Варіант відповіді	К-ть	%
так, у кримінальних провадженнях, де я брав/брала участь	9	6,9
так, чув/чула про такі випадки від колег	22	16,9
ні, на практиці не зустрічав/-ла	96	73,8
важко відповісти	3	2,3

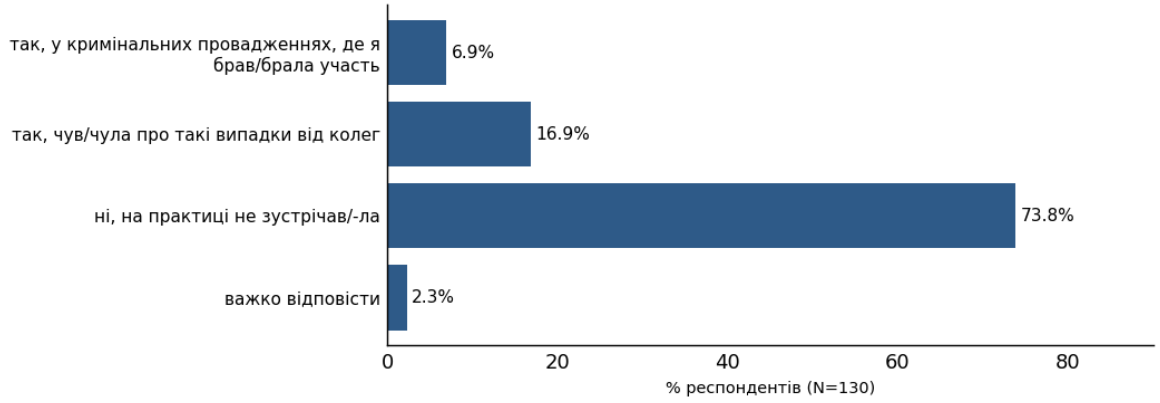


Рис. 19. Використання інструментів ШІ для оцінки ЕД

Варіант відповіді	К-ть	%
так, регулярно використовую	6	4,6
ні, але вважаю впровадження таких інструментів перспективним	63	48,5
ні, і не вбачаю необхідності	61	46,9

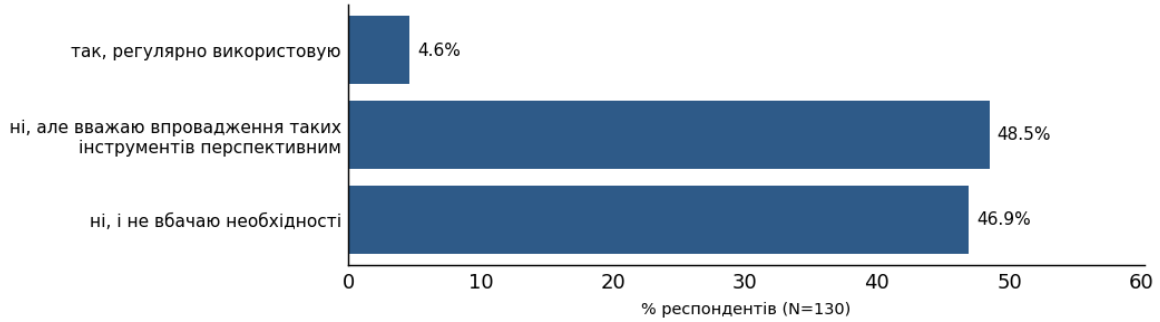


Рис. 20. Тягар доказування автентичності аудіо-/відео

Варіант відповіді	К-ть	%

на сторону, яка подає доказ (зараз де-факто)	82	63,1
на сторону, яка оспорює доказ	12	9,2
повинен діяти механізм перерозподілу	22	16,9
повинна бути обов'язкова експертиза за рахунок суду/держави	6	4,6
важко відповісти	8	6,2

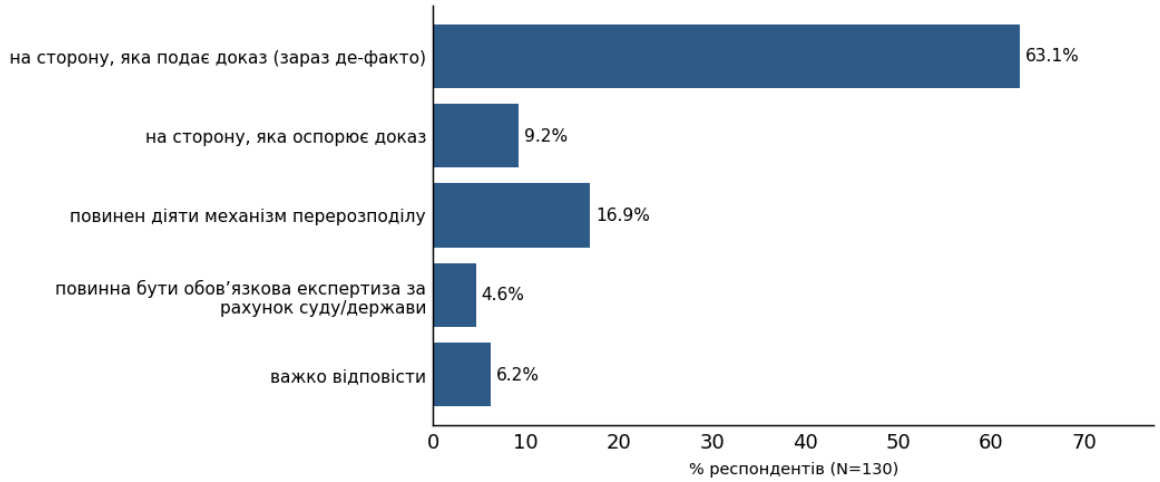


Рис. 21. Обов'язкова експертиза на ШІ-генерацію

Варіант відповіді	К-ть	%
так, для всіх без винятку	19	14,6
так, але лише за наявності обґрунтованого клопотання сторони	46	35,4
ні, лише за рішенням слідчого/суду в конкретному випадку	50	38,5
важко відповісти	15	11,5

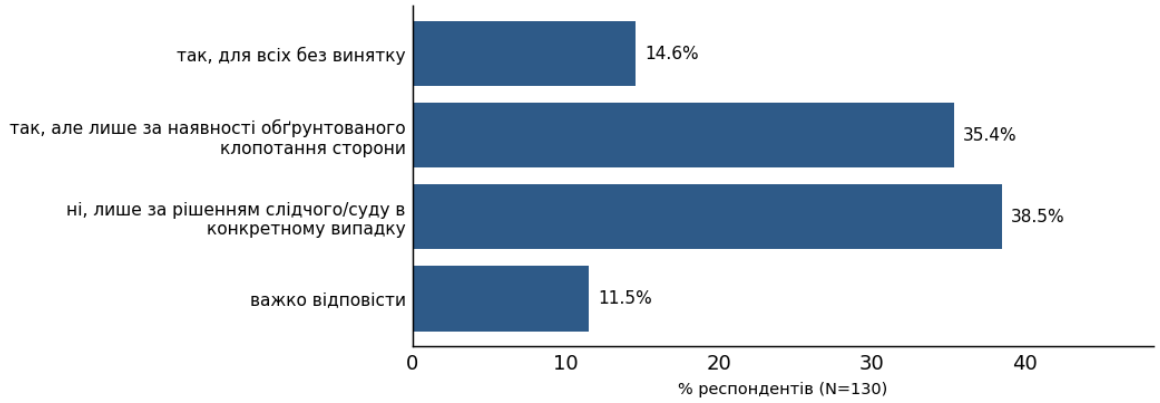
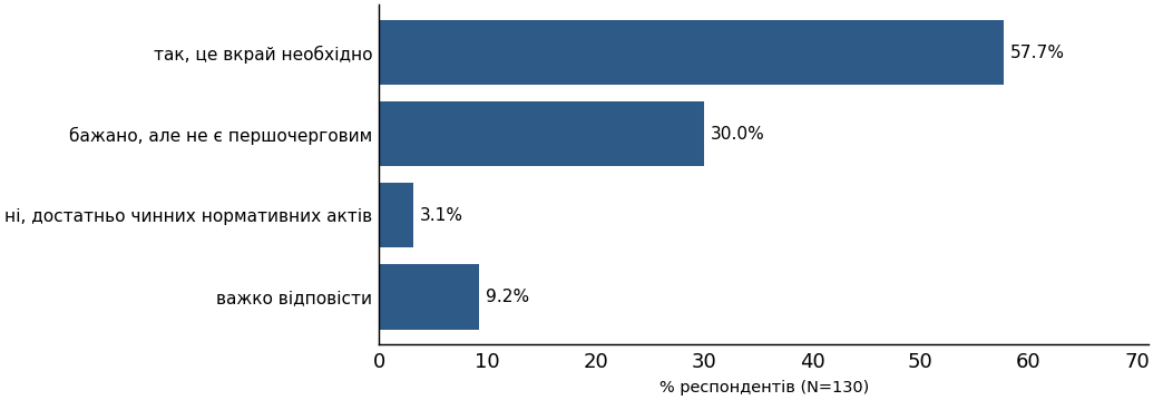


Рис. 22. Єдиний стандарт збирання/фіксації/зберігання ЕД

Варіант відповіді	К-ть	%
так, це вкрай необхідно	75	57,7
бажано, але не є першочерговим	39	30,0
ні, достатньо чинних нормативних актів	4	3,1
важко відповісти	12	9,2


так, це вкрай необхідно
57.7%
бажано, але не є першочерговим
30.0%
ні, достатньо чинних нормативних актів
3.1%
важко відповісти
9.2%
0
10
20
30
40
50
60
70
% респондентів (N=130)