ПЕНІТЕНЦІАРНА АКАДЕМІЯ УКРАЇНИ
МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

СМАЛЬ ІННА АНАТОЛІЇВНА

УДК 343.13:004.65 (043.3)

ДИСЕРТАЦІЯ

ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ І ПРАКТИКА ЗАСТОСУВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Спеціальність 081 «Право»
Галузь знань 08 «Право»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **І. А. Смаль**

Науковий керівник **Богатирьов Іван Григорович ,**
доктор юридичних наук, професор

Чернігів – 2025

АНОТАЦІЯ

Смаль І. А. Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю (081 – Право). – Пенітенціарна академія України, 2025.

Робота є комплексним науковим дослідженням, спрямована на розв'язання низки теоретичних та прикладних питань, пов'язаних з використанням електронних доказів у кримінальному процесі України.

У межах проведеного дослідження було досліджено витоки, становлення та розвиток концепції електронних доказів у кримінальному процесі крізь призму доктринальних підходів, судової практики та технологічного прогресу. З метою визначення перспективних напрямів подальших наукових розвідок здійснено комплексний огляд наукових джерел, нормативного регулювання та прикладів практичного застосування. Особливу увагу приділено впливу цифровізації та стрімкого розвитку інформаційних технологій на формування нових форм доказової інформації. Аналіз судової практики засвідчив наявність неоднозначних підходів до використання електронних доказів у кримінальних провадженнях, що значною мірою обумовлено відсутністю законодавчо закріпленого визначення цього поняття у чинному КПК України.

За результатами дослідження встановлено, що електронні докази відіграють дедалі важливішу роль у доказуванні, що зумовлює необхідність формування єдиної концепції їх правового регулювання та процесуального використання. Саме інституціоналізація електронних доказів, як окремого правового інституту, здатна забезпечити правову визначеність, посилити гарантії прав людини та сприяти ефективності кримінального судочинства. Усе це свідчить про потребу в комплексному дослідженні електронних доказів не лише як технічного чи доказового засобу, а як правового явища, що набуває

ознак самостійного інституту.

З огляду на це, у роботі було виокремлено основні періоди формування інституту електронних доказів у кримінальному процесуальному праві, що дало змогу простежити еволюцію наукових поглядів, нормативного закріплення та практичного застосування в умовах технологічного поступу. Зокрема, до таких періодів віднесено: І період— 1970-2000 р. Становлення доктринальних підходів щодо поняття «електронний документ»; ІІ період — 2001-2012 р. Подальший розвиток наукових уявлень щодо інформації, отриманої з електронних джерел та законодавче закріплення терміну « електронний документ»; ІІІ період— 2012-сучасний період. Прийняття КПК України, подальший доктринальний пошук оптимальних моделей використання інформації в електронному вигляді як доказу.

Виділено характерні ознаки електронних доказів, як то відтворюваність —можливість копіювання без втрати первинного змісту; нематеріальність – існують у вигляді цифрових даних, закодованих у вигляді бінарних або інших електронних сигналів та можуть бути відображені лише через спеціальні технічні пристрої цифровий формат, які зберігаються, передаються та обробляються за допомогою електронних пристроїв; динамічність — можливість змінюватися під впливом програмного забезпечення або користувацьких дій; залежність від технічних носіїв (для збереження, перегляду, перевірки електронного доказу потрібне спеціальне програмне забезпечення або обладнання); відсутність жорсткої прив’язки до матеріального носія (можливість існування однієї і тієї інформації одночасно на різних, не зв’язаних між собою, носіях); наявність метаданих (електронні докази містять метадані, які не є основним змістом файлу, але допомагають визначити його автентичність, час створення, редагування, авторство, тощо).

Окрему увагу приділено дослідженню правової природи електронних доказів, що сприяло пошуку додаткових аргументів щодо необхідності виділення електронних доказів як самостійного процесуального джерела.

Підтримано думку українських вчених - процесуалістів про необхідність виділення електронних доказів в окреме процесуальне джерело та висловлено власну аргументацію з цього приводу. Правова природа електронних доказів, унікальні характеристики дають підстави для віднесення їх до самостійного процесуального джерела, а отже буде достатньою аргументацією для визначення окремого порядку отримання доказової інформації, її дослідження та оцінки. Додаткові аргументи, що обґрунтовують необхідність такого кроку: 1)трансформація інформаційного середовища; 2) правова визначеність та уніфікація судової практики; 3) невідповідність традиційних джерел доказів сучасним технологічним реаліям; 4) захист прав учасників кримінального провадження; 5) європейські стандарти та міжнародна практика.

Звернуто увагу на існування термінологічного багатоманіття для позначення такого «феномену» як електронні докази та сформульовано власне визначення даного поняття: *«Електронний доказ – це інформація в електронному вигляді, що містить відомості про обставини, що мають значення для кримінального проводження та підлягають доказуванню, створена, збережена, або передана за допомогою електронних пристроїв, систем, або мереж та яка існує в формі, що забезпечує її автентичність, цілісність та придатність для дослідження».*

Здійснено аналіз наукових підходів до класифікації електронних доказів, запропонованих вітчизняними дослідниками та розроблено авторську класифікацію електронних доказів із виокремленням релевантних критеріїв, що враховують їх походження, форму, змістовну природу та процесуальні особливості, а саме : 1) за формою існування; 2) за способом формування; 3) за технічним середовищем існування. Доведено теоретичне та практичне значення класифікації електронних доказів, оскільки саме вона сприяє адаптації кримінального процесу до умов цифрової епохи, формуванню єдиних стандартів доказування з врахуванням процесуальних особливостей їх збирання, збереження, дослідження та оцінки.

Системно проаналізовано положення кримінального процесуального законодавства та практичні аспекти використання як доказу інформації в електронному вигляді та більш детально досліджено окремі види електронних доказів, зокрема, акцентовано увагу на проблемах правової регламентації електронного документа та практики використання як доказу. Обґрунтовано тезу, що електронний документ є одним із видів електронних доказів.

Констатовано, що оригіналом електронного документа є електронний документ з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Проаналізовано ряд законопроєктів щодо врегулювання використання електронних доказів у кримінальному провадженні та доведено, що наполегливе ігнорування законодавцем специфічної сутності інформації в електронному вигляді та намагання ситуативно вирішити проблемні питання, пов'язані з використанням такої інформації в процесі доказування в кримінальних провадженнях, яке проявляється у чисельних змінах та доповненнях кримінальних процесуальних норм, призводить лише до поглиблення проблеми процесуальної забезпеченості використання як доказу інформації в електронному вигляді.

Досліджено поняття показання технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі в контексті електронних доказів. При дослідженні даного виду електронних доказів окрему увагу приділено питанням недопустимості доказів та обґрунтовано пропозицію про необхідність внесення змін до КПК, спрямованих на забезпечення сталості та єдності судової практики щодо використання електронних доказів у кримінальному провадженні .

Обґрунтовано думку, що показання технічних приладів і технічних засобів, що мають функції фото і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, які визначені самостійним процесуальним джерелом доказів у кримінальному провадженні щодо кримінальних проступків, є не чим іншим, як одним із видів електронних доказів. Запропоновано зміни до ст. 245-1 КПК України, зокрема в частині необхідності термінологічного уточнення —замість «зняття показань технічних приладів та технічних засобів» використовувати поняття «отримання електронних даних з технічних приладів та технічних засобів» та до ст.3 КПК України, доповнивши її визначенням терміна «електронні дані» — це інформація в електронному вигляді, яка придатна для сприйняття людиною після обробки автоматичними програмними засобами.

Розглянуто особливості використання як доказу інформації з відкритих джерел та обґрунтовано доцільність та перспективність подальших наукових розвідок у цьому напрямку. Сформульовано власне бачення порядку проведення такої слідчої (розшукової) дії як огляд комп'ютерних даних та розроблено протокол огляду електронних даних.

Детально вивчено одне із найбільш дискусійних питань щодо використання дефініцій «оригінал», «дублікат», «копія» у контексті електронних доказів та аргументовано необхідність законодавчого закріплення положень щодо необхідності підтвердження автентичності копії електронного доказу шляхом застосування хешування чи іншим способом, що забезпечить можливість перевірки автентичності та цілісності інформації та запропоновані відповідні зміни до КПК України.

Зроблено висновок, що існування електронних доказів в специфічному середовищі, обумовленому використанням певних технічних засобів чи пристроїв та програмного забезпечення не дозволяє поширювати категорії «оригінал», «дублікат» і «копія» у їхньому традиційному значенні на

електронні докази. Запропоновано визначити в КПК України можливості надання не тільки оригінала інформації в електронному вигляді, але і її копії.

Логічною частиною роботи став розгляд проблемних питань дотримання «права на приватність» під час провадження слідчих (розшукових) та негласних слідчих (розшукових) дій. В цьому напрямку здійснено комплексний аналіз положень кримінального процесуального законодавства, чинних міжнародних правових договорів, практики Європейського суду з прав людини та відповідно національної судової практики та запропоновані зміни до КПК України в частині запровадження нової слідчої(розшукової) дії — обшук електронних пристроїв, які забезпечать виконання завдань кримінального провадження, визначених статтею 2 КПК України та дотримання пропорційності втручання в гарантовані статтею 8 ЄКПЛ право на повагу до свого приватного і сімейного життя, кореспонденції.

Наголошено, що під час проведення обшуку (ч. 6 ст. 236 КПК України) вже відбувається втручання в права гарантовані ст. 8 ЄКПЛ, навіть без вилучення відповідних електронних пристроїв. Для забезпечення права на повагу до кореспонденції запропоновано таку модель поведінки агентів держави, коли функції слідчого і особи, яка здійснює перегляд такої інформації в електронному вигляді будуть розділені (це може бути експерт). Окремо має бути контроль за інформацією, розголошення якої не допускається (журналістські джерела, адвокатська таємниця, таємниця нарадчої кімнати, тощо). Відібрана в такий спосіб інформація має пройти контроль слідчого судді до того як буде передана слідчому для використання у кримінальному провадженні як доказу. В такому випадку буде забезпечено і законність (в контексті забезпечення гарантій щодо невтручання у приватне, сімейне життя та кореспонденцію) і пропорційність такого втручання. Це може бути як один із можливих варіантів дотримання ст. 8 ЄКПЛ під час входження в «електронний простір» людини.

За результатами дослідження автором сформульовано низку висновків та

пропозицій змін до законодавства, спрямованих на удосконалення як нормативної регламентації, так і практики використання в кримінальному провадженні електронних доказів.

Ключові слова: верховенство права, докази, джерела доказів, досудове розслідування, електронний документ, електронні докази, кримінальний процес, кримінальне провадження, кримінальне правопорушення, міжнародні стандарти, обшук електронних пристроїв, спеціаліст, слідчі(розшукові) дії, слідчий суддя, права людини.

SUMMARY

Smal I. A. Theoretical principles of formation and practice of application of electronic evidence in criminal proceedings. – Qualifying scientific paper on manuscript rights.

Thesis for obtaining Doctor of Philosophy degree in specialty (081 – "Law"). – Penitentiary Academy of Ukraine, Chernihiv, 2025.

The thesis is a comprehensive scientific study aimed at solving a number of theoretical and applied issues related to the use of electronic evidence in the criminal process of Ukraine.

The research examined the origins, formation and development of the concept of electronic evidence in criminal proceedings through the prism of doctrinal approaches, judicial practice and technological progress. In order to identify promising areas for further scientific research, a comprehensive review of scientific sources, normative regulations and examples of practical application was carried out. Particular attention was paid to the impact of digitalization and the rapid development of information technologies on the formation of new forms of evidentiary information. Analysis of judicial practice has shown the presence of ambiguous approaches to the use of electronic evidence in criminal proceedings, which is largely due to the lack of a legally established definition of this concept in the current of Criminal Procedure Code of Ukraine.

The results of the study find out that electronic evidence is playing an increasingly important role in proving evidence, which necessitates the formation of a unified concept of its legal regulation and procedural use. It is the institutionalization of electronic evidence as a separate legal institution that can ensure legal certainty, strengthen human rights guarantees, and promote the efficiency of criminal justice. All this indicates the need for a comprehensive study of electronic evidence not only as a technical or evidentiary means, but as a legal phenomenon that is acquiring the characteristics of an independent institution.

In view of this, the paper identified the main periods of the formation of the institution of electronic evidence in criminal procedural law, which made it possible to trace the evolution of scientific views, regulatory consolidation and practical application in the context of technological progress. In particular, such periods include: Period I - 1970-2000. Formation of doctrinal approaches to the concept of "electronic document"; period II - 2001-2012. Further development of scientific ideas regarding information obtained from electronic sources and legislative consolidation of the term "electronic document"; period III - 2012-present period. Adoption of the Criminal Procedure Code of Ukraine, further doctrinal search for optimal models of using information in electronic form as evidence.

The characteristic peculiarities of electronic evidence are highlighted, such as reproducibility - the ability to copy without losing the original content; intangibility - they exist in the form of digital data, encoded in binary or other electronic signals and can be displayed only through special technical devices in digital format, which are stored, transmitted and processed using electronic devices; dynamism - the ability to change under the influence of software or user actions; dependence on technical media (special software or equipment is required to store, view, and verify electronic evidence); lack of a rigid link to the material medium (the possibility of the same information existing simultaneously on different, unrelated media); presence of metadata (electronic evidence contains metadata that is not the main content of the file, but helps determine its authenticity, time of creation, editing, authorship, etc.).

Special attention is paid to the study of the legal nature of electronic evidence, which contributed to the search for additional arguments regarding the need to distinguish electronic evidence as an independent procedural source.

The opinion of Ukrainian scientists - proceduralists about the need to allocate electronic evidence as a separate procedural source is supported and one's own argument on this issue is expressed. The legal nature of electronic evidence and its unique characteristics provide grounds for classifying it as an independent procedural source, and therefore will be sufficient argumentation for determining a separate procedure for obtaining evidentiary information, its research, and evaluation. Additional arguments justifying the need for such a step: 1) transformation of the information environment; 2) legal certainty and unification of judicial practice; 3) inconsistency of traditional sources of evidence with modern technological realities; 4) protection of the rights of participants in criminal proceedings; 5) European standards and international practice.

Attention is drawn to the existence of terminological diversity to designate such a "phenomenon" as electronic evidence, and the actual definition of this concept is formulated: *"Electronic evidence is information in electronic form containing information about circumstances that are relevant to criminal proceedings and are subject to proof, created, stored, or transmitted using electronic devices, systems, or networks and which exists in a form that ensures its authenticity, integrity, and suitability for research".*

An analysis of scientific approaches to the classification of electronic evidence proposed by domestic researchers was carried out and an author's classification of electronic evidence was developed, highlighting relevant criteria that take into account their origin, form, substantive nature and procedural features, namely: 1) by form of existence; 2) by method of formation; 3) by technical environment of existence. The theoretical and practical significance of the classification of electronic evidence has been proven, since it contributes to the adaptation of the criminal process to the conditions of the digital era, the formation of uniform standards of

evidence, taking into account the procedural features of their collection, storage, research and evaluation.

The provisions of criminal procedural legislation and practical aspects of using information in electronic form as evidence were systematically analyzed, and individual types of electronic evidence were examined in more detail, in particular, attention was focused on the problems of legal regulation of electronic documents and the practice of using them as evidence. The thesis that an electronic document is one of the types of electronic evidence was substantiated.

It has been established that the original of an electronic document is an electronic document with mandatory details, including the author's electronic signature or a signature equivalent to a handwritten signature in accordance with the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

A number of draft laws regulating the use of electronic evidence in criminal proceedings have been analyzed and it has been proven that the legislator's persistent ignoring of the specific nature of information in electronic form and attempts to situationally resolve problematic issues related to the use of such information in the process of providing evidence in criminal proceedings, which is manifested in numerous changes and additions to criminal procedural norms, only leads to a deepening of the problem of procedural security of using information in electronic form as evidence.

The concept of testimony of technical devices and technical means that have the function of photo-cinema, video recording or means of photo-cinema, video recording in criminal proceedings in the context of electronic evidence was investigated. When studying this type of electronic evidence, special attention was paid to the issues of inadmissibility of evidence and a proposal was substantiated on the need to make amendments to the Criminal Procedure Code of Ukraine aimed at ensuring the consistency and unity of judicial practice regarding the use of electronic evidence in criminal proceedings.

The opinion is substantiated that the testimony of technical devices and technical means that have the functions of photo and film shooting, video recording, or means of photo and film shooting, video recording, which are determined as an independent procedural source of evidence in criminal proceedings regarding criminal offenses, is nothing more than one of the types of electronic evidence. Amendments to Article 245-1 of the Criminal Procedure Code of Ukraine have been proposed, in particular regarding the need for terminological clarification — instead of “taking readings from technical devices and technical means”, the concept of “obtaining electronic data from technical devices and technical means” should be used, as well as to Article 3 of the Criminal Procedure Code of Ukraine, supplementing it with the definition of the term "electronic data" - this is information in electronic form that is suitable for human perception after processing by automatic software.

The peculiarities of using information from open sources as evidence were considered and the feasibility and prospects of further scientific research in this direction were substantiated. The author's own vision of the procedure for conducting such an investigative (detective) action as a review of computer data was formulated and a protocol for reviewing electronic data was developed.

One of the most controversial issues regarding the use of the definitions "original", "duplicate", "copy" in the context of electronic evidence has been studied in detail and the need for legislative consolidation of provisions regarding the need to confirm the authenticity of a copy of electronic evidence by using hashing or another method has been argued. That will ensure the possibility of verifying the authenticity and integrity of information and the proposed corresponding amendments to the Criminal Procedure Code of Ukraine.

It is concluded that the existence of electronic evidence in a specific environment, due to the use of certain technical means or devices and software, does not allow the categories of "original", "duplicate" and "copy" in their traditional meaning to be extended to electronic evidence. It is proposed to define in the Criminal

Procedure Code of Ukraine the possibilities of providing not only the original information in electronic form, but also its copy.

The logical part of the work was to consider problematic issues of observing the "right to privacy" during investigative (search) and covert investigative (search) actions. In this direction, a comprehensive analysis of the provisions of criminal procedural legislation, current international legal treaties, the practice of the European Court of Human Rights and, accordingly, national judicial practice was carried out, and amendments were proposed to the Criminal Procedure Code of Ukraine regarding the introduction of a new investigative (search) action — search of electronic devices that will ensure the fulfillment of the tasks of criminal proceedings defined by Article 2 of the Criminal Procedure Code of Ukraine and compliance with the proportionality of interference with the right to respect for one's private and family life and correspondence guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

It is emphasized that during the search (Part 6 of Article 236 of the Criminal Procedure Code of Ukraine) there is already an interference with the rights guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, even without the seizure of the relevant electronic devices. To ensure the right to respect for correspondence, a model of behavior of state agents is proposed, when the functions of the investigator and the person who reviews such information in electronic form will be separated (this may be an expert). There should be separate control over information that is not allowed to be disclosed (journalistic sources, attorney-client privilege, secret of the conference room, etc.). Information selected in this way should be controlled by the investigating judge before being transferred to the investigator for use in criminal proceedings as evidence. In this case, both the legality (in the context of ensuring guarantees of non-interference in private, family life and correspondence) and the proportionality of such interference will be ensured. This may be one of the possible options for complying with Article 8 of the European Convention for the Protection of Human

Rights and Fundamental Freedoms when entering a person's "electronic space".

Based on the results of the study, the author formulated a number of conclusions and proposals for changes to the legislation aimed at improving both regulatory regulation and the practice of using electronic evidence in criminal proceedings.

Key words: rule of law, evidence, sources of evidence, pre-trial investigation, electronic document, electronic evidence, criminal process, criminal proceedings, criminal offense, international standards, search of electronic devices, specialist, search actions, investigating judge, human rights.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких відображено основні результати дослідження:

1. Смаль І. А. Проблемні аспекти застосування електронних доказів у кримінальному судочинстві. *Право і суспільство*. 2021. № 4. С. 226–232. DOI: 10.32842/2078-3736/2021.4.30.

2. Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу. *Прикарпатський юридичний вісник*. Одеса, 2022. Вип. 2. С. 122–127. DOI: 10.32837/pyuv.v0i2.1028.

3. Смаль І. А. Практичні аспекти зняття показань технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі. *Юридичний науковий електронний журнал.* 2023. № 6. С. 552–558. DOI: https://doi.org/10.32782/2524-0374/2023-6/127.

4. Смаль І. А. Мережа Інтернету як джерело доказової інформації у кримінальному провадженні. *The Journal of Eastern European Law / Журнал східноєвропейського права*. 2024. № 128. С. 237–243. DOI: 10.32755/sjcriminal.2024.01.063.

Наукові праці, в яких засвідчено апробацію матеріалів дослідження:

1. Смаль І. А. Історичні передумови появи електронних доказів як засобів доказування в кримінальному процесі. *Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2020 : матеріали міжнар. наук.- практ. конф. (м. Чернігів, 23–24 квіт. 2020 р.)* : у 2 т. Чернігів : Акад. ДПтС, 2020. Т. 2. С. 266–268.

2. Смаль І. А. Перспективи використання електронних доказів як засобів доказування у кримінальному процесі. *Теорія та практика сучасної юриспруденції : матеріали XXVI всеукр. наук.-практ. конф. (м. Харків, 20 груд. 2020 р.)* : у 2 т. Харків : Нац. юрид. ун-т ім. Ярослава Мудрого, 2020. Т. 2. С. 324–326.

3. Остапчук Л. Г., Смаль І. А. Кіберзлочинність та електронні докази в кримінальному судочинстві. *Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2021 : матеріали міжнар. наук.- практ. конф. (м. Чернігів, 22–23 квіт. 2021 р.)* : у 2 т. Чернігів : Акад. ДПтС, 2021. Т. 2. С. 135–138.

4. Смаль І. А. Проблематика огляду носіїв цифрових даних через призму забезпечення прав та законних інтересів особи. *Інтеграція теорії у практику : проблеми, пошуки, перспективи : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 5 листоп. 2021 р.)*. Чернігів : Акад. ДПтС, 2021. С. 186–189.

5. Смаль І. А. Окремі аспекти збирання та процесуального закріплення інформації з електронних носіїв. *Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квіт. 2023 р.)* : у 2 т. Чернігів : Акад. ДПтС, 2023. Т. 1. С. 327–330.

6. Смаль І. А. Межі втручання у приватне спілкування під час збирання електронних доказів у кримінальному процесі. *Трансформації особистості, суспільства та ринку праці: виклики майбутнього та вплив на освіту : зб. тез доп. міжнар. наук.-практ. конф., м. Харків, 20–22 верес. 2023 р*. Харків : ХНУ ім. В. Н. Каразіна, 2023. С. 440–441.

7. Смаль І. А. Втручання у право на приватність під час здійснення досудового розслідування у вимірі стандартів статті 8 Конвенції про захист прав людини і основоположних свобод. *Кримінальний процес: сучасний вимір та перспективні тенденції : матеріали VI Харків. кримін. процес. полілогу (м. Харків, 17 квіт. 2024 р.)*. Харків : Право, 2024. С. 138–143.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВАКС – Вищий антикорупційний суд України

ВП ВС – Велика палата Верховного Суду

ВР— Верховна Рада

ВС – Верховний Суд

ГПК – Господарський процесуальний кодекс України

ЕОМ - Електронно-обчислювані машини

ЄДРСР – Єдиний державний реєстр судових рішень

ЄКПЛ або Конвенція – Конвенція про захист прав людини та основоположних свобод

ЄРДР – Єдиний реєстр досудових розслідувань

ЄСПЛ або Суд або Євросуд – Європейський суд з прав людини

ЗУ – Закон України

КАС – Кодекс адміністративного судочинства України

ККС ВС – Касаційний кримінальний суд Верховного Суду

КПК Естонії – Кримінально-процесуальний кодекс Естонії

КПК Латвії – Кримінально-процесуальний кодекс Латвії

КПК Литви – Кримінально-процесуальний кодекс Литви

КПК – Кримінальний процесуальний кодекс України

КПК ФРН – Кримінально-процесуальний кодекс Федеративної Республіки Німеччина

КСУ – Конституційний Суд України

НС(Р)Д – негласні слідча (розшукові) дії

ООН – Організація Об’єднаних Націй

ОП ВС – Об'єднана палата Верховного Суду

С(Р)Д – слідчі (розшукові) дії

ЦПК – Цивільний процесуальний кодекс України

ВСТУП

Обґрунтування вибору теми дослідження. Світ, у якому ми живемо, не можливо уявити без новітніх інформаційно-цифрових та комунікаційних технологій. Ми щодня користуємось мобільним зв'язком, електронною поштою, месенджерами, інтернет-банкінгом та іншими цифровими ресурсами як у повсякденному житті, так і в професійній діяльності. Науковий прогрес не оминув і сферу суспільних відносин в кримінальному провадженні, що в своєю чергою, призвело до того, що у кримінальному процесі електронні пристрої, що містять значний обсяг інформації в електронному вигляді, все частіше стають об'єктами дослідження. Для того, щоб органи досудового розслідування та суду могли ефективно використовувати цю інформацію як доказ, необхідно враховувати особливості її збирання, зберігання, дослідження та оцінки.

Сучасні кримінальні правопорушення, пов'язані з використанням цифрових технологій, дедалі більше впливають на приватне життя мільйонів людей у всьому світі. Так, кібератаки, злам фінансових акаунтів, втручання в електронні системи, викрадення та незаконне використання персональних даних — усе це підриває основи демократичного суспільства та громадської безпеки.

З огляду на швидкий розвиток цифрових технологій та зростання кіберзлочинності, кримінальне процесуальне законодавство України, особливо в умовах правового режиму воєнного стану має своєчасно адаптуватися до нових викликів. Цьому може слугувати вдосконалення правових механізмів збору, збереження, дослідження та оцінки електронних доказів, а також забезпечення ефективного міжнародного співробітництва у сфері протидії та запобігання кримінальним правопорушенням.

Вибір теми дослідження зумовлений її актуальністю для правозастосовної практики у сфері кримінального судочинства, оскільки електронні докази відіграють ключову роль у розслідуванні кримінальних правопорушень. Однак, для їх ефективного використання у кримінальному провадженні необхідно розробити

чіткі процесуальні механізми, що забезпечують надійну ідентифікацію, збереження інформації в електронному вигляді, адже електронні дані можуть бути вразливими до змін, знищення або фальсифікації. Це, в свою чергу, передбачає вдосконалення законодавчого регулювання, підготовки кваліфікованих фахівців та розширення технічних можливостей правоохоронних органів та судової системи. Законодавчий процес у сфері використання електронних доказів має ґрунтуватися на всебічному науковому аналізі, що охоплює як теоретичне обґрунтування правових норм, так і вивчення практики їх застосування. Непродумані або недостатньо обґрунтовані законодавчі ініціативи можуть створити серйозні труднощі у правозастосуванні.

Тому результатом проведеного нами дослідження стали конкретні пропозиції щодо вдосконалення законодавства, які відповідають сучасним технологічним реаліям та практичним потребам кримінального процесу в Україні. Технічний прогрес на стільки змінив нормативне регулювання, правозастосування, що вимагає перегляду стандартів підготовки фахівців. Програми навчання слідчих, дізнавачів, прокурорів і суддів повинні включати основи цифрової грамотності, адже без неї ефективна робота в сучасних умовах стає неможливою.

Крім того, проблема використання електронних доказів у кримінальному провадженні набуває ще більшої актуальності у зв’язку з тим, що цифровізація кримінального процесу прямо пов’язана з питаннями захисту прав людини. Входження в електронний простір під час проведення досудового розслідування досить часто супроводжується втручанням у приватне життя, а отже може порушувати права, гарантовані як Конституцією України, так і Конвенцією про захист прав людини і основоположних свобод.

Додатковим чинником актуалізації досліджуваної проблематики є події, що відбуваються в Україні з 2014 року. Збройний конфлікт, який 24 лютого 2022 року переріс у повномасштабну військову агресію російської федерації проти України, створив безпрецендентні виклики для правоохоронної та судової системи. Умови воєнного стану вимагають розслідування значної кількості воєнних злочинів, багато з яких фіксуються саме з допомогою цифрових технологій. Відео та

фотодокази, електронні документи, перехоплення комунікацій, записи з безпілотних летальних апаратів і супутникові дані стали невід'ємною частиною доказової бази у справах про воєнні злочини.

Однак, чинне кримінальне процесуальне законодавство виявилося недостатньо адаптованим до сучасних цифрових реалій. Відсутність чітких процедур збирання, перевірки та оцінки електронних доказів ускладнює їх використання у кримінальному провадженні, веде до відсутності єдності судової практики, що зрештою негативно позначається на правозастосуванні.

Отже, тема дисертаційного дослідження є надзвичайно актуальною, оскільки її результати можуть сприяти формуванню теоретичної бази для адаптації кримінального процесу до цифрових викликів сьогодення та майбутнього. Відсутність належного нормативного регулювання електронних доказів у кримінальному судочинстві впливає на неоднозначність судової практики щодо їх використання у кримінальних провадженнях.

Проблематика використання електронних доказів вже тривалий час перебуває в центрі уваги наукової спільноти. Дослідники аналізують різні аспекти цього питання, зокрема, правову природу електронних доказів, їхню допустимість, способи збирання, збереження та оцінки у кримінальному процесі. У сфері кримінального процесу питання електронних доказів досліджували такі українські вчені, як Д. О. Алєксєєва-Процюк, П. Є. Антонюк, Н. М. Ахтирська, М. В. Багрій, І. Г. Богатирьов, О. М. Брисковська, Д. Гавловський, І. В. Гловюк, С. І. Гонгало, М. В. Гуцалюк, М. І. Демура, С. В. Івашко, І. Г. Каланча, О. В. Капліна, А. В. Коваленко, С. О. Ковальчук, О. Г. Козицька, Д. І. Клепка, І. О. Крицька, Д. О. Літкевич, О. П. Метелев, І. Ю. Мірошников, В. В. Мурадов, Ю. Ю. Орлов, А. В. Ратнова, О. В. Сіренко, Г. Г. Січкаренко, А. В. Скрипник, В. І. Сліпченко, А. В. Столітній, С. Р. Тагієв, І. А. Тітко, В. Г. Хахановський, Є. С. Хижняк, Д. М. Цехан, С. С. Чернявський.

В цивільному процесі різні аспекти досліджуваної тематики вивчали: А. Ю. Каламайко, В. В. Комаров, О. М. Лазько, А. Ю. Луспеник, Д. О. Москвичук;

у господарському процесі: І. В. Булгакова, А. М. Найченко, О. О. Присяжнюк, О. М. Стороженко, А. М. Найченко; в адміністративному судочинстві: Н. Є. Блажівська, І. В. Казачук.

Напрацювання у сфері цивільного, господарського та адміністративного процесуального права мають важливе значення і для кримінального процесу, оскільки багато правових питань, пов'язаних із електронними доказами, є спільними для різних юрисдикцій. Зокрема, це стосується проблеми визначення електронного доказу як джерела доказів, вимог до його автентифікації, стандартів доказування. Водночас кримінальний процес має свою специфіку, що вимагає подальшого глибокого дослідження особливостей збирання, зберігання, використання електронних доказів у кримінальному процесі.

Попри значний внесок науковців у розробку проблематики електронних доказів, низка ключових теоретичних і практичних аспектів використання інформації в електронному вигляді у кримінальному процесуальному доказуванні досі залишається недостатньо дослідженою або не має однозначного вирішення.

Насамперед важливим є комплексний аналіз понятійного апарату, оскільки термінологія, що використовується у нормативних актах і правозастосовній практиці, залишається неоднозначною. Зокрема, досі існують наукові дискусії щодо використання понять «копія», «оригінал», «дублікат» електронного доказу, а відповідно відсутність чіткого нормативного регулювання цих понять відображається на судовій практиці.

Крім того, дискусійним залишається питання про необхідність виокремлення електронних доказів як окремого процесуального джерела, що потребує більш глибокого теоретичного та практичного обґрунтування. Особливу увагу слід приділити питанням автентичності та достовірності електронних доказів у кримінальних провадженнях, адже відсутність чітких критеріїв їхньої оцінки може впливати на законність судового рішення.

Окремим напрямом, що потребує подальшого дослідження, є правові аспекти проведення обшуку електронних пристроїв, адже такі пристрої містять великий

обсяг інформації, що може призвести до надмірного втручання у приватне життя людини і існування ризику зловживання з боку правоохоронних органів. Саме актуальність цих проблем визначило вибір теми дисертації та окреслила основні напрями дослідження, спрямовані на вдосконалення теоретичних і практичних підходів застосування електронних доказів у кримінальному процесі.[1]

З огляду на висловлене можемо констатувати, що нині існує необхідність проведення комплексного наукового дослідження, виробленні науково обґрунтованих пропозицій з удосконалення чинного кримінального процесуального законодавства в частині використанні електронних доказів в процесі доказування.

Зв'язок роботи з науковими програмами, планами, темами. Обрана тема ґрунтується на положеннях Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу (затвердженій Законом України від 18 березня 2004 р. № 1629-IV), Національної стратегії у сфері прав людини (затвердженій Указом Президента України від 24 березня 2021 р. № 119/2021), Стратегії розвитку системи правосуддя та конституційного судочинства на 2021–2023 р.р. (затвердженій Указом Президента України від 11 червня 2021 р. № 231/2021), Пріоритетних напрямів розвитку правової науки на 2016–2020 роки (затверджених постановою загальних зборів Національної академії правових наук України від 3 березня 2016 р.), Плані реалізації Стратегії кібербезпеки України

[1] Принагідно хочемо зазначити, що в процесі дослідження нами усвідомлено, що термін «застосування електронних доказів», який міститься в назві дисертації може не зовсім точно відображати зміст окремих процесуальних дій, зокрема, тих, які зазвичай асоціюються з терміном «використання електронних доказів». Водночас обраний нами термін «застосування» вжито свідомо — у широкому правозастосовному значенні , яке охоплює всю сукупність дій, пов'язаних з електронними доказами. Адже застосування електронних доказів—це не лише їх використання як джерела інформації, а й комплекс процесуальних, технічних та юридичних заходів, спрямованих на отримання, збирання, збереження, аналіз, автентифікацію та представлення в процесуальній формі. Це поняття також охоплює використання сучасних цифрових технологій та електронних пристроїв для забезпечення достовірності, автентичності та цілосності електронних даних. Використання електронних доказів у кримінальному провадженні — це комплекс саме процесуальних заходів, спрямованих на збирання, отримання, збереження, дослідження та оцінку інформації в електронному вигляді як доказу. У цій дисертації ми переважно використовуватимемо термін «використання електронних доказів», оскільки він краще розкриває змістовне наповнювання дослідження та дозволяє більш точно визначити сутність аналізованих процесуальних аспектів.

відповідно до Рішення Ради національної безпеки і оборони України від 30 грудня 2021 року, введеного в дію Указом Президента України від 1 лютого 2022 року № 37/2022.

Дисертацію виконано на кафедрі кримінально-виконавчого та кримінального права в рамках науково-дослідних робіт кафедри ННІ права, правоохоронної діяльності та психології Пенітенціарної академії України в рамках науково-дослідних робіт на 2017–2021 роки на тему «Права і свободи людини і громадянина та їх захист кримінально-правовими, кримінально-виконавчими засобами й системою заходів запобігання злочинам» (державний реєстраційний номер 0117u007206) і на 2022–2026 роки на тему «Проблеми запровадження та застосування кримінально-правових засобів реагування в умовах реформування законодавства України про публічно-правову відповідальність» (державний реєстраційний номер 0122U002480).Тема дисертаційної роботи затверджена вченою радою Пенітенціарної академії України 20 грудня 2019 року (протокол №16).

Мета і завдання дослідження. Метою роботи є отримання в процесі проведеного дослідження нових результатів та наукових висновків щодо використання електронних доказів у кримінальному процесуальному доказуванні, удосконалення чинного кримінального процесуального законодавства України та практики його застосування.

Досягнення поставленої мети зумовила необхідність вирішення таких завдань:

дослідити витоки, становлення та розвиток концепції електронних доказів у кримінальному процесі крізь призму доктрини, практики та технологічного прогресу та визначити основні періоди становлення інституту електронних доказів у кримінальному процесуальному праві;

− вивчити правову природу електронних доказів у кримінальному процесі;

– з’ясувати характерні ознаки електронних доказів та їх місце в системі процесуальних джерел доказів;

– узагальнити існуючі наукові підходи до класифікації електронних доказів та запропонувати власну класифікацію електронних доказів у кримінальному процесі;

– надати характеристику електронного документу як різновиду електронного доказу та його співвідношення з іншими видами доказів;

– довести, що Інтернет може бути джерелом доказів, що мають електронну форму;

– охарактеризувати правову природу показань технічних приладів та технічних засобів, що використовується у ст.245-1 КПК України як можливого різновиду електронних доказів;

– вивчити та узагальнити наукові погляди та судову практику щодо категорій «оригінал», «дублікат» та «копія» електронних доказів у кримінальному провадженні та висловити власне бачення;

– проаналізувати актуальні питання імплементації практики Європейського суду з прав людини щодо забезпечення дотримання прав, передбачених ст.8 ЄКПЛ, у контексті проведення обшуку електронних пристроїв у кримінальних провадженнях;

– сформулювати науково обґрунтовані пропозиції з удосконалення правового регулювання і практики використання електронних доказів у кримінальному процесуальному доказуванні.

Об'єктом дослідження є суспільні відносини, які регулюють використання інформації з електронних носіїв у кримінальному процесуальному доказуванні, в практичній діяльності органів досудового розслідування та в судовій практиці.

Предметом дослідження є теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі.

Методи дослідження вибрані з урахуванням специфіки мети і завдань дослідження, його об'єкта та предмета. Для досягнення поставленої мети та формулювання обґрунтованих висновків у процесі роботи використано комплекс загальнонаукових і спеціальних методів наукового дослідження, що є

традиційними для правової науки: діалектичний, формально-логічний, герменевтичний, узагальнення та порівняльно-правовий. Так, діалектичний метод дозволяє осмислити поставлену мету дослідження та завдання, які необхідно виконати для її реалізації та дослідити електронні докази як правову категорію(підрозділи 1.1, 1.2), розкрити окремі аспекти втручання у права прав людини під час отримання доказової інформації у електронному вигляді (підрозділ 3.3); герменевтичний, за яким з'ясовано правовий зміст норм КПК та законодавчих пропозицій та виявлені дефекти нормативного регулювання (підрозділи 2.2, 2.3, 3.1,3.2,3.3). Історико-правовий метод використовується для дослідження історичних аспектів розвитку та становлення інституту електронних доказів у кримінальному процесуальному праві України (підрозділ 1.1). Порівняльно-правовий метод дозволив дослідити та порівняти поняття електронних доказів у кримінальному процесі та інших галузях права для подальшого вдосконалення кримінального процесуального законодавства України, осмислити правові проблеми пов’язані з практикою використання електронних доказів та їх місце у системі процесуальних джерел доказів (підрозділи 1.2, 1.3). Водночас, даний метод надав можливість порівняти категорій «оригінал», «дублікат», «копія» та дослідити їх практичне значення у правозастосовній практиці та зробити висновок про необхідність законодавчо закріплення необхідності підтвердження автентичності отриманої інформації в електронному вигляді (підрозділ 3.2). Формально-логічний метод став підґрунтям для розкриття та вдосконалення поняття електронного доказу, співставлення його з іншими поняттями, які використовуються в законодавстві та доктрині (підрозділи 1.2, 1.3). Застосування системно-структурного методу дозволило відмежувати електронні докази від інших видів доказів (підрозділ 1.3). Під час проведення анкетування та узагальнення його результатів використано метод конкретно-соціологічних досліджень (Додатки № А, Б). Методи аналізу, синтезу та індукції дозволили виявити та дослідити правові аспекти використання електронних доказів у процесі доказування, сформулювати основні характерні ознаки електронних доказів та виявити у судовій

практиці проблеми, пов’язані з використання інформації в електронному вигляді та напрацювати шляхи їх вирішення. Метод узагальнення надав можливість сформулювати обґрунтовані висновки, спрямовані на вдосконалення нормативної регламентації досліджуваних питань, подолання проблем, що мають місце в правозастосовній практиці (розділи 1, 2, 3). Зазначені методи використовувалися у взаємозв’язку, що сприяло повноті дослідження й обґрунтованості сформульованих наукових висновків і пропозицій.

Використання комплексу перелічених вище методів сприяло формуванню повного і всебічного уявлення про предмет дослідження, а також забезпеченню й обґрунтованості сформульованих наукових висновків і пропозицій

Емпіричну базу дослідження складають рішення ЄСПЛ, рішення Конституційного Суду України, рішення Верховного Суду, матеріали проведеного узагальнення судової практики, під час якого опрацьовано понад 570 судових рішень, внесених до Єдиного державного реєстру судових рішень. У межах дослідження проведено анкетування, під час якого опитано 1289 практичних працівників у сфері кримінального судочинства: суддів, прокурорів, слідчих, дізнавачів та адвокатів.

Наукова новизна отриманих результатів. Дисертація є одним із самостійних комплексних досліджень теоретичних засад формування і практики використання електронних доказів у кримінальному процесі, в якій на основі аналізу проблем нормативно-правового та правозастосовного характеру розкрито особливості використання електронних доказів у кримінальних провадженнях з урахуванням європейських правових стандартів справедливого правосуддя та забезпечення прав учасників кримінального провадження, а також надано обґрунтовані пропозиції щодо вдосконалення чинного кримінального процесуального законодавства та практики його застосування в Україні.

Уперше дисертантом:

– досліджено витоки, становлення та розвиток концепції електронних доказів у кримінальному процесі крізь призму доктринальних підходів, судової

практики та технологічного прогресу. Виокремлено основні періоди формування інституту електронних доказів у кримінальному процесуальному праві: І період— 1970-2000 р. Становлення доктринальних підходів щодо поняття «електронний документ»; ІІ період — 2001-2012 р. Подальший розвиток наукових уявлень щодо інформації, отриманої з електронних джерел та законодавче закріплення терміну « електронний документ»; ІІІ період— 2012-сучасний період. Прийняття КПК України, подальший доктринальний пошук оптимальних моделей використання інформації в електронному вигляді як доказу.

– сформульовано авторське визначення поняття електронний доказ – це інформація в електронному вигляді, що містить відомості про обставини, що мають значення для кримінального проводження та підлягають доказуванню, створена, збережена, або передана за допомогою електронних пристроїв, систем, або мереж та яка існує в формі, що забезпечує її автентичність, цілісність та придатність для дослідження.

– з’ясовано специфіку використання як доказу показань технічних приладів і технічних засобів, що мають функції фото і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису та надано пропозицію щодо внесення змін до кримінального процесуального законодавства щодо застосування такої слідчої (розшукової)дії як зняття показань технічних приладів і технічних засобів, що мають функції фото і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису;

– системно проаналізовано положення кримінального процесуального законодавства щодо такого різновиду огляду як огляд комп’ютерних даних в контексті перспективності використання Інтернету як джерела доказів, що мають електронну форму та розроблені пропозиції щодо процесуального оформлення такої слідчої(розшукової) дії.

Удосконалено:

– наукові підходи українських учених щодо теоретичних та практичних

напрацювань правової природи електронних доказів, їх унікальних ознак та необхідності виділення електронних доказів в окреме процесуальне джерело;

– теоретичні уявлення про правовий статус електронних документів та інших видів електронних доказів;

– наукові розробки, спрямовані на забезпечення законодавчого унормування обов'язкового підтвердження автентичності отриманої доказової інформації в електронному вигляді шляхом хешування або обов'язкового призначення експертизи;

– обґрунтування наукової позиції щодо використання понять «оригінал», «дублікат», «копія» у контексті електронних доказів;

Набули подальшого розвитку:

– наукові розробки щодо необхідності запровадження різновиду слідчої (розшукової) дії обшук – обшук електронних пристроїв;

– пропозиції щодо вдосконалення кримінального процесуального законодавства шляхом внесення окремої глави щодо електронних доказів до КПК України;

– доктринальні погляди щодо необхідності врахування практики ЄСПЛ під час проведення обшуку електронних пристроїв та напрацьовані зміни до кримінального процесуального законодавства, якими буде забезпечено виконання завдань кримінального провадження, визначених ст. 2 Кримінального процесуального кодексу України та дотримання пропорційності втручання в гарантовані Конституцією України та ст. 8 ЄКПЛ право на повагу до свого приватного і сімейного життя, кореспонденції.

Практичне значення отриманих результатів полягає в тому, що авторські висновки і пропозиції, сформульовані у дисертації, можуть бути використані у:

– науково-дослідній діяльності – для подальшої розробки теоретичних і практичних проблем кримінального процесуального доказування. Акт про впровадження результатів дисертаційного дослідження аналітичної та правової роботи Касаційного кримінального суду Верховного суду від 25.09.2024 р.;

– у нормотворчій діяльності – при вдосконаленні кримінального процесуального законодавства України. Акт про впровадження результатів дисертаційного дослідження комітету Верховної Ради України з питань правоохоронної діяльності від 03.10.2024 р.;

– у правозастосовній діяльності — з метою надання практичної допомоги дізнавачам, слідчим, прокурорам, суддям у використанні електронних доказів у кримінальному процесі України. Акт про впровадження результатів дисертаційного дослідження Тренінгового центру прокурорів України від 26.06.2024 р.; Акт про впровадження результатів дисертаційного дослідження Національної школи суддів України від 24.07.2024 р.;

– у навчальному процесі — під час викладання курсу кримінального процесу та інших кримінально- процесуальних дисциплін, а також підготовки навчально-методичних матеріалів з кримінального процесу (підручників, навчальних посібників тощо). Акт про впровадження результатів дисертаційного дослідження Національного юридичного університету імені Ярослава Мудрого від 16.08.2024 р..

Особистий внесок здобувача. Дисертація є самостійним комплексним дослідженням, яке відображає особистий здобуток автора. В опублікованих у співавторстві працях становлять власні теоретичні розробки дисертанта, авторська частка яких складає 50 %. Наукові ідеї, що належать співавторам опублікованих праць, у дисертації не використовувалися.

Апробація матеріалів дисертації. Дисертацію підготовлено на кафедрі кримінального, кримінально-виконавчого права та кримінології Пенітенціарної академії України, схвалено і рекомендовано до захисту. Основні положення дисертації оприлюднювалися і були предметом обговорення на міжнародних, всеукраїнських, всеукраїнських за міжнародною участю конференціях, полілогах, зокрема: «Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2020» (м. Чернігів, 23–24 квітня 2020 р.); «Теорія та практика сучасної юриспруденції» (м. Харків, 20 грудня 2020 р.); «Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук

– 2021» (м. Чернігів, 22–23 квітня 2021 р.); «Інтеграція теорії у практику: проблеми, пошуки, перспективи» (м. Чернігів, 5 листопада 2021 р.); «Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану – 2023» (м. Чернігів, 25–26 квітня 2023 р.); «Трансформації особистості, суспільства та ринку праці: виклики майбутнього та вплив на освіту» (м. Харків, – 22 вересня 2023 р.); VI Харківського кримінально процесуального полілогу «Кримінальний процес: сучасний вимір та перспективні тенденції» (м. Харків, 17 квітня 2024 р.).

Публікації. Основні положення та висновки, що сформульовані в дисертації, викладено у десятьох наукових публікаціях, серед яких чотири статті – у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук (одна у співавторстві з Остапчук Л. Г), а також у семи тезах, опублікованих у збірниках доповідей науково-практичних конференцій та полілозі.

Структура та обсяг дисертації визначені відповідно до мети, завдань, а також специфіки об’єкта і предмета дослідження. Робота складається зі вступу, трьох розділів, 9 підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 329 сторінок, з яких основний текст викладено на 212 сторінках, а список використаних джерел (421 найменувань) – 53 сторінки, додатки- 62 сторінки.

РОЗДІЛ І
ПРАВОВА ПРИРОДА ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

1.1. Витоки, становлення та розвиток концепції електронних доказів у кримінальному процесі крізь призму доктрини, практики та технологічного процесу

У сучасному світі процеси глобалізації та інформатизації суттєво впливають на всі сфери життя, зокрема і на кримінальне судочинство. Саме розвиток інформаційних технологій призвів до появи нового виду доказів — електронних доказів, які набувають все більшого значення у кримінальному процесі. З огляду на їхню специфіку, такі докази не лише розширюють межі доказової бази, а й висувають нові вимоги до їх збирання, зберігання та оцінки, що вимагає адаптації правозастосовної практики та переосмислення традиційних підходів до доказування.

Саме тому в процесі дослідження ми звертаємо до історичних аспектів формування концепції електронних доказів, щоб простежити періоди становлення і розвиток інституту електронних доказів у кримінальному процесуальному праві. зрозуміти передумови виникнення електронних доказів та оцінити наскільки сучасні підходи узгоджуються з основоположними принципами доказового права. Це дозволить оцінити правові підстави використання електронних доказів у кримінальному процесуальному доказуванні та визначити наскільки сучасні підходи відповідають основоположним принципами доказового права.

Адже, як зазначає О. В. Шведова «історичне дослідження будь-якої галузі науки має дуже важливе значення, бо дає цілу систему важливих прецедентів і є емпіричною основою як для створення загальної теорії науки, так і для узагальнення певних практичних рекомендацій» [360, с. 14].

З метою визначення напрямів дослідження, які на сьогодні є найбільш актуальними для наукового осмислення, вважаємо за необхідне провести комплексний огляд наукових джерел, автори яких тим чи іншим чином торкалися тематики електронних доказів. Це дозволить констатувати, що сталі наукові уявлення про систему кримінального процесуального права, термінологію, яка склалася у вітчизняній процесуальній теорії, підходи до багатьох положень теорії доказів повинні бути ретельно переглянуті науковцями. Однак мова не йде про докорінні зміни у правосвідомості науковців та практиків.

Нова правова реальність, на формування якої впливає науково-технічний прогрес,[2] [див. до примітки 81] потребує перегляду багатьох уявлень про сутність окремих кримінальних процесуальних інститутів для їх ефективної реалізації. В першу чергу це стосується кримінального процесуального доказування [110, с.67].

Становлення і розвиток електронних доказів як самостійного правового інституту є надзвичайно актуальним у контексті цифровізації сучасного суспільства. Зростання кількості правовідносин, що відбуваються у віртуальному просторі, зумовлює стрімке збільшення випадків використання інформації в електронному вигляді у кримінальному провадженні. Це, у свою чергу, висуває нові вимоги до процесуального регулювання та теоретичного осмислення таких доказів. Незважаючи на те, що електронні докази вже активно застосовуються в правозастосовній практиці, їхнє законодавче визначення залишається фрагментарним і неповним. Наукова доктрина також не виробила єдиної позиції щодо правової природи електронних доказів, що зумовлює неоднозначність у підходах до їх оцінки, допустимості та належності. Актуальним є й питання

---

[2] Інформаційна революція — це метафора, яка відображає революційний вплив інформаційних технологій на всі сфери життя суспільства в останній чверті XX сторіччя. 70-ті роки XX ст. називають четвертою інформаційною революцією, яка зумовлена винаходом мікропроцесорної технології і персонального комп'ютера. Вона характеризується переходом від механічних, електричних засобів перетворення інформації до електронних та створення програмного забезпечення цього процесу. «Вінцем» цього етапу є поява всесвітньої мережі – Інтернету, що уможливило інформаційний обмін в глобальних масштабах.

гармонізації національного кримінального процесуального законодавства із міжнародними стандартами, зокрема у сфері забезпечення права на справедливий суд.

Саме інституціоналізація електронних доказів, як окремого правового інституту, здатна забезпечити правову визначеність, посилити гарантії прав людини та сприяти ефективності кримінального судочинства. Усе це свідчить про потребу в комплексному дослідженні електронних доказів не лише як технічного чи доказового засобу, а як правового явища, що набуває ознак самостійного інституту.

Перш ніж перейти до розгляду вказаного питання, зауважимо, що деякі учені розглядають інституціоналізацію не лише як технічну сторону утворення нового інституту, а більш як змістовний процес [118, с. 29].

Поняття інституціоналізації дозволяє виражати процеси трансформації соціальних явищ і відносин зі статусу неформалізованих в статус формалізованих об'єктів і тому можна зробити висновок, що в усіх випадках мова йде про процес запровадження/виникнення інститутів (інститутоґенез) [118, с. 30].

Процес виникнення, формування та розвитку електронних доказів в доктрині, законодавстві та правозастосовній практиці дозволяє нам виокремити основні періоди становлення інституту електронних доказів у кримінальному процесі, розглянути та комплексно проаналізувати кожен з них, а також виявити їх особливості. Це в свою чергу дозволить нам стверджувати, що становлення інституту електронних доказів та формування доктринальних уявлень про них є взаємопов’язаними процесами, що можуть бути проаналізовані крізь призму хронологічного, змістовного та нормативного розвитку.

Нами уже було доведено, ґенеза уявлень про електронні докази фактично передує та супроводжує становлення правового інституту електронних доказів у кримінальному процесуальному праві, а отже сприятиме визначенню природи електронних доказів та відповідно їх законодавчому регулюванню [257].

Еволюція доктринальних підходів та правозастосовної практики включає появу ідеї про можливість використання інформації в електронному вигляді у доказуванні; розширення наукових досліджень у сфері електронних доказів; формування загальноприйнятих підходів до визначення правової природи, ознак електронних доказів. Цей процес відбувався поступово, у відповідь на розвиток інформаційних технологій та поширення кіберзлочинності.

Осягнувши щонайменше зазначені аспекти, нами в процесі дослідження сформоване цілісне уявлення необхідне для проведення ґрунтовного теоретико-практичного аналізу. Огляд наукових джерел буде здійснено відповідно до окреслених дослідницьких напрямів, із дотриманням хронологічного підходу, що дозволить простежити еволюцію наукових поглядів і тенденції їхнього розвитку. У межах проведеного нами дослідження аналізується не лише науковий доробок учених щодо електронних доказів, а й процес їх нормативного закріплення. Важливо, що цей аналіз проводитиметься з урахуванням трьох ключових періодів, кожен із яких відображатиме певний рівень формування наукових уявлень та правових концепцій. Таким чином, дослідження структуровано охопить як загальну динаміку наукових розвідок, так і специфічні особливості кожного періоду. Особлива увага приділятиметься працям вітчизняних учених, оскільки їхні дослідження становлять ключову основу для подальшого аналізу та осмислення проблематики.

Визначення періодів становлення та розвитку інституту електронних доказів у кримінальному процесуальному праві ґрунтується на аналізі еволюції *правового регулювання електронних доказів, розвитку судової практики,* а також на *наукових напрацюваннях у цій сфері.*

Такий підхід дає змогу простежити зміни у правовому та практичному підході до електронних доказів, враховуючи внесок наукової спільноти у формуванні їхнього сучасного розуміння. Це надасть нам можливість чітко показати, як на різних періодах змінювалося розуміння поняття електронні докази.

В наукових дослідженнях спочатку застосовувалося поняття «електронний документ», що згодом знайшло своє закріплення в національному законодавстві України (Закон України «Про електронні документи та електронний документообіг») [223]. Пізніше, з розвитком цифрових технологій учені стали говорити про «електронні докази», розумуючи під ними значно більше ніж електронний документ. На відміну від іншого законодавства (цивільного, адміністративного, господарського) в КПК України не знайшло закріплення визначення поняття електронного доказу, що є незрозумілим підходом законодавця, та негативно позначається на правозастосуванні.

За темпоральним принципом, залежно від наведених вище критеріїв, можливо виокремити такі основні періоди становлення та розвитку інституту електронних доказів у кримінальному процесуальному праві:

І період— 1970-2000 р. Становлення доктринальних підходів щодо поняття «електронний документ»;

ІІ період — 2001-2012 р. Подальший розвиток наукових уявлень щодо інформації, отриманої з електронних джерел та законодавче закріплення терміну « електронний документ»;

ІІІ період— 2012-сучасний період. Прийняття КПК України, подальший доктринальний пошук оптимальних моделей використання інформації в електронному вигляді як доказу .

Піддаючи аналізу виокремлений нами перший період становлення та розвитку інституту електронних доказів, варто констатувати, що для цього періоду характерним є стрімкий розвиток науково-технічного прогресу в XIX ст., який в свою чергу сприяв винайденню засобів для створення аудіовізуальних документів[3] [до примітки див. 249, с. 41].

---

[3] Так, перший фотоапарат А. Ф. Грекова з'явився в 1840 р., перші спроби відтворення звукової інформації спеціальним пристроєм – фонографом, належать Т. А. Едісону (1857 р.), перший засіб для відтворення безперервного руху зображень на екрані запропоновано Луї де Пренсом у 1893 р. Створений у 1943 р. Максом Н'юменом перший 1500-ламповий комп'ютер став потужним імпульсом для розробки й вдосконалення нових поколінь комп'ютерної техніки, включаючи сучасні кишенькові ПК.

Починаючи з кінця XX ст. паперові носії поступово втрачають статус основного засобу збереження інформації. Зі зростанням обсягів даних виникла потреба у більш компактних та зручних пристроях для зберігання. Це сприяло появі різноманітних мікроносіїв інформації: магнітних стрічок, плівок, мікрокарт, дисків тощо. Поряд з ними використовувалися перфоносії, зокрема перфострічки та перфокарти, а згодом і електронні носії (дискети, оптичні диски та флеш-накопичувачі).

Сам термін «електронний документ» виник у в 1970–х роках XX століття разом із появою так званих машинних документів.

Одним із перших нормативно-правових актів, що визначали поняття електронного документу стали Інструктивні вказівки Держарбітражу СРСР від 29.06.1979 р. "Про використання як доказів в арбітражних справах документів, підготовлених за допомогою електронно-обчислювальної техніки"[4] [до примітки див. 139].

Вітчизняний науковець криміналіст В. К. Лисиченко одним із перших почав говорити про необхідність трансформації доказів у кримінальному процесі та появу нового виду документів. У своєму дисертаційному дослідженні ще в 1974 році науковець вказує на те, що широке впровадження обчислювальної техніки «створює об'єктивні підстави для того, щоб відомості про факти і практичну діяльність людей, які закріплені знаками штучних мовних систем (машинних мов), розглядались у загальнонауковому і правовому сенсі як самостійний різновид документів» [121, с. 49]. У зв'язку з цим, він вважав необхідним врегулювання питання про доказове значення носіїв фактичної інформації, зафіксованої за допомогою таких засобів [121, с. 11–12].

[4] У цих вказівках до електронних документів відносили всі документи, із застосуванням електронно-обчислювальної техніки. Відповідно до пункту 9 цього документа, дані, що зберігаються на технічних носіях, зокрема перфострічках, перфокартах, магнітних стрічках, магнітних дисках, можуть використовуватися як докази у справі за умови їхнього перетворення у форму придатну для звичайного сприйняття та зберігання у матеріалах справи.

Характеризуючи перший період становлення і розвитку інституту електронних доказів у кримінальному процесуальному праві (1970-2000–х р.р.), необхідно відмітити, що стрімкий розвиток електронно-обчислювальної техніки і телекомунікаційних технологій не лише змінив повсякденне життя, а й вплинув на правову сферу, зокрема, на інститут доказів та доказування у кримінальному процесі. Водночас не можна говорити про кардинальну зміну самого кримінального процесу: традиційні слідчі (розшукові) дії (обшук, огляд, виїмка) залишилися незмінними, як і сам характер багатьох злочинів (вбивства, грабежі, торгівля наркотиками тощо). Однак, науковці та правники почали звертати увагу на необхідність правового врегулювання питання доказового значення носіїв інформації, зафіксованої за допомогою обчислювальної техніки. Це стало першим кроком до усвідомлення важливості електронних доказів у кримінальному судочинстві.

Наприкінці 70-х та протягом 80-х років як документи, виготовлені на паперових носіях за допомогою електронно-обчислювальної техніки, так і документи на технічних носіях, були визнані науковцями новим видом документів, а подальше законодавче закріплення сприяло широкому впровадженню таких документів в документообіг і визнання їх доказової сили при розслідуванні злочинів.

У 1980-х роках з появою перших програм для створення текстів розпочався новий етап розвитку документування. Комп'ютеризація та автоматизація обробки інформації докорінно змінили функції та властивості документів, їх зовнішній вигляд та спосіб зберігання. Паперові документи поступово втрачали свою беззаперечну першість, адже документи почали існувати в цифровому форматі, що надавало нові можливості редагування, копіювання, зберігання та передавання. З цим пов'язане те, що документ почали ототожнювати з матеріальним носієм, оскільки інформація, закріплена на ньому, піддається однаковим процесам: запису (перетворенню), зберіганню (передачі), одержанню (збиранню, пошуку) та читанню. [244, с. 307].

В. В. Бірюков, В.В. Коваленко у практичному посібнику « Криміналістичне документознавство» зазначають, що в 1987 році український правознавець, вчений криміналіст М. Я. Сегай звернув увагу на появу нового виду судових експертиз, які досліджують не тільки паперові, але й кіно- та фотодокументи» [20, с. 14].

Саме в цей період М. В. Салтевський веде мову про появу «безпаперових» документів, які виготовлені комп'ютерами та визначив криміналістичне поняття документа та використання його як джерела доказів, ототожнюючи його з матеріальним носієм, на якому інформація зафіксована поза пам'яттю людини або ЕОМ [244, с. 308–309]. Серед науковців існує думка, що термін «електронні докази» в науковому середовищі з'явився в 2013–2016 роках. Однак, одним із перших визначень електронних доказів запропоновано науковцями І. Котляревським, Д. М. Киценко ще в 1998 році [109, с. 71].

У 1990 –х роках стрімко зросло використання комп'ютерів, Інтернету, що призвело до нового рівня кіберзлочинності. Фіксування у всьому світі кримінальних правопорушень, що вчинені з використанням комп'ютерних технологій стало предметом стурбованості міжнародних інституцій. Адже вчинення таких кримінальних правопорушень не обмежується кордонами певної держави і тому виникла необхідність узгодження питання міжнародного співробітництва, вироблення спільної політики спрямованої на захист суспільства від кіберзлочинності.

Даний період становлення та розвитку інституту електронних доказів відзначився такими подіями, зокрема у 1996 році відбулася одна із перших зустрічей на міжнародному рівні щодо розвитку інформаційного суспільства та забезпечення безпеки, конференція «Інформаційне співтовариство і розвиток», що відбулася в Мідранді (ПАР) 13–15 травня 1996 року [400].

У 1997 році була прийнята європейськими міністрами юстиції на 21-й Конференції Резолюція № 1[5] [до примітки див. 410].

10–11 жовтня 1997 року у Страсбурзі відбувався Другий Саміт глав держав та урядів, на якому вирішувалися важливі питання пов'язані з розвитком кіберзлочинності.

У 1998 році на 53 сесії Генеральної Асамблеї ООН прийнята Резолюція A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки»[6] [до примітки див. 395].

Резолюція Генеральної Асамблеї ООН A/RES/54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» від 01.12.1999 р.[7] [до примітки див. 396; 47, с. 284].

Ідеї та принципи резолюції були продовжені в 1999 році на наступній 54-й сесії ГА ООН в резолюції A/RES/54/50 «Роль науки і техніки в контексті міжнародної безпеки та роззброєння» [411].

Отже, підсумовуючи, вище зазначене констатуємо, що розвиток комп'ютерних технологій та Інтернету став ключовим фактором у формуванні підходів до використання інформації в електронному вигляді як доказів у кримінальному процесі. Саме в 1980-х роках почали з'являтися перші визначення поняття «електронного документа», що було зумовлено активним впровадженням електронно-обчислюваної техніки та автоматизованих систем обробки даних.

---

[5] Надані рекомендації підтримки роботи, що проводиться Європейським комітетом з проблем злочинності щодо кіберзлочинності для зближення внутрішньодержавних положень кримінального права і створення можливостей для застосування ефективних засобів для розслідування таких правопорушень.

[6] В резолюції 53/70 вперше на найвищому рівні наголошується, що нові технології та засоби потенційно можуть бути використані в цілях, несумісних з задачами забезпечення міжнародної стабільності та безпеки, та можуть негативно впливати на безпеку держав, піднімалося питання необхідності розроблення міжнародних принципів, спрямованих на укріплення глобальних інформаційних і телекомунікаційних систем та на боротьбу з інформаційним тероризмом і криміналом.

[7] вперше вказала на загрози міжнародній безпеці інформаційного простору стосовно не лише до цивільної, а також до військової сфери.

Другий період становлення та розвитку інституту електронних доказів (2001-2012 р.р.) характеризується науковим осмисленням природи електронних доказів, формуванням доктринальних підходів до їх класифікації, оцінки, безпосередньо пов'язаний з процесами конвергенції та інтеграції у правовий простір України норм міжнародного права з метою однакового нормативного врегулювання найбільш важливих питань міжнародного співробітництва – спочатку шляхом їх закріплення в міжнародних багатосторонніх угодах договірного характеру у вигляді норм міжнародного права, з наступним їх запозиченням національною правовою системою, зокрема, системами національного кримінального та кримінального процесуального законодавства.

23 листопада 2001 року Комітетом міністрів Ради Європи була прийнята Конвенція про кіберзлочинність, яку Україна ратифікувала 07 вересня 2005 р. (01 липня 2006 р. набрала чинності)[8] [до примітки див. 106].

КК УРСР 1960 року не містив спеціальних статей, що стосувалися злочинів у сфері використання електронно-обчислюваних машин. Однак, розвиток комп'ютерних технологій, поява випадків неправомірного втручання в ЕОМ викликав необхідність законодавчого регулювання такої категорії злочинів. Прийнятий в 2001 році КК України[9] [111]. В 2004 році прийнято ЗУ «Про внесення змін до Кримінального і Кримінально-процесуального кодексів України», в якому статті 361, 362, 363 КК України викладено в новій редакції і доповнено новими статтями (ст. 361-1, 361-2, 363-1) [221].

Одним з перших нормативно-правових актів в Україні, який був прийнятий з метою встановлення основних організаційно-правових засад електронного документообігу та використання електронних документів в Україні, був Закон України від 22.05.2003 р. «Про електронні документи та електронний

---

[8] В Преамбулі до Конвенції про кіберзлочинність наголошено на першочерговій необхідності спільної політики держав, спрямованої на захист суспільства від кіберзлочинності, зокрема, шляхом прийняття законодавства у сфері боротьби з кіберзлочинністю та застосування електронних доказів.

[9] вже містив розділ XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем комп'ютерних мереж», який включав три статті, таким чином визнавши статус комп'ютерної інформації як об'єкта права власності і відповідно об'єкта злочину .

документообіг» № 851-IV. Український законодавець визначив електронний документ як документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною [223].

Таким чином, можна визначити характерні риси для другого періоду: стрімка інформатизація суспільства, криміналізація кіберпростору, прийняття перших законодавчих актів щодо електронного документа, прийняття Конвенції про кіберзлочинність, яка в свою чергу також стимулювала запровадження поняття електронних доказів у правозастосування.

В цей період українські вчені-криміналісти, висвітлюючи різні аспекти комплексного криміналістичного дослідження документів, приділяли достатньо уваги дослідженню документів, виконаних за допомогою комп'ютерної технології та необхідності використання електронного документу в якості джерела доказу.

Електронний документ як джерело доказу.

Ще в 2004 році Г. Л. Чигрина у своїй дисертаційній роботі « обґрунтовує необхідність використання «електронного документу» як джерела доказу [358, с. 15].

У посібнику з криміналістики «Криміналістика у сучасному викладі», 2005 р. професор М. В. Салтевський обґрунтовував необхідність більш широко розуміти доказове документів, виконаних на сучасних ЕОМ та використовувати при кримінальних правопорушень [245, с. 209].

Салтевський М. В., Гаенко В. І., Литвинов О. М. почали розглядали електронний документ як матеріальне джерело доказів та відносили його як до письмових документів, так і до речових доказів [246, с. 85].

Використання вченими терміновжитку для позначення інформації в електронному вигляді.

М. В. Салтевський використовує поняття інформаційно-віртуальні сліди [243, с. 375]; Д. В. Бєзруков — «цифрові сліди» [15, с. 181]; В. О. Голубєв — інформаційні сліди [50, с. 108], і при цьому вчені акцентують увагу на відсутності матеріальної форми таких доказів.

Поява комп'ютера, призвела до появи нових документів – електронних, які мають як спільні риси з паперовими документами, так і специфічні риси, що в свою чергу вимагає конкретизації понятійного апарату [153, с. 166].

У посібнику науковці надали визначення поняттю «електронні докази» – це сукупність інформації, яка зберігається в електронному вигляді на всіх типах електронних носіїв і в електронних засобах та звернули увагу на особливість цих доказів, яка полягає в тому, що вони не можуть сприйматися безпосередньо, а мають бути інтерпретовані у певний спосіб і проаналізовані за допомогою спеціальних технічних засобів і програмного забезпечення [16, с. 451–452].

Також визначення комп'ютерних слідів пропонує і Пашнєв Д. В. в дисертації, розуміючи їх як зміни комп'ютерної інформації [148, с. 8, 13, 15].

О. В. Шведова у дисертації дає визначення електронного документа як джерела доказів – матеріальний носій юридично значущої інформації, зафіксованої у формі електронних даних, яка може бути створена, передана, збережена, оброблена, перетворена і представлена електронними засобами або на папері у формі, придатній для сприйняття, одержана з дотриманням процесуального порядку її збирання [360, с. 27–28].

С. М. Стахівський в монографічному дослідженні відзначає появу такої категорії як «електронні речові докази», під якими розуміє будь-які носії комп'ютерної інформації чи програмні об'єкти (комп'ютерні віруси, бази даних) та дає визначення електронного документу як комп'ютерної інформації в цілому, яка має доказове значення у кримінальному провадженні та одним із перших звертає увагу на невизначеність правового статусу ні самої мережі Інтернет, ні інформації яка в ній знаходиться. На його думку Інтернет може бути джерелом цінної доказової інформації [267, с. 226–227, 246–248].

Аналізуючи різні підходи вчених, практиків з приводу визначення поняття «документ» А. С. Білоусов в своїй праці «Криміналістичний аналіз об'єктів комп'ютерних злочинів», 2008 р. визначає поняття віртуального сліду як будь-якої зміни стану автоматизованої інформаційної системи, що викликана системою команд, пов'язана з подією злочину і зафіксована у вигляді комп'ютерної інформації на матеріальному носієві та акцентує увагу на тому, що зміст таких документів без застосування апаратних і програмних засобів не може бути сприйнятий людиною [18, с. 5,8,9].

В 2008 році В. Д. Басай, С. В. Томин також звернули увагу на появу «нетрадиційних слідів злочину», а саме віртуальних слідів та необхідність їх виділення в окрему групу [10, с. 221–222].

Крім того, необхідно відмітити наукові праці П. Д. Біленчука, А. В. Кофанова, О. Л. Кобилянського «Комп'ютерна злочинність у кредитно-фінансовій індустрії: криміналістичний аналіз», 2011 р., в якій вчені займалися вивченням нового криміналістичного об'єкту (документи на машинних магнітних носіях інформації) [17, с. 30]; та К. О. Щербаковської «Засоби мобільного зв'язку при розслідуванні торгівлі дітьми», 2011р. яка називає сліди «комп'ютерні», оскільки вони виникають під впливом комп'ютерних технологій і зберігаються на комп'ютерних засобах [368, с. 1109].

Характерні ознаки «електронних доказів»

Є. Ращенко виділяє специфічні ознаки інформаційних слідів: вони повинні вилучатися або з носієм інформації, або шляхом копіювання з використанням спеціальних програмних продуктів, із залученням спеціалістів та враховувати їх особливості на всіх етапах роботи з ними: збирання, закріплення та дослідження» [239, с. 76–78].

Така думка автора збігається з нашим баченням етапів роботи з електронними доказами та факторів, що впливають на їх автентичність та достовірність. Адже методи збирання, фіксації, збереження інформації в електронному вигляді, а також відповідність процедур їх отримання

процесуальним нормам визначають рівень їхньої доказової сили та можуть впливати на допустимість таких доказів у кримінальному провадженні.

Розглядаючи доказове значення «електронних документів» у кримінальному судочинстві М. Ф. Сокиран підкреслює, що ключовим елементом документа є інформація, яка міститься на носієві, при цьому електронний підпис є обов'язковим реквізитом такого документа [265, с. 141].

Про особливі правила роботи з електронними доказами, визнання даних доказів недопустимими наголошував В. О. Голубєв: «Щоб гарантувати їх признання в якості доказів, необхідно суворо дотримуватися кримінально-процесуального законодавства, а також стандартизованих прийомів і методик їх вилучення» [50, с. 151].

Викладені думки вчених-криміналістів багато в чому залишаються актуальними на сучасному етапі дослідження правових аспектів електронних доказів. Водночас як у досліджуваному періоді, так і сьогодні, науковці пропонують різні підходи до визначення таких понять як «цифрові сліди», «електронні докази», «віртуальні сліди», «електронний документ», «комп'ютерні сліди», «електронні речові докази», «інформаційні сліди».

В 90-х роках, із розвитком комп'ютерних технологій та їх запровадженням у різні сфери суспільного життя, виникла потреба у проведенні експертиз, пов'язаних з дослідженням комп'ютерних об'єктів, а також документів, виконаних за допомогою комп'ютерної техніки [13, с. 156; 55, с. 168], у зв'язку з цим науковці того періоду звернули увагу на специфіку «електронних доказів», намагаючись визначити їх характерні ознаки.

Тобто, ще на початку 2000-х років вчені вели мову про «електронні докази», «електронні речові докази» та визначали їх через категорію інформації. А також звернули увагу на досить нове джерело доказової інформації – Інтернет.

Науковцями також піднімалося актуальне і на даний час питання достовірності електронних доказів [16, с. 452].

М. Ф. Сокиран підкреслює актуальність питання достовірності даних, зафіксованих у цифровій формі та їх допустимості та перспективності подальших досліджень як з позиції теорії судових доказів, так і криміналістики, оскільки виявлення внесених змін на рівні аналізу цифрової інформації неможливо без застосування спеціальних методик та технологій [265, с. 142–143]. Така думка науковця набуває особливої актуальності в умовах швидкого розвитку цифрових технологій, масового поширення дипфейків, підробки інформації в електронному вигляді. Сьогодні технічні можливості дозволяють створювати цифрові фальсифікації, які майже неможливо відрізнити від оригіналу без застосування спеціальних методів аналіза.

В. О. Голубєв робить акцент на необхідності суворого дотримування кримінально-процесуального законодавства, а також стандартизованих прийомів і методик вилучення електронних доказів [50, с. 151].

Також в цей період активно обговорювалися питання щодо ролі спеціаліста та необхідності його обов’язкової участі при роботі з комп'ютерними доказами [18, с. 10; 150, с. 90–92].

Ще на початку 2000-х років фахівці з кримінального процесу досліджували питання «копії» та «оригіналу» електронних документів [13, с. 160; 18, с. 12], акцентували увагу на тому, що збирання, доступ, зберігання, поширення, використання інформації з застосуванням принципово нових технологій є втручанням у приватне життя людини, і одним із головних питань є визначення меж такого втручання [57, с. 13].

Саме в цей період правознавці спрямовували свої зусилля на обґрунтування необхідності більш детального вивчення електронної інформації та можливість використання як джерела доказу, що в свою чергу вплинуло на внесення змін до кримінально-процесуального законодавств та закріплення дефініції електронні носії інформації (ст. 63 КПК України 1960 р.) [215].

Так, у судових рішення вказаного періоду з’являються перші згадки про використання інформації в електронному вигляді як доказу та для позначення такої

інформації використовують терміни «виїмка електронних файлів документів, електронних файлів аудіо розмов» [208];«документи в електронному вигляді» [28; 211]; «електронний носій» [209; 210] «відео, -фотоматеріали» [212]; підробні електронні документи [37]; надавався дозвіл на проведення обшуку з метою відшукання магнітних та електронних засобів зберігання та передачі інформації [207]; дозвіл на проведення виїмки документів, які містять державну таємницю, а саме електронних файлів документів по контррозвідувальній справі, електронних файлів аудіо розмов, отриманих в результаті вказаних вище ОТЗ, електронних файлів із роздруківками текстів цих розмов [208], прикметно, що ця інформація витребовувалася з метою дослідження обставин втручання у приватне життя громадянина; цікава аргументація використана в судовому рішенні « в даному випадку слідчим в поданні ставиться питання про зняття інформації з каналів зв'язку в електронному вигляді, однак інформація у електронному вигляді не посвідчується, а тому не буде доказом по вказаній кримінальній справі» [155].

Це свідчить про поступове визнання судами значущості таких доказів та необхідності їх оцінки в межах кримінального процесу.

На підставі викладеного можна виділити особливості другого періоду:

– офіційне закріплення в законодавчих актах поняття «електронний документ» (Закони України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV, «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV);

– процеси конвергенції та інтеграції у правовий простір України норм міжнародного права (ратифікація Конвенції про кіберзлочинність);

– внесення змін до КК України (комп'ютерна інформація як об'єкт злочину);

– закріплення в КПК України поняття електронні носії інформації.

Ключовими характеристиками другого періоду є стрімке використання інформації в електронному вигляді як доказу та істотне відставання законодавства від потреб практики. В основному дослідженням «нетрадиційних доказів» займалися вчені-криміналісти, тоді як в сфері кримінального процесуального права

такі дослідження майже не проводилися. Науковці, які вивчали цей напрям, зосереджували свої зусилля на обґрунтування необхідності глибшого аналізу проблематики доказової інформації в електронному вигляді. Їхня діяльність була спрямована на формування нових доктринальних підходів, які б враховували специфіку інформації в електронному вигляді, її ідентифікації, збереження та оцінки як доказу.

Що стосується правозастосовної практики, то можна зазначити, що в цей період органи досудового розслідування та суди використовують інформацію з електронних носіїв (комп'ютерів, телефонів, мережевих логів) у розслідуванні злочинів як допоміжну інформацію, без усвідомлення їх як доказів. Відсутні чіткі критерії як така інформація повинна фіксуватися, зберігатися та оцінюватися.

Відправною датою відліку третього періоду (2012–сучасний період) нами визначено прийняття КПК України в 2012 році. В КПК України, який набув чинності 20.11.2012 р., з'явилося досить багато нових дефініцій[10] [до примітки див. 113].

Прийняття 03 вересня 2015 році ЗУ «Про електронну комерцію» № 675-VIII [226], внесення змін до ГПК, ЦПК, КАС України ЗУ «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 03 жовтня 2017 року № 2147-VIII [213], що стосувалися електронних доказів, в свою чергу було поштовхом до наукових досліджень у цих галузях. Внесення змін до ГПК, ЦПК, КАС України хоч і не стосується

[10] КПК України хоч і не вводить поняття електронних доказів, але містить дуже багато «цифрового» технічні засоби фіксації та носії інформації (п.1 ч.3 ст.104 КПК); виготовлені дублікати документів, а також копії інформації, у тому числі комп'ютерних даних, та спосіб їх ідентифікації; (п.3.ч.3.ст.104 КПК), оригінальні примірники технічних носіїв інформації (ч.3 ст.107 КПК); носії комп'ютерних даних (п.4 ч.2 ст.105 КПК); матеріальні носії передання інформації між особами (ч.4 ст.261 КПК); носії інформації, на яких зафіксовані відомості (ч.2,3 ст.266 КПК); носії інформації (у тому числі комп'ютерні дані) (п.1 ч.2 ст.99 КПК); оригіналом електронного документа є його відображення (ч.3 ст.99 КПК); копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах(ч.4 ст.99 КПК).

кримінального процесуального законодавства, однак є суттєвим прогресом для доказового права, адже вперше було проведено поділ джерел доказів на на письмові, речові та електронні, надано визначення електронного доказу.

Отже, з'явився новий вид доказів – електронні докази. До цього законодавство оперувало категорією «електронний документ», яка як уже зазначалося з'явилася у 2003 році з прийняттям Законів «Про електронні документи та електронний документообіг» № 851-IV, «Про електронний цифровий підпис» № 852-IV [223; 222].

В окресленому нами третьому періоді процесуалісти, використовуючи надбання наукової діяльності минулих років, міжнародний досвід в аналізованій сфері діяльності, продовжили пошук оптимальних підходів до використання електронної інформації у доказуванні у кримінальних провадженнях. Дискурс стосувався питання визначення статусу інформації в електронному вигляді як доказу, її гносеологічної і правової природи, а також встановлення критеріїв для виділення такої інформації в окреме процесуальне джерело .

Необхідно відмітити, що за кордоном дослідження щодо використання доказового значення інформації в електронному вигляді у кримінальному процесі почалися набагато раніше ніж в пострадянських країнах та Україні. Можна назвати таких зарубіжних вчених та їх роботи: К. Браун (Brown C. Computer Evidence: Collection and Preservation, 2009 p.) [371], Е. Кейсі (Casey E. Digital Evidence and Computer Crime, 2000p., Casey E. The value of forensic preparedness and digital-identification expertise in smart society, 2017 p.) [387, 388], Дж. У. Чизама (Chisum J. W. Crime Reconstruction and Evidence Dynamics, 2010p.) [389], С. Мейсон (S.Mason. International Electronic Evidence, 2008p.; Mason S. Electronic Signatures in Law, 2016 p.; Mason S. Report on the Use of Electronic Evidence in Civil and Administrative Law Proceedings and its Effect on the Rules of Evidence and Modes of Proof : A Comparative Study and Analysis, 2016 p.) [401, 406-408], Д. Сенг (Mason S., Seng D. Electronic Evidence, 2017p), Б. Шафтер, Д. Мішала, Д. Торренсе (B. Schafter The Admissibility of Electronic Evidence in Court: Fighting Against High-Tech Crime)

[416]. Напрацювання даних вчених містять багато цінної інформації для розуміння суті електронних доказів та практичної роботи з даним потенційним джерелом доказів.

До теми розуміння інформації, зафіксованої у електронній формі, яка виступає одним із видів доказів у кримінальному процесі у цей період зверталося багато вітчизняних учених. Серед найбільш помітних праць початку третього визначеного нами періоду слід відмітити наукові праці С. Й. Гонгало [51–54]. Автор обґрунтовує доцільність розмежування понять «електронний документ» та «інші інформаційні дані» («образи документів», «комп'ютерна інформація») та введення в обіг терміну «електронно-цифровий об'єкт [53, с. 14].

Січкаренко Г. Г. називає юридичні ознаки електронного документа: машинний носій інформації; комп'ютерна інформація; реквізити, що дозволяють ідентифікувати форму і зміст комп'ютерної інформації. Обов'язковий реквізит — електронний цифровий підпис [249, с. 60–61].

Єдиної думки серед процесуалістів щодо віднесення інформації в електронному вигляді до самостійного джерела доказів немає, водночас більшість дослідників визнають нетрадиційність цієї категорії доказів.

Вчені, досліджуючи правову природу електронних доказів, виокремлюють також такі ключові аспекти щодо використання інформації в електронному вигляді як доказу:

З точки зору законодавчого забезпечення:

визначення місця електронних доказів у системі доказів [268, с. 179]; необхідність запровадження окремої процесуальної категорії для інформації, зафіксованої та існуючої в цифровій (електронній) формі – електронні докази [65, с. 44]; виокремлення їх у самостійне джерело доказів у кримінальному провадженні [140]; визнання самостійним видом доказів у кримінальному процесі [98, с. 123]; вдосконалення інституту електронних доказів на законодавчому рівні [152, с. 247]; відсутність законодавчого закріплення поняття електронних доказів [142, с. 138]; необхідність розвитку міжнародного аспекту електронних доказів, удосконалення

законодавства щодо порядок отримання транснаціональних електронних доказів [417 с. 301]; законодавчого забезпечення можливості використання у кримінальному судочинстві електронного доказу не просто як наукової ідеї, а й як самостійного інституту доказування [273 с. 7];

З точки зору доктринальних підходів:

визначають, що інформація в електронному вигляді є нематеріальною; для її сприйняття і дослідження необхідне використання технічних засобів; зберігається на певному носії, оперативній пам'яті ЕОМ або каналу зв'язку; може копіюватися або переміщуватися на інший носій без втрати властивостей [353, с. 257]; необхідність теоретичної розробка концепції електронних доказів, з'ясування напрямів імплементації конвенційних вимог у законодавство України щодо боротьби з кіберзлочинністю [6, с. 123]; формування цілісного теоретичного бачення нормативного закріплення міжнародної взаємної правової допомоги для одержання електронних доказів та внесення пропозицій щодо закріплення такого механізму в спеціальному законі України [8, с. 193]; такі докази можуть бути створені як людиною так і бути результатом роботи інформаційної системи; потребують специфічного порядку збирання, перевірки та оцінки; не мають нерозривного зв'язку з матеріальним носієм [3, с. 251].

З точку зору проблеми правозастосування:

вдосконалення методики збирання та дослідження електронних доказів на досудовому провадженні та дослідження цих доказів у суді [133, с. 318; 249, с. 211]; дотримання чіткого виконання процедури їх збирання, вивчення, копіювання, дублювання, відтворення та збереження цілісності; необхідність використання криптографічного принципу хешування [124, с. 75]; забезпечення прав та законних інтересів особи при використанні інформації в електронному вигляді [66]; пов'язаність електронної інформації з приватністю (право на особисте життя та його таємницю, таємниця кореспонденції [252, с. 132]; відсутність чіткого процесуального порядку отримання електронних доказів, необхідність виокремлення специфічних підстав визнання їх недопустимими, недостатність

спеціальних знань у слідчих під час виявлення та фіксації електронних доказів [142, с. 138]; питання щодо оцінки електронних доказів, одержаних у межах міжнародної правової допомоги [8, с. 192]; відсутність базового обсягу знань у сфері інформаційних технологій; необхідність залучення спеціалістів та розробки повноцінної методики збирання, збереження та використання таких доказів [133, с. 314]; забезпечення цілісності збереження цифрової інформації за допомогою спеціального програмного забезпечення та за участі спеціаліста [353, с. 257]; відсутність у законодавчій та правотворчій діяльності правоохоронних та судових органів єдиного підходу до розуміння електронних доказів [80 с.32].

Різні аспекти використання електронних доказів у кримінальному процесі знайшли своє відображення також в дисертаціях вчених.

Так, в дослідженні «Речові докази у кримінальному провадженні», 2017 р. І. О. Крицькою вдосконалено доктринальне визначення поняття речового доказу, з'ясовано співвідношення речових доказів з цифровими джерелами доказової інформації [115].

Дисертація С. О. Ковальчука присвячена висвітленню теоретичних питань концепції речових доказів. Досліджуючи правову природу речових доказів, дослідник розглядає електронні докази як електронні документи, а їх матеріальні носії – як речові докази. При цьому, обґрунтовує необхідність визнання їх самостійним видом доказів у кримінальному процесі по аналогії з їх закріпленням в адміністративному, господарському і цивільному процесах з урахуванням їх існування в електронно-цифровій формі [98, с. 123].

У порядку огляду наукових джерел за предметом нашого дослідження слід також вказати на роботу А. В. Ратнової «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні», 2021 р. В своїй дисертації вчена приділяє увагу дослідженню кримінального процесуального та криміналістичного порядку використання електронних документів під час доказування у кримінальному провадженні. Вона акцентує

увагу на такій проблематиці як відсутність єдиного підходу до сутності та місця електронних документів у системі доказів під час здійснення слідчої та судової практики; виокремлює основні особливості електронних документів, якими на її думку, є наявність метаданих, електронна форма та необхідність візуалізації електронних документів за допомогою спеціального обладнання та програм; пропонує авторське визначення «електронного документа»; обґрунтовує необхідність віднесення електронних документів до самостійного джерела доказів у КПК України. Також значний обсяг матеріалу присвячений дослідженню електронних документів з точки зору їх допустимості та аналізу міжнародного досвіду використання електронних документів у процесі доказування. Вчена акцентує увагу на тому, що міжнародні організації працюють над введенням та запровадженням єдиних правил для збору, збереження та використання електронних документів, розроблення методик та поширення кращих практик під час роботи з електронними документами, незважаючи на відсутність визначення електронних документів у законодавстві багатьох країн Європи [238].

Науково близькою до теми нашого дослідження є й дисертація А. В. Скрипника “Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні”, 2021 р., яка представляє собою комплексне дослідження використання інформації з електронних носіїв та спрямована на вирішення найактуальніших практичних проблем. У своїй дисертаційній роботі вчений досліджує проблемні теоретичні та практичні аспекти використання інформації з електронних носіїв у кримінальному процесуальному доказуванні, визначає її характерні риси. Особливу увагу приділяє визначенню категорій «оригінал», «дублікат», «копія» щодо цифрової інформації, досліджує конституційно-правові аспекти використання цифрової інформації у кримінально-процесуальному доказуванні, наводячи аргументи, які мають значення не лише з теоретичної, але і практичної точки зору. Також науковець досліджує іноземний досвід використання цифрової інформації у кримінальному процесуальному доказуванні в англосаксонській та романо-германській правовій системі, що є

досить цінним для імплементацію досвіду інших країн в процесуальне законодавство України [250].

Дослідження зазначених науковців суттєво збагатили українську правову науку, розширивши уявлення про електронні докази та їхню роль у кримінальному процесуальному доказуванні. Вони не лише поглибили теоретичне осмислення цієї проблематики, а й сприяли розвитку практичних підходів до роботи з електронними доказами, піднісши рівень їх вивчення на якісно новий етап.

Широке використання в цей період інформації в електронному вигляді як доказу у правозастосовній практиці підтверджується аналізом рішень ВС в ЄДРСР: допустимості як доказів випадкових аудіо-відео [241]; копія відеозапису є оригіналом електронного документа [168]; відсутність оригіналу пристрою не створює недопустимість доказу [206]; аудіозаписи месенджерів не є НСРД зняття інформації з транспортних телекомунікаційних мереж [180]; копія відеозапису оригінал електронного документа [179]; допустимість відеозапису перенесеного з флеш накопичувача на оптичний диск [175]; допустимість огляду інтернет-сайтів [192]; твердження сторони захисту щодо можливого втручання та редагування аудіо-, відеозаписів, недостовірності відображеної на них інформації, отриманої в ході НСРД, мають спиратися на об’єктивні дані безсумнівного сприйняття таких фактів чи переконливо підтверджуватися іншими доказами або ґрунтуватися відповідними технічними висновками спеціалістів [191]; доступ до мобільного телефона не повинен здійснюватися через ухвалу НСРД [190]; огляд інформації у телефоні не становить НСРД та не передбачає необхідності здійснення тимчасового доступу до речей і документів. Для копіювання не потрібні спеціальні знання. Для ідентифікації осіб та їх голосу за матеріалами відео-та аудіозаписів залучення експерта не є обов’язковим [197]; безперервність відеозапису-гарантія достовірності та належності доказу [196]; щодо належності як доказів роздруківок з мережі Інтернету [156]; огляд телефону без дозволу слідчого судді (фотографії, текстові повідомлення) [195] добровільно виданий телефон не потребує легалізації отримання інформації в електронному вигляді, що на ньому міститься в порядку

тимчасового доступу [199]; дослідження судом протоколу огляду інтернет сторінок, скріншотів сторінок та завантажених відеофайлів [198]; відсутність потреби засвідчення електронних доказів електронним підписом; метадані не є достовірним джерелом інформації про історію маніпуляцій з файлом, оскільки такі можуть змінюватися незалежно від його вмісту [200]; про допустимість протоколу огляду мобільного телефона та ноутбука через відсутність ухвали суду про тимчасовий доступ (НСРД та добровільна видача) [204]; визначення поняття електронні докази [205]; оцінка достовірності копії відеофайлу [203].

Підсумовуючи, зазначимо, що характерними ознаками останнього періоду є:

– саме з цього періоду починається бурхлива розробка і розвиток уявлень про електронні докази у працях вчених;

– оформлення докринальної моделі наукового бачення регламентації процедури збирання, фіксування, оцінки електронних доказів;

- унормування на законодавчому рівні, в тому числі в кодифікованих актах окремих положень щодо використання інформації в електронному вигляді як доказу;

– використання електронних доказів у кримінальних провадженнях через практику правоохоронних органів та суду, вироблення підходів до оцінки їх допустимості та достовірності.

Цей період характеризується інтеграцією та вдосконалення, зокрема, шляхом гармонізації національного правового регулювання, імплементацією міжнародних норм, а також упровадження новітніх технологій перевірки достовірності доказів. Особливе значення матиме використання штучного інтелекту, що уможливлює збір та обробку великих обсягів електронних даних із різних джерел, сприяє подоланню проблем deepfake маніпуляцій, а також забезпечує ефективну підтримку судових процесів.

Отже, у процесі дослідження ми прийшли до висновку, що на сьогодні можна стверджувати про становлення інституту електронних доказів у кримінальному процесуальному праві. Його повноцінне формування потребує вдосконалення

законодавства, внесення змін в КПК України із закріпленням поняття «електронні докази», визначення процесуального механізму отримання, фіксації, перевірки та оцінки таких доказів.

1.2. Поняття електронних доказів у кримінальному процесі

Без точного і ясного визначення понять неможливо в процесі пізнання успішно рухатися вперед [90, с. 30].

До визначення сутності електронних доказів існує різноманіття наукових підходів, які відображають специфічні ознаки електронного доказу та підкреслюють його особливу правову природу. Специфічні ознаки електронних доказів детально досліджувалися вченими-процесуалістами та криміналістами, проте, у доктрині кримінального процесу та практиці кримінального процесуального доказування це питання є і на даний час досить важливим як у термінологічному, так і гносеологічному значені.

Визначити, що ми маємо на увазі під поняттям «електронні докази», а також обґрунтувати необхідності вживання саме такого терміну для позначення інформації з електронних носіїв, непросте завдання. Вид доказів, з якими ми маємо справу, науковцями визначається через наступні терміни: «цифровий доказ», «комп'ютерний доказ», «віртуальний доказ», «комп'ютера інформація», «інформація з електронних носіїв», «електронна інформація» і т. п. Усі ці терміни, а також визначення, які дають їм науковці, на нашу думку, відображають певні аспекти того, що цей вид доказів має відмінні риси, які дозволяють виділити його серед інших джерел доказів. На основі вивчення та дослідження різних точок зору науковців, запропонуємо власне бачення окремих аспектів дослідження.

В українському науковому середовищі на окреслену тематику наявні доробки різного рівня та глибини дослідження. Але навіть поверхневий аналіз запропонованих науковцями визначень «нетрадиційних доказів» демонструє широкий діапазон та відсутності єдності в наукових колах.

Переходячи до дослідження наукових праць, ми не ставимо на меті викладення їх за хронологічним критерієм. Наведені праці відрізняються високим рівнем науковості, висвітлюють різні аспекти і є найбільш яскравим підтвердженням термінологічної невизначеність (цифрові докази, електронні докази, цифрова інформація, електронне відображення). Крім того, вважаємо за необхідне звернутися до теоретичних досліджень використання електронної інформації, які проводилися науковцями інших галузей юридичної науки, зокрема цивільного, адміністративного, господарського процесу. Результати таких досліджень можуть бути використані для вирішення спільних з кримінальним процесуальним правом питань.

Електронний документ.

Як ми вже вказували, одним із перших науковців хто звернув увагу на необхідність трансформації доказів, який тривалий час існували в кримінальному процесі та появу нового виду документів—електронного був відомий науковець криміналіст В. К. Лисиченко [121, с. 11–12; 122, с. 49].

В наукових працях 2000-х років електронний документ визначали через категорію інформації, яка записана за допомогою цифрових методів фіксації на відповідний носій. Вчений криміналіст М. Ф. Сокиран вважав електронний підпис обов’язковим реквізитом електронного документа [265, с. 141].

Необхідно звернути увагу на досить цікаве визначення електронного документа як джерела доказу О. В. Шведової. На її думку, електронний документ – це матеріальний носій юридично значущої інформації, зафіксованої у формі електронних даних, яка повинна бути представлена у формі, придатній для сприйняття, одержана з дотриманням процесуального порядку її збирання [360, с. 27–28].

Про необхідність конкретизації понятійного апарату в зв’язку з появою нових документів – електронних наголошують і інші науковці [153, с. 166], а також підкреслювали необхідність введення в обіг терміну «електронно-цифровий об’єкт», яким позначати всі інші об’єкти, що не відповідають вимогам

«електронного документа», але існують поряд з ним у віртуальному (електронному) середовищі [53, с. 14].

Віртуальні сліди, цифрові сліди, інформаційні сліди.

В. Д. Басай, С. В. Томин розглядали віртуальні сліди як результат впливу (знищення, модифікації, копіювання, блокування) на комп'ютерну інформацію, у будь-яких змінах комп'ютерної інформації, пов'язаних з подією злочину. Поряд з цим ще в 2008 році висловлювали точку зору щодо необхідності виділення віртуальних слідів в окрему групу та виділяли такі особливості даних доказів: вони існують на матеріальному носії, але не доступні безпосередньому сприйняттю; для їх вилучення необхідне обов'язкове використання програмно-технічних засобів; вони не мають чіткої прив'язки до приладу, що здійснив запис інформації, тому є досить нестійкими, оскільки можуть бути легко знищені. Отримувані сліди завдяки своїй природі є внутрішньо ненадійні природі, оскільки їх можна неправильно зчитати [10, с. 221–222].

До такої думки приєднується А. С. Білоусов, який визначає поняття віртуального сліду як будь-якої зміни стану автоматизованої інформаційної системи, що викликана системою команд, пов’язана з подією злочину і зафіксована у вигляді комп’ютерної інформації на матеріальному носієві та виділяє аналогічно особливості таких доказів [18, с. 5, 9]. Автор, надаючи майже аналогічне визначення, називає такі докази «комп’ютерними слідами» [148, с 8, 13, 15]. К. О. Щербаковська також веде мову про «комп’ютерні сліди» [368, с. 1109]. В науковій літературі можна зустріти і інші терміни, такі як «інформаційно-віртуальні сліди» [243, с. 375]; «цифрові сліди» [15, с. 181]. Варто зазначити, що у кримінально-правовій науці українські учені «нетрадиційним слідам» дають також назву інформаційні сліди [50, с. 108; 239, с. 76].

До речі, в наукових працях 2000-х років можна зустріти такі визначення «нетрадиційних доказів» як матеріальні сліди електронного характеру [131, с. 10]; «безпаперовий документ» – матеріальний носій, на якому інформація зафіксована поза пам'яттю людини або ЕОМ [244, с. 308–309];

Зокрема, вітчизняні учені Ю. Ю. Орлов та С. С. Чернявський пропонують визначають електронні відображення як форму зберігання відомостей за допомогою знакових систем [140; 358].

Електронні докази.

Інший учений процесуаліст С. М. Стахівський відзначає появу такої категорії як «електронні речові докази», під якими розуміє будь-які носії комп'ютерної інформації чи програмні об'єкти (комп'ютерні віруси, бази даних), а також пропонує визначення електронного документу як комп'ютерної інформації [267, с. 246–248].

Сам термін «електронні докази» одними із перших запропонували науковці такі науковця як: О. І. Котляревський, Д. М. Киценко., які визначали такі докази через категорію інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах [109]. Аналогічне визначення дає В. В. Мурадов, який зазначає, що електронні докази – це сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв [133, с. 317].

Колектив авторів Національної академії прокуратури України зазначає, що поняття «електронні докази» – це інформація, що зберігається в електронному вигляді на будь-яких типах електронних носіїв, в електронних пристроях чи електронних інформаційних системах та відповідає вимогам ст. 84 КПК [68, с. 112].

Як ми бачимо теоретики кримінального процесуального права визначають поняття електронних доказів через категорію інформації. Так, Н. М. Ахтирська вказує, що електронні докази – це дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій [6, с. 125], таким чином фактично ототожнює електронні докази та дані, використовуючи тлумачення цього терміну, яке застосовано в Конвенції про кіберзлочинність.

На думку Д. Алєксєєвої-Процюк та О. Бриськовської «електронні докази» є «фактичними даними, що зберігаються в електронному вигляді на будь-яких типах

електронних носіїв та в електронних засобах та які після обробки спеціальними технічними засобами та програмним забезпеченням стають доступними для сприйняття людиною» [3, с. 250].

Підтримує їх позицію і О. В. Сіренко, який вважає, що електронні докази – це дані про обставини, що мають значення для кримінального провадження і існують у нематеріальному вигляді в межах технічного носія чи каналу зв'язку та сприйняття та дослідження яких можливо за допомогою технічних засобів та програмного забезпечення [248, с. 211].

Аналізуючи вищенаведене, ми робимо висновок, що в ньому дослідниками робиться акцент на нематеріальну природу даних в електронному вигляді та можливість їх сприйняття та дослідження за допомогою технічних засобів та відповідного програмного забезпечення.

І. Вернидубов та С. Белікова електронними доказами визначають інформацію в електронному вигляді про факти і обставини, що мають значення для справи та зафіксована за допомогою передбачених законодавством електронних носіїв або така, що передається по каналах електрозв’язку. [27, с. 304].

На думку науковців С. О. Ковальчука, С. І. Хом’яченка, Т. О. Часової зміст електронних доказів складають фактичні дані, на підставі яких можуть бути встановлені факти й обставини, що мають значення для кримінального провадження і підлягають доказуванню, та які існують в електронно-цифровій формі [98, с. 121–122; 351, с. 178].

Також звернемо увагу на підхід, запропонований О. Г. Козицькою, яка визначає електронний доказ як цифровий об’єкт, який був засобом чи знаряддям вчинення кримінального правопорушення; зберіг електронно-цифрові сліди кримінального правопорушення, був предметом або об’єктом вчинення кримінального правопорушення або містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [102, с. 420].

На нашу думку, такий підхід запропонований авторкою, не в повній мірі розкриває правову природу електронних доказів, адже фактично електронні докази ототожнюються тільки з речовими доказами.

Отже, ми бачимо, що у переважній більшості науковці розглядають терміновжиток «електронні докази», і дефініція, як правило, пов'язана з категорією «інформація».

У звичному розумінні електронна (цифрова) інформація не є матеріальною. Вона стає придатною для сприйняття лише за допомогою спеціальних технічних пристроїв – певних матеріальних об'єктів, хоча може зберігатися та перетворюватися незалежно від таких матеріальних об'єктів. Наприклад, матеріальний носій електронної (цифрової) інформації CD-диск через неналежне зберігання може піддатися дії магнітної сили, і тоді вся інформація, яка містилися на ньому, зникне, тобто попри наявність матеріального об'єкта фактичних даних не буде [65, с. 41]. Аналогічний приклад можна привести якщо матеріальний носій інформації буде відформатований.

Специфічна природа інформації в електронному вигляді полягає в тому, що вона є доступною для сприйняття людиною не безпосередньо, а тільки після обробки її спеціальними програмними засобами [64, с. 118].

Досить цікаве дослідження провів А. В. Скрипник, порівнюючи терміни «інформація», «відомості», «дані». З урахуванням досліджених етимологічних, семантичних і філософських аспектів у контексті цифрових технологій, він робить висновки, з якими важко не погодитися: 1) людина не може сприймати дані; 2) те, що вона може сприймати, є інформацією; 3) сприйнята інформація стає відомостями [250, с. 70].

Нами наведені приклади поглядів учених на доцільність використання терміну «електронний» для позначення інформації в електронному вигляді. Разом з тим, у науковому дискурсі простежуються і інші підходи— зокрема, деякі дослідники оперують терміном «цифрові докази».

Так, А. В. Скрипник вважає термін «цифровий» найбільш доречним для позначення такої інформації, оскільки це підкреслює дискретність даних, оброблюваних ЕОМ чи іншими засобами [250, с. 73]; «цифровий доказ» є більш точним і «краще відображає кібернетичний аспект передачі, обробки та збереження інформації з огляду на процеси перетворення інформації за допомогою бінарного (двійкового) коду» [79].

Д. М. Цехан також використовує термін «цифрові докази» («digital evidence») та визначає їх як фактичні дані, представлені у цифровій формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ [353, с. 259]. Термін «цифровий» підтримують також і інші вчені.

На думку І. О. Крицької більш доцільно використовувати категорії «цифрові джерела доказової інформації» [114, с. 302; 115, с. 38].

Г. Авдєєва, Е. Живуцька-Козловська під поняттям «цифрові докази» розуміють фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об’єктивного вирішення справи [1, с. 131, 141].

А. В. Скрипник пропонує два визначення цифрових доказів: теоретичне і нормативне. На його думку, цифровий доказ – це: а) цифрова інформація, отримана шляхом відтворення з використанням технічних засобів змісту файлу, який знаходиться на носії цифрових даних; б) цифрова інформація, отримана у передбаченому КПК порядку, на підставі якої дізнавач, слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [250, с. 92].

Однак, в юридичній літературі попри прагнення науковців розробити визначення розглядуваному поняттю, існує підхід, відповідно до якого «для розуміння концептуальної суті досліджуваного поняття не має суттєвого ідеологічного та технологічного значення, як будуть називатися докази – комп’ютерними, електронними, цифровими, інформаційно-технологічними» [102, с. 418].

Поділяємо думку Д. О. Алексєєвої-Процюк та О. М. Брисковської, що не можна ототожнювати поняття «цифрові докази», «комп'ютерні об'єкти», «кібердокази», «електронні документи», «електронне відображення», «цифрові джерела доказової інформації», «електронні докази». [3, с. 250].

Г. Авдєєва, Е. Живуцька-Козловська звертають увагу також на те, що науковці в галузі кримінально-правових наук одночасно використовують терміни «електронні» та «цифрові» докази, хоча ці терміни не є тотожними [1, с. 131]. Протилежної точки зору дотримуються вчені М. В. Гуцалюк, П. Є. Антонюк, вони стверджують про синонімічність (під кутом зору використання) таких понять, як «електронна інформація» і «цифрова інформація» у вітчизняному правовому полі [65, с. 37]. Про тотожності понять «цифрова інформація» та «електронна інформація» веде мову також Д. О. Літкевич, при цьому більш правильним він вважає термін «цифрова інформація» [123, с. 65].

Варто зазначити, що виділення будь-якого явища можливо лише через визначення його характерних ознак, які надають йому відмінного змісту, відмежовуючи від інших феноменів. При побудові будь-якого поняття необхідно враховувати закони логіки, відповідно до якого зміст кожного поняття становить сукупність існуючих ознак, які відтворюють якість предмета і відрізняють його від інших предметів [76, с. 43].

Тотожні поняття – це різні знакові вирази, які мають різний смисл, але однаковий денотат. Тотожні поняття не треба плутати з абсолютними синонімами (тобто, знаками, що мають однаковий смисл і однаковий денотат) [107, с. 150].

Звертаючись до тлумачних словників, ми можемо уточнити значення цих термінів, однак як цілком зрозуміло, що один і той самий термін у різних науках може вживатися у різному значенні.

Так, тлумачний словник з інформатики визначає електронний (electronic) (див. цифровий)[11] [до примітки див. 279, с. 326, 587]. Ми навмисно не даємо

[11] як слово, що розкриває зміст інновацій, реалізованих із застосуванням цифрових, інформаційних, мережних, веб- та інтернет-технологій. По відношенню до апаратних компонентів ПК характеризує їхню електронну сутність і

визначення терміну цифровий, який мається в цьому словнику, оскільки на нашу думку не потрібно при дослідження термінології та сутності понять «цифровий», «електронний» настільки глибоко вникати в специфічну термінологію технічних наук, однак необхідно розуміти сутність даних понять.

Висловлюючи власну думку стосовно цього питання, зазначимо таке – безумовно, «цифровий» і «електронний» не є однозначно тотожними поняттями, хоча часто науковцями та правозастосовниками вживаються як синоніми, але як з юридичної, так і технічної точки зору між ними є відмінності. Поряд з цим, цифрова інформація — це інформація представлена у вигляді цифрового коду, вона може передаватися за допомогою електронних, оптичних або інших цифрових технологій; електронна інформація — це інформація, що існує в електронні формі незалежно від способу її зберігання. Вона може включати аудіо- та відеофайли, текстові документи, бази даних, тощо.

Тому в нашому дослідженні ми схиляємося до використання поняття «інформація в електронному вигляді», оскільки таке формулювання підкреслює, що інформація має електронну форму незалежно від її аналогового чи цифрового походження. Отже, коли мова йде про математично закодовану інформацію, то доречно використовувати поняття «цифрова інформація», а якщо мова йде про юридичне визначення, то все таки, на нашу думку, більш логічно використовувати поняття «інформація в електронному вигляді».

Водночас, навряд чи можна заперечувати те, що науковці, використовуючи термінологію «електронний», «цифровий» для позначення інформації ведуть мову про один і той же об’єкт і в даному випадку суттєвим і важливим є тільки те, до якого спільного знаменника прийде наукова думка. І повністю погоджуємося з думкою А. В. Скрипника, «що для того, щоб усунути термінологічне багатоманіття, потрібно зрозуміти сутнісні особливості досліджуваного явища, а вже потім визначити найбільш відповідний термін для позначення поняття» [250, с. 68].

відношення. У мережах передачі даних і мережних технологіях прикметник «електронний» є синонімом терміну «цифровий»; цифровий [син. – електронний] (digital)».

Варто також зазначити, що Конвенція про кіберзлочинність хоч і не дає визначення поняття «електронні докази», в преамбулі якої зазначено одну із цілей – надання можливості *збирання доказів*, що стосуються кримінального злочину, *в електронній формі* (курсив наш - І. Смаль) [106]. Доцільно також звернути увагу на подію, яка сталася 17 листопада 2021 року – це ухвалення Комітетом міністрів Ради Європи Другого додаткового протоколу до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів [411]. Термінологія, яка використовується в даному протоколі, в свою чергу, свідчить про поширення в країнах Європи терміну «електронні докази», «докази в електронній формі».

Аргументація на користь більш доцільного вживання терміну «електронні докази» підсилюється результатами опитування (Додаток Б). Заради справедливості доцільно зауважити, що і у практиків не має одностайності стосовно цього питання. Однак, на питання щодо найбільш коректного вживання терміну для позначення інформації з комп'ютерів, смартфонів та інших технічних приладів переважаюча думка все таки «електронний», а не «цифровий».

Незважаючи на те, що з 2017 році ЦПК, КАС, ГПК містить поняття «електронні докази», застосування такого джерела доказів залишається таким же дискусійними як і в кримінальному процесі. У вітчизняній науці щодо цього питання донедавна були відсутні комплексні наукові дослідження.

Необхідно відмітити дисертацію Д. О. Московчука «Електронні докази у країнах континентального та загального права: порівняльно-правове дослідження» (2023). Наукова праця хоч і стосується дослідження електронних доказів у цивільному процесуальному праві України, однак питання підняті науковцем можуть мати значення для подальшого вдосконалення кримінального процесуального законодавства. Так, науковцем дано визначення електронних доказів, побудовано дворівневу модель системи електронних доказів залежно від особливостей джерел їх отримання та способу використання в процесі судового доказування. Обґрунтовано доцільність запозичення наявної в судах країн загального права практики подання до суду разом з паперовою копією

електронного документа також метаданих. Науковець наголошує на необхідності більш чіткої регламентації в нормах законодавства значення електронного підпису для юридичної сили електронного доказу [130].

В дослідженні Ю. С. Павлова визначає поняття електронного доказу та його місце в системі традиційних засобів доказування; досліджує сутність електронного документа. Дослідниця висловлює думку щодо відсутності термінологічної різниці між використанням назви «електронний» або «цифровий доказ», оскільки вони відображають одну й ту саму сутність доказової інформації та є тотожними поняттями [145, с. 69]; визначає електронні докази через категорію інформації, яка представлена в електронній формі, що має значення для розгляду справи, дослідження якої здійснюється за допомогою спеціальних програмно-технічних засобів [146, с. 108] та наголошує на необхідності дослідження правової природи електронних доказів саме через їх ознаки, які відображають специфіку електронних доказів [144, с. 14].

Електронні засоби доказування як самостійний вид виділяє М. Гетьманцев на підставі особливостей носія такої інформації. Тобто електронним за своєю сутністю є саме джерело (носій) інформації, що має доказове значення, а сама інформація залишається у формі письмових знаків, усного мовлення тощо [48, с. 19].

На думку С. А. Чванкіна термін «електронні докази» включають всі форми доказів, які створюються, змінюються або зберігаються на різних формах пристроїв, за допомогою яких дані можуть зберігатися або передаватися, включаючи аналогові пристрої [356, с. 247].

В дослідженні «Докази і доказування у адміністративно-деліктному процесі» (2015) І. В. Казанчук дає визначення електронного документу як самостійного джерела доказів, інформація в якому представлена у формі електронних даних, включаючи відповідні реквізити документа, в тому числі і електронний цифровий підпис та інші, який може бути сформований, переданий, збережений і перетворений електронними засобами у візуальну форму,

автентичність якого може бути підтверджена електронним цифровим підписом та іншими незмінними сертифікованими засобами [82, с. 6, 17].

Дисертація А. Ю. Каламайка «Електронні засоби доказування в цивільному процесі» (2016) є однією із перших в науці цивільного процесуального права України науковою працею, що присвячена дослідженню електронних засобів доказування, в якій визначено поняття, види електронних засобів доказування та виявлені особливості їх використання при вирішенні цивільних справ [83; 84].

Ведучи мову про доволі широку палітру напрямів наукового осмислення проблематики електронних доказів як у кримінальному процесі, так і в інших галузях права та юридичних науках і все ж доводиться констатувати відсутність єдності у розумінні окремих базових питань даної тематики, зокрема стосовно формулювання визначення «електронні докази». Проблема уніфікації та застосування єдиних підходів до тлумачення понять надзвичайно важлива й актуальна.

Водночас як практикуючому правнику не можна ігнорувати чинні наразі процесуальні норми – положення КПК України. Під час правового осмислення даної проблематики, пропонуючи внесення змін до кримінального процесуального законодавства, варто враховувати специфіку закріпленої у законі системи процесуальних джерел доказів - носіїв інформації.

Тому, на даному етапі дослідження звернемося до законодавчого регулювання даного виду доказів.

Так, в ст. 100 ЦПК України, ст. 99 КАС України та ст. 96 ГПК України визначено[12] [до примітки див. 59; 99; 355]. Отже, ми бачимо, що законодавець визначає електронні докази через категорію інформації.

---

[12] що електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет).

Одним із основних законів, що регулюють суспільні відносини у досліджуваній нами сфері, є Закон України «Про інформацію». Так, відповідно до ст. 1 цього закону інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [230]. ЦК України інформацію відносить до нематеріальних благ і застосовує аналогічну дефініцію для її визначення (ст. 200 ЦК України) [354].

Звідси випливає, що інформація – це: а) відомості; б) відомості та дані; в) дані.

Виходячи з наведеної дефініції можна стверджувати, що дані та відомості є складовою частиною інформації і співвідносяться між собою як частина та ціле.

В ст. 1 ЗУ «Про захист інформації в автоматизованих системах» від 5 липня 1994 р. (були внесені зміни в дану статтю Законом України від 31 травня 2005 р. № 2594-IV) було дано визначення інформації в автоматизованій системі як сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення; на даний час Закон України «Про захист інформації в інформаційно-комунікаційних системах» не містить визначення поняття інформація, а відсилає до Закону України «Про інформацію» [229].

Що стосується поняття електронних доказів у кримінальному процесуальному праві України, то чинний КПК не оперує поняттям «електронний доказ». Однак, деякі норми, опосередковано торкаються окремих аспектів функціонування електронних доказів у кримінальному процесі. Окремо зупинимося на одних із останніх змін до КПК щодо «електронних доказів». Так, 15.03.2022 Верховною Радою України було прийнято Закон № 2137-IX, спрямований на підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам та внесені зміни в ряд статей КПК України [216].

Ми бачимо, що законодавець вніс зміни в ст. 99 КПК України, у пункті 1 частини другої слова «(у тому числі електронні)» замінено словами «(у тому числі комп’ютерні дані)». Хочемо звернути увагу, що поняття електронні носії

інформації існувало в КПК 1960 р. (ст. 63 КПК) [215] і відповідно було перенесено в КПК 2012 р. (ст. 99 КПК) [113].

Однак, ні КПК 1960 року, ні КПК 2012 року не розкривав зміст даного терміновжитку. Надалі ми бачимо, що законодавець вводить нове поняття «комп'ютерні дані» та відносить їх до такого процесуального джерела доказів як документи. Оскільки, в ст. 3 КПК України визначення терміну «комп'ютерні дані» також відсутнє, то за загальним правилом, передбаченим ч. 3 ст. 3 КПК України необхідно звернутися до інших законів України для роз'яснення його змісту.

Можемо знайти визначення в Законі Україні «Про електронні комунікації» поняття «дані» – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки, технічними та програмними засобами [224], в Законі України «Про електронну ідентифікацію та електронні довірчі послуги» є визначення дефініції «електронні дані» – будь-яка інформація в електронній формі [225].

Логіку законодавця можна прослідкувати за Пояснювальною запискою до проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за «гарячими слідами» та протидії кібератакам»[13] [до примітки див. 220].

Звернемося також до змісту Конвенції про кіберзлочинність Ради Європи[14], [до примітки див. 106].

---

[13] мета даного законопроєкту – підвищення ефективності кримінальних розслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються злочину, в електронній формі. Також із зазначеною метою вводяться терміни «комп'ютерні дані» і «комп'ютерна система» (п. 1 ч. 2 і ч. 4 ст. 99, п. 3 ч. 3 ст. 104, п. 4 ч. 2 ст. 105, абз. 2 ч. 1 ст. 159 та ін.), якими оперує Конвенція про кіберзлочинність.

[14]в ст. 1 якої є визначення яке застосовується для цілей цієї Конвенції «комп'ютерна система» означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку ***даних***; ***«комп'ютерні дані»*** означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою.

Отже, якщо порівнювати поняття «інформація», визначення якому дає ЗУ «Про інформацію», ЦК України, то поняття інформація є більш ширше ніж дані. Визначення поняття «дані», яке зазначено в Конвенції про кіберзлочинність, в ЗУ України «Про електронні комунікації», включає в себе інформацію.

Повернемося ще раз до визначення «комп'ютерні дані», яке дає Конвенція: «представлення фактів, інформації або концепцій *у формі, яка є придатною для обробки у комп'ютерній системі»* (курсив наш - І. Смаль). Тобто, дане визначення говорить саме за себе: апріорі ця інформація не може бути сприйнята людиною.

Вводячи нове поняття в процесуальний кодекс, потрібно було надати йому визначення і тоді в практикуючих юристів не виникали б питання, що все таки мав на увазі законодавець. Тим більше, такі питання виникають ще і тому, що ст. 99 КПК вживання конструкції інші носії інформації (у тому числі комп'ютерні дані) є не досить логічне. А ч.4 ст. 99 КПК вказує на те, що комп'ютерні дані є фактично частиною інформації, що також викликає логічно запитання до законодавчої конструкції цієї норми.

Як бачимо з тлумачного словника з інформатики до комп'ютерів (computer) відносять наступне:[15] [до примітки див. 279, с. 380].

В тлумачному словнику основних понять і термінів програмування є наступне визначення: дані (data)-1. значення, записані в оперативній пам'яті або іншому пристрої комп'ютера; 2. інформація, підготовлена для передачі, зберігання й обробки в обчислювальній машині, тобто представлена в символьній (цифровій) формі [361, с. 10].

Дані (data)—[16] [до примітки див. 279, с. 307–308]. Отже, з урахуванням природи інформації в електронній формі, а також самого поняття «дані»,

---

[15] успадкована система, суперкомп'ютер, кластер, мейнфрейм, сервер, робоча станція, персональний комп'ютер, персональний суперкомп'ютер, комп'ютер-моноблок, мультимедійний комп'ютер, десктоп, лептоп, портативний комп'ютер, ноутбук, мініноутбук, субноутбук, нетбук, ультрамобільний персональний комп'ютер, смартбук, мобільний інтернет-пристрій, палмтоп, комп'ютер у вигляді записника, кишеньковий ПК, хендхелд, надолонний комп'ютер, персональний цифровий секретар, підприємницький цифровий секретар, планшетний комп'ютер, мобільний пристрій, комунікатор, смартфон, мобільний телефон, стільниковий телефон, камерофон).

[16] зареєстровані сигнали або факти; форма існування й подання інформації; інформація, підготовлена для певної мети(формат) або представлена у вигляді, придатному для обробки автоматичними засобами при можливій участі

«комп’ютерні дані» – представлення фактів, інформації у формі придатній для обробки у комп’ютерній системі (так як його інтерпретує Конвенція про кіберзлочинність), сприйняття комп’ютерних даних безпосередньо слідчим, прокурором, судом фізично неможливо.

Досить зрозуміле і однозначне тлумачення поняття «дані» можна зустріти в зарубіжних науковців. Дані — це «будь-яка інформація, що зберігається на комп'ютері»; файл — це «набір даних або інформації, що зберігається під певним ім'ям на диску» [409, с. 150]. Якщо все таки вважати, що комп’ютерні дані — це відповідно інформація в електронному вигляді, яка придатна для сприйняття людиною після обробки автоматичними програмними засобами, то все стає на свої місця.

Однак, на нашу думку, більш логічним терміновжитком для позначення інформації в електронному вигляді є «електронні дані», відповідне визначення якому, як ми зазначали вище, є у профільному Законі «Про електронну ідентифікацію та електронні довірчі послуги» [225].

Для кращого розуміння термінів, що стосуються доказів які мають електронну форму (електронних доказів) і використовуються у КПК України та судових рішеннях, необхідно пояснити також співвідношення цих термінів між собою. Електронні носії інформації (носії інформації в електронному вигляді), а відповідно до термінології КПК носії інформації (п. 3 ч. 2 ст. 99 КПК) містять в собі електронні дані (в термінології КПК комп’ютерні дані (п. 1 ч. 2 ст. 99 КПК)) та електронні документи (підписані кваліфікованим електронним підписом ст. 5 ЗУ «Про електронні документи та електронний документообіг»).

Це свідчить про те, що ця норма законодавства демонструє певну нечіткість у співвідношенні понять електронні документи, комп’ютерні дані, носії інформації.

людини; окремі факти, що характеризують об’єкти, процеси й явища в предметній області, а також їх властивості; представлення фактів, понять або команд у формалізованому вигляді, зручному для інтерпретації людиною або автоматичної обробки комп’ютером.

Включення комп'ютерних даних до складу «носіїв інформації» не зовсім точне, оскільки комп'ютерні дані — це змістовна частина, а носій інформації — це фізичний об'єкт наприклад, диск, флеш-накопичувач). Формулювання «інші носії інформації (у тому числі комп'ютерні дані)» є дещо некоректним, оскільки, як ми зазначали комп'ютерні дані — це сама інформація. Не узгоджується ця норма також з концепцією електронних доказів.

На нашу думку, дослідження термінології, що використовується у чинних нормативно-правових актах, а також в законопроєктах, які є на розгляді у ВР стосовно поняття електронних доказів, дає можливість визначення переваг і недоліків окремих із них, а також оцінка потенційних наслідків їх використання для правозастосовної практики. І дане дослідження буде нами продовжено в наступному розділі.

Зважаючи на важливість визначення ознак досліджуваного поняття, оскільки вони дають можливість акумулювати різноманітні його аспекти, всебічно охопити різні прояви, перейдемо до цього напрямку нашого дослідження в розділі 1.3. Передусім підкреслимо, що у науці вже існує досить детальне розкриття цієї проблематики. Ми вважаємо за необхідне побудувати нашу наукову роботу саме таким чином, щоб потім надати обґрунтоване власне бачення поняття електронні докази.

1.3. Характерні ознаки електронних доказів та їх місце в системі процесуальних джерел доказів

Питання з'ясування ролі електронних доказів у кримінальному процесі набуває в сучасних умовах інформаційного суспільства все більшу актуальність і потребує якомога швидшого законодавчого вирішення. Помилки, які допускаються при розслідуванні кримінальних правопорушень, вчинених з використанням інформаційних технологій, тягнуть за собою втрату інформації, яка б могла стати потенційним доказом.

Ми підтримуємо позицію тих науковців та практиків, які обґрунтовують необхідність виокремлення електронних доказів як окремого самостійного процесуального джерела доказу у кримінальному провадженні та звернемося до питання їх характерних рис. Адже для належного розуміння сутності електронного доказу перш за все слід визначити ті специфічні ознаки, що відрізняють його від інших джерел доказів. Задля уникнення зайвого дублювання вже наявних наукових напрацювань, а також зважаючи на обмежений обсяг нашого дослідження, зауважимо відразу, що характеристика електронних доказів, зокрема, їх відмінних рис була предметом ретельної наукової розвідки.

Важливе наукове значення мають різні підходи до тлумачення їхнього правової природи та унікальних характеристик. Проте у доктрині кримінального процесу та практиці кримінального процесуального доказування це питання до цього часу залишається дискусійним. Тому, з метою встановлення чітких орієнтирів для побудови подальших концепцій та висновків у межах цієї дисертації необхідно визначитися з характерними ознаками електронних доказів, що в свою чергу, дасть можливість навести додаткові аргументи необхідності виділення електронних доказів як самостійного джерела.

Аналіз наукових праць дозволяє констатувати широке та досить різнорідне коло виділених ознак, що характеризують електронні докази та дають підстави для відмежування їх від інших джерел доказів. Переважна більшість дослідників виділяють ті чи інші характерні риси, однак підходи до їх визначення істотно різняться. У цьому контексті для систематизації наукових поглядів пропонується виділити три узагальнюючі критерії, за якими можна класифікувати ознаки електронних доказів: форма існування, спосіб формування, середовище існування.

Ми вважаємо, що осмислення вказаних аспектів, створює основу для глибшого теоретико-практичного розуміння природи електронних доказів та дозволяє виокремити їх ключові ознаки. У подальшому ці ж критерії буде використано для систематизації класифікаційних підходів до електронних доказів, що забезпечить послідовність та внутрішню логіку дослідження. Результати огляду

наукових джерел, у яких висвітлюються ознаки електронних доказів, подаватимуться відповідно до окреслених вище дослідницьких векторів. Такий підхід дозволить упорядкувати наукові ідеї та простежити логіку виділення характерних ознак електронних доказів.

Форма існування

– існування у нематеріальному вигляді [3, с. 251; 10, с. 222; 18, с. 9; 26, с. 50; 27, с. 303; 124, с. 75; 125, с. 180; 145, с. 187; 350; 353, с. 259];

– можливість існування у декількох формах: статичній (у вигляді двійкового коду, файлу із зовнішніми атрибутами, оперативної пам'яті) і динамічній (у вигляді вторинно сформованої у часі сигнальної згортки, фізичних полів електромагнітних, електричних, оптичних й акустичних сигналів) [250, с. 87];

– їх не можна безпосередньо сприймати та досліджувати, тільки за допомогою технічних засобів і програмного забезпечення [3, с. 251; 10, с. 222; 18, с. 9; 27, с. 303; 67, с. 41; 84, с. 50; 102, с. 420; 114, с. 304; 115, с. 64–65; 116; 123, с. 119; 248, с. 211; 250, с. 87].

– потребують специфічного порядку збирання, перевірки та оцінки [3, с. 251; 115, с. 67; 239, с. 77–78];

Спосіб формування

– можуть бути створені як людиною, так і бути результатом функціонування інформаційної системи [3, с. 251; 102, с. 420];

– мають здатність до дубляжу, тобто копіювання або переміщення на інший носій без втрати своїх характеристик [3, с. 252; 26, с. 50; 67, с. 41; 102, с. 420; 352, с. 208];

– відсутність електронних копій електронних доказів [144, с. 14];

– відсутність жорсткої позиційної прив'язки як до тієї чи іншої ділянки машинного носія, так і до певного носія в цілому [2, с. 252; 115, с. 45; 250, с. 89];

– має особливий статус оригіналу і може існувати у такому статусі у декількох місцях [53, с. 13; 146, с. 106–107];

– невидимі «неозброєним оком», а тому для їх виявлення послуговуються спеціальним програмним та апаратним інструментарієм; також вони здебільшого нестійкі до впливу фізичних чинників, оскільки легко модифікуються, знищуються тощо; їх відносно легко копіювати, найчастіше не втрачаючи якості [349, с. 15];

– вони не можуть сприйматися безпосередньо, а мають бути інтерпретовані у певний спосіб і проаналізовані за допомогою спеціальних технічних засобів і програмного забезпечення [10, с. 222; 16, с. 451–452];

– конвергентність (здатність одиничного доказу входити у сукупність інших доказів і набувати в зв'язку з цим доказове значення [353, с. 257].

Середовище існування

– фіксованість комп'ютерної інформації на матеріальному носієві [18, с. 5];

– наявність ідентифікаційних атрибутів [18, с. 7];

– можуть існувати в декількох місцях одночасно, наприклад, якщо зроблено копію з телефона на інший пристрій, то така інформація буде міститися на двох пристроях [101, с. 176; 125, с. 180];

– мультиплікативність, тобто можливість одночасного існування на різних носіях [67, с. 41];

– можливість дистанційного внесення змін до них та знищення [3, с. 251–252];

– не речовий характер, який пов'язаний із відсутністю твердого зв'язку з матеріальним носієм [114, с. 304].

– не мають нерозривного зв'язку з матеріальним носієм; вільно переміщуються в електронній мережі без технічного носія [3, с. 251–252];
– мінливість (можливість бути зміненою з віддаленого доступу або взагалі без участі людини за допомогою спеціально створеної програми) [149, с. 297–298; 114, с. 304].

– трансльованість (можливість бути переданою з одного носія на інший), мультиплікативність (можливість одночасного існування однієї і тієї ж інформації на різних носіях) та мінливість (можливість бути зміненою з віддаленого доступу

або взагалі без участі людини за допомогою спеціально створеної програми) [149, с. 297–298].

– вони є нестійкими, за певних обставин інформація в пам’яті пристрою може бути змінена або втрачена [102, с. 420];

– «вразливість» як ознака електронних доказів [10, с. 222; 18, с. 9; 350, с. 82].

За результатами нашого дослідження, учені досить часто називають одну і ту ж ознаку електронних доказів, але в різній інтерпретації.

Слід зауважити, що запропонований поділ є доволі умовним, оскільки окремі ознаки електронних доказів можуть відповідати кільком критеріям. Так, певна характеристика може одночасно відображати і спосіб формування і середовище існування. Така класифікація має радше аналітичний, ніж жорстко структурований характер і слугує інструментом для впорядкування наукових поглядів та ідей щодо ознак електронних доказів, що наводяться у фаховій літературі.

У працях науковців також простежується певна єдність у виділенні ключових ознак, що дозволяють відмежувати електронні докази від інших джерел доказів. Погоджуючись із науковими поглядами щодо притаманності електронним доказам вищезазначених ознак, водночас вважаємо за доцільне виокремити також низку специфічних характеристик, які, на погляд автора, найбільш повно розкривають сутність електронних доказів та дають підстави для виділення їх як окремого процесуального джерела. До таких ключових ознак ми відносимо:

1) відтворюваність —можливість копіювання без втрати первинного змісту. Ця ознака водночас розширює можливості сторін кримінального провадження щодо доступу до доказів, але й актуалізує проблему забезпечення автентичності та збереження первісного змісту інформації;

2) нематеріальність –існують у вигляді цифрових даних, закодованих у вигляді бінарних або інших електронних сигналів та можуть бути відображені лише через спеціальні технічні пристрої цифровий формат, які зберігаються, передаються та обробляються за допомогою електронних пристроїв;

3) динамічність — можливість змінюватися під впливом програмного забезпечення або користувацьких дій. Електронні докази легко змінюються або видаляються, що створює ризик втрати або підробки доказів. Ця ознака враховується для запобігання віддаленому знищенню або зміні інформації на електронних пристроях[17] [до примітки див. 331];

4) залежність від технічних носіїв (для збереження, перегляду, перевірки електронного доказу потрібне спеціальне програмне забезпечення або обладнання);

5) відсутність жорсткої прив'язки до матеріального носія (можливість існування однієї і тієї інформації одночасно на різних, не зв'язаних між собою, носіях). Яким чином ця ознаки враховуються у судовій практиці можна побачити на прикладі конкретних судових рішень;

6) наявність метаданих (електронні докази містять метадані, які не є основним змістом файлу, але допомагають визначити його автентичність, час створення, редагування, авторство). Це фактично додаткова інформація про певний електронний об'єкт. Наприклад, у фотографіях та відео за допомогою метаданих можемо визначити час та дату зйомки, місцезнаходження (GPS- координати), параметри камери, формат та тип файлу; в електронній пошті —можемо визначити адресу відправника та одержувача, час відправлення повідомлення, IP- адресу сервера, тощо.

Хочемо відзначити, що дискусія щодо місця електронного доказу у системі процесуальних джерел доказів з погляду de jure і de lege ferenda розпочалася ще в 1970 роки і до цього часу не отримала логічного завершення. Системний аналіз наукових підходів щодо місця інформації в електронному вигляді в системі доказів дає підстави для виділення чотирьох підходів: (1) можливість віднесення цієї категорії об'єктів до документів; (2) можливість віднесення цієї категорії об'єктів

[17] Слідчий, обґрунтовуючи клопотання про обрання запобіжного заходу у вигляді тримання під вартою,зазначив, що підозрюваний при фактичній можливості доступу до Інтернету та веббраузерів може віддалено знищити, спотворити будь-які електронні документи,які містяться на носіях інформації,вилучених у нього під час проведення обшуку та облікових записах, що ним використовувалися для вчинення кримінальних правопорушень.

до речових доказів; (3) можливість віднесення цієї категорії об'єктів як до документів, так і до речових доказів; (4) необхідність виокремлення електронних джерел доказової інформації як самостійного процесуального джерела [67, с. 40].

З погляду de jure, враховуючи законодавче закріплення лише чотирьох джерел доказів, можна розглянути думку науковців, що електронний документ на цей час може бути документом або речовим доказом. Розмежувати електронний документ від речового доказу в електронній формі необхідно по доказовому значенню інформації чи матеріального об'єкта, на якому зберігається така інформація [132, с. 170]. Однак, ми вважаємо, що таке законодавче закріплення не дає фактичного розуміння, що електронний документ є одним із видів електронних доказів.

В свою чергу деякі науковці термін «електронний документ» тлумачать як різновид, одну із форм існування іншого джерела доказів – документа [140, с. 14].

Як один із різновидів окремої групи речових доказів пропонують розглядати «комп'ютерні об'єкти» також і А. С. Білоусов та Д. В. Пашнєв [18, с. 14; 149, с. 297–298].

І. О. Крицька, опонуючи науковцях, які вважають за необхідне «електронні докази» визнавати речовими доказами, приходить до висновку, що цифрові носії інформації повинні визнаватися речовими доказами тільки в тих випадках, коли доказове значення мають відомості про їх зовнішні ознаки, властивості, місце розташування або інші характеристики [114, с. 303]. Однак, в дисертаційному дослідженні І. О. Крицька з погляду de jure з урахуванням чинного законодавства обстоює позицію щодо доцільності визнання цифрових джерел доказової інформації саме речовими доказами, виходячи з того, що їх змістом є сама цифрова інформація, матеріальною формою – її цифровий носій, а процесуальною – відповідне процесуальне оформлення [115, с. 76].

На нашу думку, якщо вживати категорію «речові докази» для об'єктів, що існують в електронній формі, варто зазначити, що їхнє визнання речовими доказами не випливає безпосередньо з їх процесуальної природи, передбаченої

кримінальним процесуальним законодавством. Натомість такий «статус» їм надається шляхом прийняття відповідного процесуального рішення слідчого чи дізнавача про визнання носія інформації в електронному вигляді речовим доказом. Це в свою чергу, створює підстави для застосування до нього заходів забезпечення, зокрема, накладення арешту слідчим суддею.

Звернемо увагу також на існування альтернативної думки. Так, А. В. Столітній, І. Г. Каланча вважають електронні докази штучно створеним інститутом і відповідно який має значення тільки в теоретичному аспекті, адже джерела доказів, що визначені статтею 84 КПК України відповідно до чинного кримінального процесуального законодавства та умов сьогодення можуть мати також електронну форму. Вони критично відносяться до ідеї виділення інформації в електронному вигляді в окреме джерело [268, с. 182].

Ми не поділяємо думку науковців, які вважають, що незважаючи на особливості такої інформації не потрібно відносити її до окремого виду доказів. Адже саме характерні ознаки електронних доказів, що були ґрунтовно проаналізовані в науковій літературі та стали предметом нашого дослідження створюють підґрунтя для їх концептуального осмислення як самостійного процесуального джерела доказів у кримінальному провадженні. Вони дають змогу вписати феномен електронних доказів у внутрішньо узгоджену систему кримінального процесуального доказування.

Про необхідність виділення електронних доказів в окреме джерело з врахуванням їх ознак зазначають також вчені Д. О. Алєксєєва-Процюк та О. М. Брисковська [3, с. 252].

С. О. Ковальчук відмічає, що електронні докази з врахуванням механізму їх залучення у кримінальне провадження та існування в електронній формі по аналогії з їх закріпленням в адміністративному, господарському і цивільному процесах, підлягають визнанню самостійним видом доказів у кримінальному процесі [98, с. 123].

Також і інші науковців, які обґрунтовують необхідність віднесення електронних доказів до окремого джерела, обумовлюють це специфічними ознаками таких доказів. Так, Д. М. Цехан відстоює подібний підхід, зазначаючи, що цифровий об'єкт, який є нематеріальним, не має відповідних якісних фізичних характеристик, має специфічну процедуру та середовище створення, здатний до копіювання та переміщення без втрати характеристик, сприймається людиною лише після обробки ЕОМ та виведення інформації на відповідний технічний пристрій (монітор), неможливо визнати матеріальним об'єктом і, як наслідок, речовим доказом чи традиційним документом [353, с. 257]. Аргументи на користь даної позиції приводить і О. П. Метелев, який стверджує, що доказове значення має власне інформація, а не матеріальний об'єкт, на якому вона зафіксована [125, с. 177; 128, с. 102].

На підтвердження нашої думки щодо необхідності виділення електронних доказів як окремого процесуального джерела варто також звернутися і до аргументації науковців М. В. Гуцалюка, П. Є. Антонюка, які аналізуючи норму ч.3 ст.99 КПК України, що цифрова (електронна) інформація не може бути документом як процесуальним джерелом доказів, адже не є матеріальним об'єктом [64, с. 119; 65, с. 41].

І. В. Казанчук звертає увагу на таку ознаку електронних доказів як відсутність зв'язку із конкретним матеріальним джерелом, аргументуючи неможливість віднесення цих доказів до речових. [82, с. 6, 15].

А. В. Ратнова в дисертаційному дослідженні пропонує визнати електронний документ самостійним процесуальним джерелом доказів, доповнивши ч.2 ст.84 КПК України, що на її думку полегшить роботу практичних підрозділів та усуне законодавчі прогалини [238, с. 42].

Не можемо погодитися з висловленою думкою Д. О. Літкевича про відсутність необхідність нормативного закріплення в КПК нового процесуального джерела доказів, а саме електронного або цифрового доказу [123, с. 78], адже попри те, що на сьогодні чинне кримінальне процесуальне законодавство дозволяє

оцінювати інформацію в електронній формі в межах наявних джерел доказів, такий підхід створює серйозні труднощі у правозастосуванні. Зокрема, відсутність чіткого визначення електронних доказів у КПК України унеможливлює формування єдиного підходу до їх збирання, зберігання, дослідження, оцінки.

А. Б. Антонюк, А. В. Русецька наголошують на важливості імплементації положень Будапештської конвенції в національне законодавство і одним із кроків називають визначення в КПК поняття «електронні докази» [5, с. 85; 6; 353, с. 259].

В свою чергу Н. М Ахтирська, О. Ю. Костюченко також піднімають на обговорення наукової спільноти важливі питання збирання електронних доказів під час міжнародного співробітництва. Науковці звертають увагу на те, що відсутність нормативної визначеності не сприяє єдності судової практики, особливо гостро постає питання щодо оцінки електронних доказів, одержаних у межах міжнародної правової допомоги [8, с. 192]. Обґрунтовують логічність прийняття спеціального ЗУ «Про електронні докази», в якому визначити поняття електронних доказів, види, способи збирання, оцінки та використання [8, с. 198].

Віддаючи належне цінності наукових ідей, висловлених авторами, водночас дозволимо собі не погодитися з доцільністю ухвалення окремого спеціального закону присвяченого електронним доказам. На нашу думку, більш обґрунтованим та ефективним підходом є внесення змін до чинного КПК шляхом доповнення його окремою главою, яка б регламентувала особливості збирання, дослідження та оцінки електронних доказів на стадії досудовому розслідування прокурором, слідчим, слідчим суддею та судом під час судового провадження. Окрему увагу необхідно приділити процесуальному порядку отримання електронних доказів у межах міжнародного співробітництва.

Н. Ахтирська, О. Костюченко, Ю. Середа, А. Виноградова, І. Мірошников також наголошують на потребі удосконалення законодавства щодо порядку отримання транснаціональних електронних доказів у процесі інтеграції України до правового простору ЄС [418, с. 301]. Це особливо важливо, оскільки інші правила КПК, пов’язані з доказами, не відповідають концепції електронних доказів, адже

всі наявні процесуальні заходи покликаються на доказ як на фізичний або матеріальний об'єкт [235, с. 9].

У цьому контексті необхідно зазначити, що у вітчизняному цивільному, адміністративному, господарському процесуальному законодавстві також обрано підхід щодо виділення електронних доказів як самостійного виду доказів (ст. 100 ЦПК, ст. 99 КАС, ст. 96 ГПК).

На думку А. В. Коваленка, А. В. Ратнової такий законодавчий підхід є прогресивним і може бути використаний і для кримінальної процесуальної галузі [93, с. 239; 236, с. 237].

Висловлюючи власну думку стосовно цього питання, зазначимо таке: безумовно, враховуючи правову природу електронних доказів, унікальні характеристики віднесення їх до самостійного джерела буде достатньою підставою для визначення окремого порядку отримання доказової інформації, її дослідження та оцінки. Окрім того, належний порядок отримання доказів має враховувати сутнісну природу та процесуальне місце останніх.

До речі, переважна більшість опитаних респондентів (1289) вважають за необхідне виділити електронні докази як окреме процесуальне джерело у кримінальному процесуальному законодавстві України (74 % суддів, 67 % прокурорів, 59 % слідчих (дізнавачів) та 100 % адвокатів) і при цьому 56% від загальної кількості опитуваних висловили думку щодо недостатнього та неповного нормативного регулювання процесуального порядку збирання доказів, 17 % не можуть визначити у цьому питанні; 62 % від загальної кількості опитуваних вважають за необхідне регламентувати в окремій главі КПК процесуальний порядок збирання, фіксації та критерії оцінки електронних доказів (Додаток Б).

Таким чином, можна зробити висновок, що як більшість науковців так і практиків переконані, що законодавче закріплення електронних доказів в кримінальному процесуальному законодавстві стане важливим кроком на шляху вдосконалення доказового права, сприятиме удосконаленню правових механізмів збирання, збереження та оцінки таких доказів.

Отже, de lege ferenda (з погляду закону, прийняття якого бажане), уявляється більш вдалим підхід, спрямований на виділення електронних доказів як самостійного процесуального джерела. Характерні ознаки, що були нами досліджені щодо цих доказів, становлять важливий аргумент на користь їх виділення в самостійне джерело. Однак, окрім цього, ми також прагнемо навести додаткові аргументи, які підкріплюють необхідність такого кроку.

1) *трансформація інформаційного середовища*. Сучасна реальність характеризується цифровізацією суспільних відносин, що зумовлює появу нових джерел інформації, які можуть мати доказове значення. Значна частина даних сьогодні створюється, зберігається і передається виключно в електронній формі, що вимагає відповідної реакції законодавця.

2) *правова визначеність та уніфікація судової практики*. Відсутність чіткого процесуального закріплення статусу електронних доказів призводить до неоднорідності у правозастосуванні, створює суперечливу судову практику їх оцінки судами, зокрема щодо допустимості, належності та достовірності. Виокремлення електронних доказів як окремого джерела сприятиме уніфікації підходів.

3) *невідповідність традиційних джерел доказів сучасним технологічним реаліям*. Електронні докази мають особливу природу—вони характеризуються нематеріальністю, динамічністю, залежністю від технічного середовища, що унеможливлює їх повноцінне включення до категорії речових доказів або документів .

4) *захист прав учасників кримінального провадження*. Такий крок сприятиме більш чіткому регулювання процедур збору, використання електронних доказів та їх оцінки, що в свою чергу дозволить уникнути юридичних колізій та забезпечить дотримання принципу справедливого судочинства.

5) *європейські стандарти та міжнародна практика*. У деяких країнах Європи електронні докази закріплені як окреме джерело. Наприклад, ст. 136 «Електронні докази» КПК Латвії визначає, що доказами в кримінальному процесі

можуть бути відомості про факти у формі електронної інформації, обробленої, збереженої або переданої пристроями або системами автоматизованої обробки даних [394]. І хоча в більшості країни Європи в кримінальних процесуальних кодексах відсутнє закріплення поняття «електронні» або «цифрові докази», наприклад, КПК Французької Республіки [390]; КПК ФРН [397]; КПК Італії [370]; КПК Литви [393]; КПК Естонії [391], КПК Португалії [392], повністю підтримуємо висловлене бачення М. В. Гуцалюка та П. Є. Антонюка, що «прогресивна нормотворча діяльність нашої держави може стати прикладом для інших країн і певним кроком у подальшій гармонізації та уніфікації норм міжнародного права» [65, с. 44].

Крім того, міжнародні документи, зокрема, Другий додатковий протокол до Будапештської конвенції про кіберзлочинність, який передбачає механізми, що надають змогу оперативно запитувати та надавати електронні докази в межах міжнародного співробітництва, містить орієнтири щодо необхідності чіткого регулювання електронних доказів в національному законодавстві.

Також в обґрунтування нашої думки вважаємо за необхідне згадати наявні рекомендації щодо України, які містяться у звіті «Про чинне законодавство і проєкти законів, що доповнюють різні питання, пов’язані з кіберзлочинністю та електронними доказами, та вносять зміни до них» від 03.11.2016 р. № 2016/DGI/JP/3608. Так, п. 9 згаданого Звіту говориться про те, що запровадження поняття «електронні докази» збільшить правову чіткість і передбачуваність закону [235, с. 7].

Хочемо відмітити, що законодавець вже робив спроби вписати електронні докази в існуючу систему процесуальних джерел, при цьому не враховуючи їх специфічну природу. Так, в законопроєкті № 2740 від 15.01.2020 р. електронну інформацію було віднесено до речових доказів за умови відповідності критеріям зазначеним у ч. 1 ст. 98 КПК України [217]. Пристрій для обробки, передавання та зберігання такої інформації був віднесений до речових доказів, крім відповідності критеріям визначеним у ч. 1 ст. 98 КПК України, також у випадку, коли електронна

інформація як речовий доказ не могла бути копійована без пошкодження чи знищення цього пристрою. Подібний підхід до розв'язання цієї прикладної та наукової проблеми також був зроблений у законопроєкті № 9484 від 17.01.2019 р. [218].

Однак, слід зазначити, що виділення електронних доказів як окремого процесуального джерела само по собі не забезпечить ефективну процедуру збирання, оцінки доказової інформації. Для забезпечення належної правозастосовної практики необхідно вирішити ряд важливих завдань, серед яких ключовими є забезпечення термінологічної точності та усунення суперечності в нормативно-правових актах. Питання визначення місця електронних доказів в системі процесуальних джерел не обмежується лише теоретичним значенням, а має й практичний характер.

Незважаючи на доволі широку палітру напрямів наукового осмислення проблематики електронних доказів у кримінальному процесі, все ж доводиться констатувати відсутність єдності у розумінні окремих базових питань даної тематики, зокрема стосовно формулювання визначення «електронні докази», на що ми детально звернули увагу у попередніх підрозділах.

Водночас, необхідно наголосити на тому, що понятійно-категоріальний апарат кримінальної процесуальної науки повинен формуватися з урахуванням цифрових інновацій. В той же час, система законодавства, як основна юридична форма права, має відповідати ознакам узгодженості та понятійної (термінологічної) єдності [126, с. 91], а для того, щоб усунути термінологічне багатоманіття потрібно після дослідження сутнісних особливостей даного «феномену» та результатів дослідження, яке проводилося в підрозділі 1.2. визначити власне визначення поняття електронних доказів.

Як відомо проблема доказового права займає одне із центральних місць у кримінальній процесуальній науці. Доказове право є фундаментом науки кримінального процесу, адже дає розуміння, якою повинна бути процесуальна форма, щоб забезпечити швидке, повне та неупереджене розслідування і судовий

розгляд, виконуючи основне завдання кримінального провадження – захист особи, суспільства та держави від кримінальних правопорушень (ст.2 КПК).

Не заглиблюючись у витоки наукової дискусії щодо проблеми доказування, яка не є предметом нашого дослідження необхідно звернути увагу на основні моменти, які ми брали до уваги при визначенні поняття «електронні докази». Таким чином, проаналізувавши характерні ознаки електронних доказів, приходимо до цілком логічного висновку, що електронний доказ відрізняється від інших доказів і формування поняття даного доказу буде мати праксеологічне значення.

З позиції логічної семантики необхідно дати таке визначення, за допомогою якого б розкривався смисл визначуваного нами терміну. Це відбувається шляхом уточнення або видозмінення усталеного смислу терміну або введення принципово нового значення і смислу для терміну.

На початковому етапі нашого дослідження нами визначалися електронні докази як будь-які дані, представлені в електронній формі, на основі яких слідчий, прокурор, суд в визначеному процесуальним законодавством порядку встановлює наявність чи відсутність обставин, які підлягають доказуванню у кримінальному провадженні [263, с. 228]. У процесі наукового осмислення ми прийшли до висновку за необхідне визначати поняття електронні докази через категорію інформації.

Цілком погоджуємося з думкою Н. Білоцерковець, що однією з умов формулювання якісної дефініції поняття електронних доказів, незалежно від їх конкретної назви, буде поняття, яке міститиме якомога менше технічних термінів і понять. Іншими словами слід дотримуватись принципу технологічної нейтральності, зміст якого полягає в тому, що встановлені чи санкціоновані державою норми права не повинні вести до різних юридичних наслідків при застосуванні різних технологій у подібних правовідносинах [19, с. 107].

Так, поняття — це форма мислення, яка є результатом узагальнення і виділення предметів деякого класу за загальними та специфічними для них ознаками» [107, с. 131]. Оскільки поняття є форма абстрактного мислення, то для

нього, як для абстрактного мислення в цілому, характерна така ознака, як зв'язок з мовою. Тобто, мовною формою понять в природній мові є слова і словосполучення. Зв'язок поняття і мови полягає в тому, що будь-яке слово реалізується, втілюється у понятті, але не всяке слово чи словосполучення виражає поняття. Функція слів чи словосполучень полягає у «називанні» понять, але вони безпосередньо не співпадають з словесним виразом ознак, що фіксуються в понятті [107, с. 134].

Отже, визначенням називається логічна процедура, за допомогою якої відшукується, будується який-небудь предмет, відрізняється від інших, а також формується значення вперше вживаного терміна чи уточнюються значення уже існуючого терміна. Назва операції визначення походить від латинського слова – definitio, дефініція. Тому часто замість назви «визначення» вживають слово «дефініція» [107, с. 165].

Звернемося до визначення доказів, яке міститься в КПК України[18] [до примітки див. 113]. Визначення поняття «доказ» забезпечує однаковість у тлумаченні гносеологічних, правових, логічних характеристик кожного із виду доказів, сприяє усуненню суперечливості й ефективності застосування певних норм, що відносяться до кожного процесуального джерела доказів [367, с. 48].

В. Г. Гончаренко визначає доказування як одну з форм практичної діяльності в процесі регулювання суспільних відносин, яка полягає у збиранні, дослідженні, оцінці й використанні *інформації* (курсив наш - І. Смаль), котра за певних умов, визначених процесуальним законом, *набуває статусу юридичних доказів* (курсив наш - І. Смаль) [56, с. 8].

Ю. М. Грошевий визначав доказування як кримінально-процесуальну діяльність спеціально уповноважених на це суб'єктів зі збирання, дослідження й

---

[18] Доказами в кримінальному провадженні є *фактичні дані* (курсив наш - І. Смаль), отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють *наявність чи відсутність фактів та обставин* (курсив наш - І. Смаль), що мають значення для кримінального провадження та підлягають доказуванню» (ст. 84 КПК України). Доказ складається як з фактичних даних так і з джерела інформації : речові докази, документи, показання, висновок експерта (ч.2 ст.84 КПК України)

оцінки доказів, мета якої є *встановлення обставин* (курсив наш - І. Смаль), що входять до предмета доказування в кримінальній справі [61, с. 199].

Досить цікаво поглянути на «факт» з філософської точки зору[19] [до примітки див. 348, с. 661].

А. М. Погорецький зазначає, що фактичні дані як відомості (інформація) про факти (обставини кримінального правопорушення) являють собою основу для одержання доказів. Однак вони стають доказами не автоматично, навіть за умови отримання їх із встановлених законом джерел, відповідно до визначеної кримінальним процесуальним законом для кожного з їх видів форми, а лише після визнання їх доказами особою, у провадженні якої перебуває кримінальне провадження. Саме з цього моменту сукупність фактичних даних та їх джерел набуває статусу доказу у кримінальному провадженні [154, с. 58].

Ми переконані, що дискусія щодо визначення поняття для позначення інформації в електронному вигляді як доказу далеко не завершена, в свою чергу пропонуємо надати власне визначення цього поняття, яке на нашу думку, поєднує як специфічні ознаки, так і загальні поняття доказів у класичному розумінні.

Відтак, *електронний доказ – це інформація в електронному вигляді, що містить відомості про обставини, що мають значення для кримінального проводження та підлягають доказуванню, створена, збережена, або передана за допомогою електронних пристроїв, систем, або мереж та яка існує в формі, що забезпечує її автентичність, цілісність та придатність для дослідження*.

Для реалізації принципу правової визначеності у вітчизняному кримінальному судочинстві необхідно законодавчо закріпити поняття електронний

---

[19] Факт — це філософське і загальнонаукове поняття, широко вживається у всіх галузях пізнання, має певний ряд смислових значень: 1) явище або подія, що насправді мала місце в реальній дійсності і встановлені як даність у безпосередньому спостережені чи експерименті засобами чуттєвого споглядання та показаннями приладів. Характеризується об’єктивністю і відносною незалежністю від способів виявлення, а тому в процесах пізнання і мислення відіграє роль свідчень про істинний стан речей в об’єктивній дійсності; 2) знання, достовірність якого не викликає сумніву і забезпечується прямим зіставленням з реальною ситуацією в дійсності за допомогою відчуттів, сприймання, уявлення; 3) судження або висловлення, що мають значення істини і в процесах пізнання та мислення виступають підставами для визначення істинності інших суджень або висловлювань, входячи до складу процедур доведення та логічного доказу.

доказ у КПК, що нами і запропоновано у відповідному законопроєкті (див. додаток Г).

Висновки до розділу 1

Аналіз теоретичних та практичних питань, пов'язаних з визначенням правової природи електронних доказів у кримінальному процесі, дозволив зробити наступні висновки:

1. Проведене в першому розділі дослідження витоків, становлення та розвитку концепції електронних доказів у кримінальному процесі крізь призму доктринальних підходів, судової практики та технологічного прогресу дозволило в процесі проведеного дослідження виокремити основні періоди : І період— 1970-2000 р. Становлення доктринальних підходів щодо поняття «електронний документ»;

ІІ період — 2001-2012 р. Подальший розвиток наукових уявлень щодо інформації, отриманої з електронних джерел та законодавче закріплення терміну « електронний документ»;

ІІІ період— 2012-сучасний період. Прийняття КПК України, подальший доктринальний пошук оптимальних моделей використання інформації в електронному вигляді як доказу .

Такий підхід надав змогу простежити зміни у правовому та практичному підході до електронних доказів, враховуючи внесок наукової спільноти у формуванні їхнього сучасного розуміння та показав, як в різні періоди змінювалося розуміння поняття «електронні докази». Термін «електронний документ» спочатку застосовувався в наукових дослідженнях, а згодом був закріплений в національному законодавстві України, пізніше розуміння «електронний документ» еволюціонувало до ширшого розуміння — «електронних доказів». На нашу думку, цей процес має логічно завершитися офіційним закріпленням поняття електронних доказів у кримінальному процесуальному законодавстві.

2. Вивчення правової природи електронних доказів у кримінальному процесі

створило передумови для аналізу наукових праць вітчизняних учених, які в різні історичні періоди заклали фундамент подальших наукових досліджень у цій сфері. Це дозволило довести відсутність єдності в змістовому наповненні досліджуваного поняття «електронні докази» як у науці, так і в судовій практиці.

3. Сформульовано авторське визначення поняття електронні докази - це інформація в електронному вигляді, що містить відомості про обставини, що мають значення для кримінального проводження та підлягають доказуванню, створена, збережена, або передана за допомогою електронних пристроїв, систем, або мереж та яка існує в формі, що забезпечує її автентичність, цілісність та придатність для дослідження.

4. Дослідження правової природи електронних доказів дозволило виділити специфічні ознаки електронних доказів:1) нематеріальність; 2) динамічність; 3) відтворюваність; 4) залежність від технічних носіїв; 5) відсутність жорсткої прив'язки до матеріального носія; 6) наявність метаданих.

5. Запропоновано розширити коло процесуальних джерел та визначити електронні докази одним із самостійних процесуальних джерел. Основні ознаки електронних доказів, які стали предметом нашого дослідження, є переконливим підґрунттям для їх виокремлення у самостійне процесуальне джерело. Окрім того, в роботі наведено додаткові положення, що обґрунтовують необхідність такого кроку, а саме: 1) трансформація інформаційного середовища; 2) правова визначеність та уніфікація судової практики; 3) невідповідність традиційних джерел доказів сучасним технологічним реаліям; 4) захист прав учасників кримінального провадження; 5) європейські стандарти та міжнародна практика.

РОЗДІЛ 2
ВИДИ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

2.1. Класифікація електронних доказів

Важливе теоретичне та практичне значення має класифікація електронних доказів, адже вона сприяє адаптації кримінального процесу до умов цифрової епохи, формуванню єдиних стандартів доказування з врахуванням процесуальних особливостей із збирання, збереження, дослідження та оцінки.

Водночас варто зазначити, що складність класифікації електронних доказів зумовлена їхньою різноманітністю, технічною природою та динамічним розвитком цифрових технологій. По перше, електронні докази охоплюють широкий спектр даних: від аудіо- відеофайлів, текстових повідомлень, електронних листів до даних із серверів, метаданих, повідомлень із соціальних мереж тощо. Це створює труднощі у вироблені єдиних критеріїв класифікації. По друге, інформація в електронному вигляді може зберігатися на різних носіях та в різних форматах. По третє, технологічний розвиток приводить до постійних змін у формах та способах існування інформації в електронному вигляді. Якщо донедавна в кримінальних провадженнях як доказ, як правило, використовувалися аудіо- відеофайли, то наразі з’являються такі форми існування інформації в електронному вигляді як блокчейн-технології, криптовалютні транзакції.

У науковій спільноті існують різні підходи до класифікації електронних доказів зважаючи на форму існування, спосіб отримання, походження, тощо. Зокрема, український учений А. Ю. Каламайко, один із перших науковців, досліджуючи на дисертаційному рівні («Електронні засоби доказування в цивільному процесі», 2016 р.) проблемні питання використання в цивільному судочинстві електронних засобів доказування, здійснив спробу класифікації електронних доказів. Так, дослідник запропонував поділити їх на три групи: 1. звуко- та відеозаписи; 2. електронний документ; 3. інформаційне повідомлення.

Крім того, за джерелом походження серед електронних засобів доказування він виділяв: 1) файли, які створюються користувачем; 2) файли, які створюються комп'ютерною системою (тобто самим електронним середовищем) [83, с. 10].

А. М. Найченко в дисертаційному дослідженні «Електронні докази в господарському процесі», 2023 р. запропонувала наступну класифікацію[20] [до примітки див. 136, с. 56, 57].

І. Вернидуб, С. Белікова, досліджуючи особливості електронних доказів у кримінальному процесі, пропонують своє бачення класифікації електронних доказів в залежності від джерел їх надходження: 1) *електронні документи;* 2) інформація, отримана з відкритих джерел *мережі Інтернет;* 3) *аудіо- та відеозаписи*; 4) *електронні повідомлення*: мультимедійні та голосові повідомлення [27, с. 302].

У своїй статті «Класифікація електронних документів, як джерел доказів, у кримінальному провадження» А. В. Ратнова аналізує існуючі класифікації електронних документів, а не електронні докази, та враховуючи наукові дослідження, пропонує власні критерії класифікації. Так, авторка пропонує наступну класифікації електронних документів: 1) залежно від комбінацій метаданих (однорангові, дворангові, трирангові, чотирирангові, п'ятирангові (гіпертекст)); 2) за доступом до інформації (відкриті та приховані метадані); 3) за ступенем захисту електронні документи поділяє на відкриті та закриті; 4) за джерелом походження (файли, які створюються користувачем та

---

[20] « 1.За господарсько-процесуальним законодавством: електронні документи (у т.ч. текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо); веб-сайти (сторінки); текстові, мультимедійні та голосові повідомлення; метадані; бази даних; інші дані в електронній формі. 2. За характером зв'язку доказів з обставинами справи: прямі, непрямі. 3. За процесом формування доказу: первинні (першоджерела, оригінал); похідні (копії). 4. За походженням: від людини; електронним приладом (камери відеоспостереження тощо). 5. За способом відтворення: прості (які не потребують додаткових засобів та методів втручання для відтворення); складні (для відтворення потрібні спеціальні (додаткові)програми, обладнання). 6. За форматом: текстові (наприклад, повідомлення, документи); графічні (наприклад, зображення, відеозаписи); мультимедійні (наприклад, повідомлення, аудіозаписи). 7. За необхідним часом на опрацювання: об'ємні; малооб'ємні. 8. Залежно від періоду виникнення: минулі (докази, що виникли до розгляду справи); триваючі (докази, що існують на момент розгляду справи). 9. За місцезнаходженням: серверах та веб-ресурсах; цифрових носіях; магнітних носіях; внутрішніх накопичувачах (внутрішня пам'ять пристрою); жорстких дисках. 10. За ступенем доступності: загальнодоступні; з обмеженим доступом; з індивідуальним доступом

комп'ютерною системою (електронним середовищем); 5) за їх місцем розташуванням: комп'ютер, смартфон, планшет, відеокамера, «розумна» побутова техніка, інтернет-сервер та інші; 6) за формою (відеозаписи, аудіо записи, електронні повідомлення, вебсайти та інформація у електронній формі) [237, с. 44].

А. В. Гутник, А. Я. Хитра пропонують аналогічну класифікацію електронних документів [63, с. 58].

В монографічному дослідженні «Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання» Р. І. Благута та А. В. Мовчан визначають види цифрових (електронних) доказів: – локальні сліди: сліди прямого впливу; докази опосередкованого впливу; викривлення інформації; знищення інформації; блокування інформації; відсутність доступу; порушення конфіденційності; порушення роботи комп'ютера; – мережні сліди: дані про користувача (контактні дані, адреса, телефон, ім'я тощо); дані про повідомлення (номер телефону, лог-файли реєстрації доступу до тих чи інших інформаційних систем); – електронна інформація: цифрові фотозображення; відеоконтент; текстові документи; веб-сайти (сторінки); метадані; бази даних [21, с. 113].

В свою чергу, учені, наукова діяльність яких зосереджена на криміналістиці та судовій експертизі, Г. К. Авдєєва та С. В. Стороженко, досліджуючи електронні сліди, фактично здійснюють їх класифікацію за місцем генерування даних, оскільки поділ відбувається залежно від того, звідки походять електронні сліди (журнали операційних систем та окремих програмних продуктів; дані електронного листування; дані на різних сайтах (Facebook, Twitter)) [2, с. 171–172].

Л. П. Гринько пропонує виокремлювати віртуальні сліди, які залишаються на електронних носіях, та ті, що містяться в мережі «Інтернет» [60, с. 23].

А. С. Колодіна та Т. С. Федорова, працюючи над дослідженням, присвяченим впровадженню інноваційних технологій у криміналістичну експертизу, досліджуючи методи виявлення, збирання, збереження та аналізу електронних доказів виокремлюють активні цифрові відбитки (створюється даними, наданими користувачем, такими як персональні дані, відео, зображення і

коментарі) та пасивні цифрові відбитки (дані, які ненавмисно залишають люди, які користуються Інтернетом і цифровими технологіями (наприклад, історія переглядів в браузері)). Також вчені проводять класифікацію за наступними критеріями: «дані зберігаються в цифрових пристроях (наприклад, комп'ютерах, смартфонах, планшетах, телефонах, принтерах, «розумних» телевізорах (Smart TV) і будь-яких інших пристроях, які мають цифрову пам'ять), зовнішніх запам'ятовуючих пристроях (наприклад, зовнішніх жорстких дисках і USB-флеш накопичувачах), мережевих компонентах і пристроях (наприклад, маршрутизаторах), серверах і хмарному сховищі (де дані зберігаються «в кількох центрах даних в різних географічних точках), а також контент і метадані як різновиди цифрових слідів» [103, с. 178].

В свою чергу, Я. Найдьон, пропонує класифікацію віртуальних слідів кіберзлочинів», поділяючи їх на 4 групи: [21] [до примітки див. 135, с. 305].

А. В. Коваленко пропонує три групи критеріїв для класифікації електронних (цифрових) слідів: 1) за ознаками слідоутворюючого об'єкта; 2) за ознаками комп'ютерних даних як сліду; 3) за ознаками носія таких даних (слідосприймаючого об'єкта) [94, с. 202].

Як ми можемо бачити така класифікація має досить глибокий криміналістичний підхід, адже вона враховує механізм утворення слідів кримінального правопорушення у цифровому середовищі. Так, запропонована автором класифікація електронних (цифрових) слідів за критеріями, що

---

[21] за походженням: 1) електронна інформація, створена ЕОМ у процесі своєї роботи; 2) електронна інформація, створена в процесі діяльності людини; 3) похідна електронна інформація, створена комп'ютером на основі введених даних користувачем, або навпаки, інформація, створена з даних, згенерованих комп'ютерною системою; за формою подання: 1) людиночитабельна інформація (інформація, доступна для сприйняття людиною); 2) машиночитабельна інформація (інформація, представлена у вигляді машинного коду); за місцем зберігання: 1) дані, що зберігаються в комп'ютерних системах (ЕОМ, сервери, локальні мережі, глобальні мережі); 2) дані, скопійовані або переміщені користувачем на електронні носії(жорсткі диски, компакт-диски, накопичувачі); 3) паперові копії людиночитабельної або машиночитабельної інформації(копії листування, скріншоти та ін.); за формою: 1) вихідні дані (інформація, введена людиною); 2) людиночитабельні та машиночитабельні бази даних; 3) коди шифрування; 4) програмне забезпечення різних видів; 5) комп'ютерні системи (ЕОМ, сервери, локальні мережі, глобальні мережі).

характеризують слідоутворюючий об’єкт (сліди утворені внаслідок отримання ввідних даних і команд від користувача та утворені внаслідок виконання електронно-обчислювальною технікою заздалегідь закладених алгоритмів), знаючи джерело електронних доказів (програмне забезпечення, мережеві дії, дії користувача), надає можливість краще розуміти спосіб вчинення кримінального правопорушення.

Дослідник пропонує класифікацію електронних (цифрових) слідів за критеріями, що характеризують комп’ютерні дані як слід .За форматуванням даних: форматовані та неформатовані; за змістом даних: основні дані та метадані; за способом сприйняття інформації: дані, що несуть інформацію в аудіовізуальній формі та дані без аудіовізуальної форми; за автентичністю: незмінні (оригінальні, автентичні) та такі, що зазнали впливу (зміни) з метою приховування ознак кримінального правопорушення; за можливістю доступу: незахищені та захищені [94, с. 207–209].

Ми вважаємо, що, класифікація електронних слідів, запропонована науковцем, на формативні та неформативні є свого роду орієнтиром для слідчих та експертів, адже неформативні дані, тобто залишкові або змінені сліди внаслідок технічних збоїв, неповного копіювання не містять чіткої структури (наприклад, пошкоджений відеофайл) і для можливого використання їх в якості доказів, потрібно їх відновлювати, або, можливо, використовувати інші докази (щоб їх пояснити), що може вплинути на їх доказове значення. І цілком очевидно, щоб без криміналістичного дослідження не має можливості використовувати їх в якості доказів у кримінальному провадженні.

Також А. В. Коваленко пропонує класифікацію електронних (цифрових) слідів за критеріями, що характеризують носій даних (слідосприймаючий об’єкт): за місцем розташування носія комп’ютерних: електронні (цифрові) сліди на локальних носіях та сліди на віддалених носіях; за призначенням та типом встановлення носія: електронні (цифрові) сліди на внутрішніх та зовнішніх носіях; за енергозалежністю запам’ятовувального пристрою носія даних: електронні

(цифрові) сліди, що містяться на енергозалежних та на енергонезалежних носіях [94, с. 209, 210].

Практичне значення класифікації електронних слідів за критеріями, що характеризують дані, як ми вважаємо, важливе для ідентифікації джерела доказів та може враховуватися при їх виявленні, збиранні та збереженні. Отже, запропоновані науковцями-криміналістами класифікації, мають більш криміналістичне значення, допомагають вибирати правильні методи дослідження, дозволяють відразу визначити природу електронних доказів та можливі ризики при отриманні їх як доказів, забезпечують коректний аналіз, спрощення роботи з різними типами цифрових слідів Але в той же час допомагають під час оцінки доказів в суді розуміти наскільки такі докази можуть бути достовірними і чи, наприклад, можуть бути використані у кримінальному провадженні без проведення криміналістичних досліджень.

Вважаємо за доцільне в аспекті дослідження підстав для класифікації електронних доказів звернутися до результатів проведеного нами опитування 1289 практикуючих юристів щодо видів електронних доказів, з якими їм доводилося мати справу у своїй практиці. Так, за результатами опитування можемо бачити, що 85 % суддів, 64 % прокурорів, 100 % слідчих (дізнавачів), 80 % адвокатів стикалися у своїй практиці з аудіозаписами; 96 % суддів, 87 % прокурорів, 90 % слідчих (дізнавачів), 100 % адвокатів – з відеозаписами; 73 % суддів, 60 % прокурорів, 75 % слідчих (дізнавачів), 80 % адвокатів – з цифровими фотографіями та зображеннями; 65 % суддів, 58 % прокурорів, 63 % слідчих (дізнавачів), 80 % адвокатів – з електронними повідомленнями, електронною поштою; 51 % суддів, 48 % прокурорів, 59 % слідчих (дізнавачів), 40 % адвокатів – з веб сайтами (веб сторінками); 36 % суддів, 33 % прокурорів, 33 % слідчих (дізнавачів), 20% адвокатів – з даними геолокації; 29 % судді, 33 % прокурорів, 44 % слідчих (дізнавачів), 20 % адвокатів – з комп’ютерними даними; 45 % судді, 37 % прокурорів, 48 % слідчих (дізнавачів), 80 % адвокатів – з електронними документами (Додаток № Б, питання 9).

Аналізуючи результати опитування, слід врахувати можливі розбіжності у розумінні респондентами поняття «електронний документ». Законодавче визначення «електронного документу» (Закон України «Про електронні документи та електронний документообіг») передбачає наявність обов'язкових реквізитів, зокрема, електронного підпису. Однак, відповіді респондентів можуть включати більш широкий підхід, трактуючи як будь-які комп'ютерні дані, що використовуються в судовій практиці. При цьому судова практика також схиляється до розширеного тлумачення, розглядаючи електронні документи, не як документи з обов'язковими реквізитами, а загалом як електронні докази. На початку нашого дослідження, проводячи опитування серед практикуючих юристів, ми не до кінця усвідомлювали ступінь ототожнення понять «електронний доказ» та «електронний документ» у правозастосовній практиці. Під час формулювання запитань щодо видів електронних доказів, з якими стикаються судді, прокурори, слідчі, дізнавачі, адвокати, ми не уточнили нашого розуміння терміна «електронний документ». Це могло призвести до неоднозначного трактування запитань респондентами та, відповідно, до отримання відповідей, які не в повній мірі відображають реальну практику використання електронних доказів.

Досить цікавими є також результати соціологічного опитування опублікованого в статті І. Г. Каланчі «Практика роботи з доказами, що мають електронну форму в кримінальному процесі України: соціологічне дослідження» [85, с. 78, 80].

Провівши дослідження існуючих класифікацій електронних доказів, запропонованих іншими науковцями, ми розробили власний підхід до їх систематизації. Для обґрунтування та побудови цієї класифікації ми застосували сукупність наукових методів, що дозволяє забезпечити її комплексний характер та практичну цінність. За допомогою аналізу та синтезу, індукції та дедукції, враховуючи як раніше обґрунтоване нами поняття електронних доказів, так і специфічні ознаки електронних доказів, сформулювали власну класифікацію. При цьому ми розглядаємо електронні докази як цілісну систему з різними рівнями

взаємозв’язку. На основі аналізу наявних підходів, використовуючи формально-юридичний метод, який використовувався для аналізу нормативних актів, метод правового моделювання та емпіричні методи: соціологічний метод (проведено опитування практикуючих юристів) та метод узагальнення судової практики використання електронних доказів ми пропонуємо наступну класифікації електронних доказів за такими критеріями:

1) за формою існування;

2) за способом формування;

3) за технічним середовищем існування.

І. За формою існування:

1) електронні документи (документи, інформація в яких зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа);

2) текстові електронні докази (повідомлення електронної пошти, листування в месенджерах, таких як Viber, WhatsAPP, Telegram, Signal, тощо, документи в електронному вигляді, файли польотових журналів, текстові повідомлення про виконання завдань БпЛа);

3) мультимедійні електронні докази (відеозаписи, цифрові фотографії, аудіозаписи, інші мультимедійні файли).

Джерело отримання таких доказів: камери відеоспостереження, відеореєстратори, мобільні телефони, комп’ютери, безпілотні літальні апарати хмарні сервіси тощо ;

4) програмні електронні докази (програмне забезпечення, лог-файли та системні журнали (записи дій користувача в операційній системі чи програмному забезпеченні), дані з баз даних (витяги з CRM (Customer Relationship Management), які можуть містити історію комунікацій, дані про фінансові операції, дані про користувачів(профілі клієнтів, електронні підписи), програмні коди, дані автозбереження у хмарних сховищах, кеш-пам’ять браузерів, дані про використання певних програм, шкідливі файли (віруси, трояни));

5) метаінформація (метадані)- це дані про дані, які містять службову інформацію про файл, електронний документ, документ в електронному вигляді тощо. Метадані можуть бути видимими та невидимими для користувача.

До метаданих можна віднести:

- файлові метадані (відомості, які містять дані про дату створення, зміни або відкриття файлу; авторство);
- мережеві метадані(IP-адреса відправника та отримувача повідомлення; час та дата відправки; дані про пристрій з якого зроблено пошуковий запит);
-метадані цифрових зображень (налаштування камери, дата і час зйомки; координати GPS.

II. За способом формування:

1) первинні електронні докази (оригінал)- файл чи запис у тій самій формі, у якій він був створений або отриманий (електронний лист у форматі .eml, або .msg; відеозапис у тому самому форматі як він був записаний на пристрій; журнал серверів про дії користувачів; блокчейн-транзакція);
2) похідні електронні докази (копія);
3) автоматично сформовані електронні докази – створені без участі людини (метадані файлів, дані бортових журналів літаків, БпЛа, автомобілів);
4) створені користувачем (повідомлення, текстові документи, відео та аудіозаписи).

Класифікація електронних доказів за способом формування має значення при оцінці достовірності та автентичності доказів, що буде нами досліджено більш детально в наступному розділі.

III. За технічним середовищем існуванням:

1) локальні електронні докази – зберігаються на фізичних пристроях (комп’ютерах, телефонах, флеш-накопичувачах, безпілотних літальних комплексах бортових комп'ютерах або GPS-реєстраторах);
2) мережеві електронні докази – зберігаються у хмарних сховищах або віддалених серверах (наприклад, дані соцмереж, листування в месенджерах, веб-ресурси);

3) гібридні електронні докази (дані, які були збережені локально, а потім завантажені в Інтернет або передані через мережу (відео з телефону, опубліковане в YouTube).

З погляду науки класифікація електронних доказів потрібна для розуміння специфіки різних електронних доказів, адже кожен вид електронного доказу має свої особливості збору, збереження, аналізу та оцінки.

Проведене нами дослідження показує, що класифікація електронних доказів у кримінальному процесі допомагає визначити їхню доказову силу, визначити критерії оцінки належності, допустимості та достовірності. Цілком зрозуміло, що один і той же цифровий об’єкт може потрапляти під кілька класифікаційних категорій. Ці підходи можуть використовуватися для аналізу ефективності використання електронних доказів в доказуванні, встановлення процесуальних особливостей збирання, дослідження, сприятимуть формуванню єдиних стандартів доказування, а також удосконаленню правового регулювання їх використання.

Якщо ми звернемося до положень ст. 96 ГПК; ст. 100 ЦПК; ст. 99 КАС України, то можемо побачити, що законодавець визначив, що електронні докази — це інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі». [59; 99; 355].

З даної правової норми вбачається, що законодавець не ототожнює електронні докази з електронними документами, а визначає електронний документ як один із видів електронних доказів і такий підхід є цілком виправданий, адже без належного розмежування цих понять виникають логічні та правові суперечності.

По перше, електронний документ має чітко визначену правову природу: він є носієм інформації, що містить обов’язкові реквізити, зокрема, електронний підпис та інші засоби ідентифікації автора. Водночас графічні зображення, плани, фотографії, відео- та звукозаписи не можуть мати електронного підпису в

класичному розумінні, оскільки вони є мультимедійними файлами, а не документами у правовому сенсі.

По друге, якщо судова практика буде сприймати відео- та звукозаписи як електронні документи, це може привести до правових колізій. Наприклад, суд може вимагати підтвердження їхньої достовірності за тими ж критеріями, що і для електронних документів, хоча методи перевірки автентичності для цих доказів суттєво відрізняються. Дане питання буде більш детально нами досліджено в третьому розділі.

По третє, на нашу думку, у класифікації електронних доказів необхідно розділяти електронні документи та інші види електронних доказів (наприклад, мультимедійні файли, програмні файли, метадані тощо).

Враховуючи, що розвиток цифрових технологій постійно створює нові види електронних доказів, на нашу думку, не є доцільним закріплення чіткого їх поділу в нормативних актах. Натомість краще в кримінальному процесуальному законодавстві використовувати широке визначення електронних доказів, яке буде охоплювати будь-яку інформацію в електронному виді, яка може мати доказове значення, тобто акцентуватися на змісті доказу, а не його формі. Такий гнучкий підхід у правовому регулюванні дозволить враховувати появу нових видів електронних доказів в зв’язку з розвитком технологій.

У подальшому ми детальніше зосередимося на дослідженні електронних доказів, враховуючи критерії поділу за формою існування. Зокрема, розглянемо окремі їх види, такі як електронні документи та мультимедійні електронні докази, оскільки саме ці категорії дозволять найкраще пояснити їхні відмінності та особливості, щоб забезпечить практичну цінність уніфікації термінології що стосується електронних доказів. А в наступному розділі нашого дослідження, присвяченому проблемним аспектам застосування електронних доказів у судовій практиці, ми, використовуючи сформовану класифікацію електронних доказів за критеріями способу формування та технічним середовищем існуванням,

обґрунтуємо ключові підходи до оцінки їх належності, допустимості та достовірності.

2.2. Електронний документ як різновид електронного доказу та його співвідношення з іншими видами доказів

В попередньому розділі нашого дисертаційного дослідження констатовано, що у науці відсутнє єдине розуміння місця електронних доказів в системі процесуальних джерел доказів: висловлюються аргументи як на користь віднесення їх до традиційних (речові докази, документи), так і на користь виділення окремої групи (електронні докази). А відповідно відсутність єдиного розуміння місця електронних доказів в системі процесуальних джерел доказів у науці впливає на судову практику. Як правило, судова практика часто ототожнює електронний доказ з електронним документом або кваліфікує його як речовий доказ.

Однак, такий підхід, на нашу думку, є неточним і не відображає справжньої природи електронних доказів. Досліджуючи правову природу електронного документа, ми проаналізуємо його особливості та продемонструємо його відмінності від інших видів електронних доказів, в тому числі текстових електронних доказів, як то повідомлення електронної пошти, листування в месенджерах, документів в електронному вигляді тощо). Це дозволить чітко окреслити межі поняття електронного документа, визначити його роль у доказовому процесі та відмежувати від більш ширшої категорії електронні докази.

Ми поділяємо думку А.-М. Ангеленюк, яку вона висвітлила у статті «Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання)», що поняття речового доказу, електронного документа та електронного доказу не тотожні [4, с. 216]. Ця думка є надзвичайно важливою для розуміння теми нашого дослідження і потребує подальшого розвитку.

У свою чергу, науковці І. В. Басиста, Л. В. Гаврилюк, А. В. Гутник, А. Я. Хитра наголошують на некоректності ототожнення електронного документа

та електронного доказу у національній судовій практиці. Саме відсутність у чинному КПК України такого різновиду доказів, як «електронні» чи «цифрові» зумовлює проблему із різним слововжитком серед науковців та практиків [11 , с.237].

Досліджуючи питання використання електронних документів як доказів у кримінальному провадженні, необхідно проаналізувати дане поняття, адже у кримінальній процесуальній науці не існує єдиного визначення поняття електронного документа і так само законодавчо не закріплене дане поняття у КПК України. Ототожнення електронного документа з електронними доказами призводить до термінологічної невизначеності у судовій практиці. У результаті суди використовують різні терміни для позначення доказової інформації в електронному вигляді, що ускладнює формування єдиної судової практики та створює ризики неоднакового застосування норм процесуального законодавства. Зокрема, у судових рішеннях можна зустріти терміни «електронні докази», «електронний документ» «комп'ютерні дані» «цифрова інформація», «файл», що фактично можуть означати одні й ті самі або схожі за правовою природою явища Це стає особливо проблемним при оцінці електронних доказів з точки зору належності, допустимості, достовірності.

До речі, за нашим дослідженням у рішеннях судів використовується різний терміновжиток для позначення доказової інформації в електронному вигляді, що досить яскраво продемонстровано у постанові ККС ВС від 06.02.2024 № 645/6247/16-к[22] [до примітки див. 194].

---

[22] «**технічний носій інформації**, на якому зафіксовано проведення слідчого експерименту…. не обґрунтовано **визнано судом першої інстанції недопустимим доказом»;** « **електронними доказами є інформація в електронній (цифровій) форм**і; «**допустимість електронного документа як доказу»**; «**технічний носій інформації** на якому зафіксовано проведення слідчого експерименту …… за своєю природою **є самостійним джерелом доказів, визначеним ст. 84 КПК України»;** «колегія суддів **оцінює інформацію, яка міститься на технічному носії інформації в електронній (цифровій) формі**, який містить дані про обставини, що мають значення для справи, як **самостійний електронний документ»;** «наданий **технічний носій інформації** на якому зафіксовано проведення цієї слідчої дії, за обставин цього кримінального провадження, **є електронним доказом** на якому міститься інформація в електронній (цифровій) формі».

Судді ККС ВС, приймаючи участь у обговоренні проблемних питань щодо допустимості електронних доказів під час судового розгляду [271] та під час участі в дискусії, присвяченій питанню щодо допустимості електронних доказів, отриманих із відкритих джерел, у межах національних кримінальних проваджень стосовно грубих порушень прав людини внаслідок російської агресії проти України [270] використовують як терміни «електронні докази», так і «цифрові докази».

Суддя ККС ВС Наталія Марчук під час презентації курсу «Кіберзлочинність і електронні докази» у межах проєкту Ради Європи «HELP (Освіта в галузі прав людини для юристів) для України, в тому числі під час війни» зазначила, що електронні докази належать до категорії документів, а матеріальні носії, на яких вони розміщені, визнаються речовими доказами [92; 273]. На нашу думку це хибне розмежування, адже відповідно до ст.84 КПК України доказ — це єдність фактичних даних та джерела їх отримання. Інформація є змістовною складовою доказу, тоді як носій, на якому ця інформація зберігається, є матеріальною частиною доказу. Тільки разом вони утворюють повноцінний доказ, оскільки носій несе в собі не тільки фізичний аспект, а й важливу роль у збереженні та передачі інформації.

З огляду на відсутність єдиного визначення поняття електронного доказу та електронного документа в кримінальній процесуальній науці та термінологічну невизначеність у судовій практиці, доцільним є звернення до історичних аспектів становлення цього поняття. Варто зазначити, що питання можливість використання електронних документів як доказів розглядалося нами у першому розділі дисертаційного дослідження та акцентувалося, що можливість використання електронних документів в якості доказів у кримінальному судочинстві вперше розглянув В. К. Лисиченко ще в 1974 році [121, с. 51]. Одним із перших нормативно-правових актів, які давали визначення поняття електронного документу, були інструктивні вказівки Держарбітражу СРСР від 29.06.1979 р. «Про використання в якості доказів з арбітражних справ документів, підготовлених за

допомогою електронно-обчислювальної техніки», в яких до електронних документів відносили всі документи, при підготовці яких використовувалася електронно-обчислювальна техніка [139].

Великий енциклопедичний юридичний словник містить визначення поняття електронного документа як матеріального носія відповідної інформації, зафіксованої у вигляді електронних даних, включаючи обов'язкові реквізити документа, без яких він не може бути підставою для його обліку і не матиме юридичної сили [25, с. 247]. Велика українська енциклопедія визначає електронний документ як документ, інформація в якому подана у формі електронних даних [23, с. 48].

Слід зазначити думку науковців щодо поняття «документа» у кримінальному процесі: документ завжди є матеріальним об'єктом; документ містить інформацію щодо факту або обставин, що встановлюються під час кримінального провадження; відомості, що містяться в документі, фіксуються за допомогою письмових знаків, звуку, зображення тощо з метою збереження інформації, а зміст документа має засвідчувальний або описовий характер; документ має бути одержаний та приєднаний до матеріалів кримінального провадження в установленому порядку [112, с. 379]. Повністю погоджуємося з даним твердженням і спробуємо його поширити на визначення поняття електронного документа.

Ю. Палеха та Н. Леміш, аналізуючи документ як процесуальне джерело доказів, стверджували, що документ включає в себе матеріальну та інформаційну складову. На їх думку матеріальна складова документа може бути виражена також у вигляді електронного середовища, забезпечує здатність зберігати й передавати інформацію в просторі й часі. Матеріальна складова документа визначає носій інформації – матеріальний об'єкт, створений природою або ж штучно людиною, за допомогою якого можна зберігати й передавати інформацію. Інформаційна складова документа містить відомості, що є важливими для кримінального провадження [147, с. 138–140].

Отже, звідси можна вести мову про двоїстість електронного документа, який у сукупності складається з інформації та матеріального носія, на якому ця інформація створюється, зберігається, відтворюється з інформації.

В той же час у міжнародному документі Комісії ООН з права міжнародної торгівлі також мається дещо інше визначення поняття електронного документа. В даному нормативному акті електронний документ визначений як інформація, утворена, надіслана, отримана або збережена електронними, оптичними чи подібними засобами, включаючи електронний обмін даними, електронну пошту, телеграми чи телекопіювання [420]. Тобто, у міжнародному праві електронний документ визначається через категорію «інформація».

Аналогічну позицію займають і науковці, досліджуючи дану правову категорію. Так, Є. С. Хижняк визначає електронний документ як інформацію, представлену в електронній формі, що має значення для розслідування кримінальних правопорушень, дослідження якої здійснюється за допомогою спеціальних програмно-технічних засобів [350, с. 81].

В. В. Мурадов, даючи визначення поняття електронний документ, зазначає, що електронний документ — це документ, інформація у якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Реквізити електронного документа мають розміщуватися відповідно до чинних нормативних документів та стандартів [134, с. 51].

В дисертаційному дослідженні «Докази і доказування у адміністративно-деліктному процесі»(2015) І. В. Казанчук дає визначення електронного документу як самостійного джерела доказів інформація в якому представлена у формі електронних даних, включаючи відповідні реквізити документа, в тому числі і електронний цифровий підпис та інші, який може бути сформований, переданий, збережений і перетворений електронними засобами у візуальну форму, автентичність якого може бути підтверджена електронним цифровим підписом та іншими незмінними сертифікованими засобами [82, с. 6, 17].

Відтак, виходячи з легального визначення поняття електронного документа можна зробити висновок про двоїстість його сутності. По перше, електронний документ містить в собі інформацію; по-друге, електронний документ має обов'язкові реквізити документа без яких він не матиме юридичної сили. Як ми вже зазначали обов'язковими реквізитами електронного документа є електронний підпис автора або підпис, прирівняний до власноручного підпису відповідно до ЗУ «Про електронну ідентифікацію та електронні довірчі послуги» (ст. 7 Закону України «Про електронні документи та електронний документообіг); по-третє, інформація в такому документі представлена у вигляді електронних даних; по-четверте, саме такий спосіб створення, передання, збереження інформації дає змогу перетворити цю інформацію за допомогою електронних засобів у форму, придатну для сприйняття її змісту людиною; по п'яте, електронний документ зберігається на матеріальних носіях або відображається в електронному вигляді.

Таким чином, електронний документ складається як з самої інформації, так і з матеріального носія, тобто пристроїв, на яких ця інформація була створена, збережена і за допомогою яких може бути відтворена.

Так, наприклад, електронний документ кардинально відрізняється від традиційного документу не тільки за формою відображення інформації, але й за самою сутністю. «Цілком очевидно, що якщо відірвати частину аркушу паперу – документ не загубить свого доказового значення, проте, втрата частини файлу цифрового (електронного) документу, призведе до його повного знищення» [126, с. 91].

Зокрема, Л. П. Піддубна, яка досліджувала правову природу документів, в своїй науковій праці відмітила, що в Україні офіційно прийняті три визначення документа, що зафіксовані у окремих державних стандартах (ДСТУ) [153].

Відповідно до п. 4.2.3 ДСТУ 2392-94, Документ – це записана інформація, яка може розглядатися як одиниця в ході здійснення інформаційної діяльності. Це визначення стосувалося не тільки паперових та друкованих матеріалів, а й машинозчитуваних записів [69, с. 12]. Натомість, ДСТУ 3017-95 визначає

документ як матеріальний об’єкт з інформацією, закріпленою створеним людиною засобом для її передачі у часі та просторі [70, с. 2].

Наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» 25.05.2023 р. № 121 на заміну стандарту ДСТУ 2732:2004 з 01.03.2024 р. вводиться стандарт ДСТУ 2732:2023. В цьому стандарті вказано про відсутність термінів, що належать до інших галузей знань, зокрема інформатики (наприклад, поняття процесів електронного документування та електронного документообігу) [70; 232].

Отже, ми можемо бачити, що ці дефініції не в повній мірі розкривають правову природу електронного документа і тому нас більше цікавить термінологія, яка стосується безпосередньо електронного документа, зокрема, яка міститься в Законі Україні «Про інформацію». Так, відповідно до ст. 1 цього Закону документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі. В свою чергу, інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [230].

Український законодавець визначив електронний документ як документ, інформація в якому зафіксована у вигляді електронних даних, включаючи *обов’язкові реквізити документа* (курсив наш - І. Смаль). Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною [223].

На підставі вищезазначеного можна стверджувати, що без обов’язкових реквізитів електронний документ не буде документом, тобто він не матиме юридичної сили. Більш того, створення електронного документа завершується накладанням електронного підпису та/або електронної печатки (ч. 3 ст. 6 Закону «Про електронні документи та електронний документообіг») і відповідно слідує логічний висновок, що оригіналом електронного документа вважається

електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до ЗУ «Про електронну ідентифікацію та електронні довірчі послуги» (ч. 1 ст. 7) [223].

ЗУ «Про електронну ідентифікацію та електронні довірчі послуги» визначає, що електронний підпис—це електронні дані, що додаються до інших електронних даних або логічно з ними пов'язується і використовується підписувачем як підпис [225]. Кваліфікований електронний підпис – це єдиний вид підпису, який відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису (ч. 6 ст. 18) [225].

Якщо мова йде про процесуальні електронні документи, які складають слідчий, або прокурор за результатами процесуальної діяльності під час досудового розслідування за результатами процесуальної діяльності, то ч.4 ст.106-1 КПК України встановлені спеціальні вимоги до їх допустимості.

Так, ч. 4 ст. 106-1 КПК України визначає, що документи, підписані, погоджені в інформаційно-комунікаційній системі досудового розслідування з використанням кваліфікованого електронного підпису, їх примірники в електронній та паперовій формах визнаються оригіналами документів.

Таким чином, ми бачимо, що законодавець у цьому випадку визначає обов'язкову умову — кваліфікований електронний підпис.

04 лютого 2019 року ВП ВС, переглядаючи справу адміністративну справу № 9901/43/19, ухвалила, що саме електронний цифровий підпис є головним реквізитом такої форми подання електронного документа. Відсутність такого реквізиту в електронному документі виключає підстави вважати його оригінальним, а отже, належним доказом у справі [286]. І тільки 23.01.2025 року ККС ВС у справі № 638/6886/22 зробив висновок та привів таку аргументацію,[23]

[23] «у кримінальному провадженні суд оцінює докази за правилами, визначеними кримінальним процесуальним законом, а саме в контексті реалізації приписів статей 84-86, 93, 94, 99 КПК, де відображені відповідні критерії

[до примітки див. 205], яка на нашу думку, свідчить про зміни в судовій практиці, а саме розуміння різниці між електронними доказами та електронними документами, усвідомлення, що це не тотожні поняття. Це вказує на еволюцію підходів до тлумачення та оцінки інформації в електронному вигляді, що в свою чергу буде впливати на формування єдиної правозастосовної практики. Адже поки не закріпленні в кримінальному процесуальному законодавстві електронні докази як окреме процесуальне джерело, судова практика розглядає їх як документ.

Постанова Об'єднаної палати ККС ВС від 29.03.2021, справа № 554/5090/16-к містить таку правову позицію, яка сформована з посиланням на положення ЗУ «Про електронні документи та електронний документообіг», що допустимість електронного документа як доказу не можна заперечувати виняткова на підставі того, що він має електронну форму та у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той же електронний документ може існувати на різних носіях» [206]. Однак, якщо подивитися на положення ЗУ «Про електронні документи та електронний документообіг», то оригіналом електронного документа вважається *електронний примірник документа з обов'язковими реквізитами* (курсив наш - І. Смаль), у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до ЗУ "Про електронну ідентифікацію та електронні довірчі послуги", тому використанням копії інформації в електронному вигляді, на наш погляд, потребує додаткової аргументації, при цьому хочемо підкреслити, що нами не заперечується можливість зберігання такої інформації на різних носіях, адже це випливає з ознак електронних доказів.

оцінки доказів на предмет їх допустимості, в тому числі й електронних документів. Вказані правила відмінні від тих, про які йдеться в Господарському процесуальному кодексі України (ч. 2 ст. 96) та Цивільному процесуальному кодексі України (ч. 2 ст. 100), за вимогами яких на електронний документ накладається кваліфікований електронний підпис відповідно до положень законів «Про електронні документи та електронний документообіг» та «Про електронну ідентифікацію та електронні довірчі послуги», без чого він не вважається допустимим доказом стосовно встановлення певних фактів».

Аналогічна аргументація використовується і в постанові ККС ВС від 15.08.2024 справа № 203/94/18,991/2/23 [199].

Таким чином, ми можемо бачити усталену практику ВС щодо допустимості використання копій «електронних документів», спираючись на положення ЗУ «Про електронні документи та електронний документообіг».

Ще на початку нашого наукового пошуку, ми обґрунтовували думку, що використання законодавчо закріпленого в ЗУ «Про електронні документи та електронний документообіг» поняття електронного документа неможливе для визначення поняття електронних доказів у кримінальному процесі. Адже, електронний документ є одним із видів електронних доказів, а відповідно їм може бути притаманна наявність певних реквізитів, однак вона не є обов'язковою. Натомість відсутність таких реквізитів не може вплинути на доказове значення такого електронного доказу як доказу у кримінальному провадженні [141, с. 124] Зважаючи на вказане, очевидною є потреба приділити в рамках нашого дослідження окрему увагу обґрунтуванню необхідності внесення змін у КПК України, тому що така не узгодженість впливає на судову практику, що буде в подальшому нами продемонстровано.

Продовжуючи висвітлення окресленої проблематики зупинимося також на аналізі окремих правових приписів у цьому напрямку. У відповідних нормативних положеннях процесуальних кодексів з інших галузей права, зокрема ЦПК, ГПК та КАС України, Законом від 03.10.2017 р. «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» закріплено норми, якими законодавець визначає електронні документи як один із видів електронних доказів [213]. Як ми бачимо законодавець використовує уніфікований підхід до розуміння «електронного доказу» та визначає його через категорію інформації в електронній (цифровій) формі [59; 99; 355].

В кримінальному процесуальному законодавстві нормативне підґрунтя використання електронного документу як доказу визначається ст. 99 КПК України,

яка говорить, що процесуальним джерелом доказів є оригінал документу. Оригіналом електронного документа є його відображення.

Отже, законодавець електронний документ відносить до документів і визначає його як спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження (ч. 1 ст. 99 КПК України) [113].

Необхідно відмітити, що законодавець, розуміючи специфічну природу інформації в електронному вигляді, намагався надати нормативне закріплення використання її як доказу у кримінальному процесі, про що свідчать відповідні законопроєкти, які були на розгляді ВР, а також якими були внесені відповідні зміни до КПК.

Звернемося до проєкту закону № 9484 від 17.01.2019 р. «Про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінальних проваджень) [218], який був знятий з розгляду, але його положення мають для нас наукову цінність. Незважаючи на те, що у пояснювальній записці зазначалося, що законопроєктом передбачається внесення змін, спрямованих на уточнення спеціальної термінології галузі інформаційних технологій, вдосконалення змісту поняття «речовий доказ» з урахуванням сучасного стану розвитку інформаційних технологій та вдосконалення положень, які регулюють тимчасовий доступ до пристроїв для обробки, передавання та зберігання електронної інформації, у тексті відсутнє визначення поняття електронного доказу або інформації в електронному вигляді.

Натомість даним законопроєктом пропонувалося електронну інформацію віднести до речових доказів[24] [до примітки див. 218]. Попри позитивне прагнення

[24] Так, ст. 98 КПК України пропонували доповнити новими частинами та викласти в такій редакції: «Інформація в електронному вигляді (електронна інформація) може бути визнана речовим доказом, якщо вона є знаряддям,

вирішити законодавчі прогалини, на наш погляд, даний підхід не досить є обґрунтованим з наукової точки зору та викликатиме труднощі у практичному застосуванні його положень. Нами в розділі І досліджено різні підходи науковців до визначення місця електронних доказів у системі процесуальних джерел і підтримана позиція щодо створення оновленої вітчизняної моделі доказування, яка відповідала б сучасному рівню розвитку досягнень науки та техніки та дозволила адаптувати доказову діяльність у кримінальному провадженні до будь-яких майбутніх інноваційних досягнень. Отже, більш вдалим буде підхід спрямований на віднесення електронних доказів до самостійного процесуального джерела.

Також хочеться відмітити пропозиції авторів законопроєкту включити до статті 3 КПК України поняття «пристрої для обробки, передавання та зберігання інформації в електронному вигляді (електронної інформації) або їх складові»[25] [до примітки див. 218].

У даному контексті слід зауважити, що не варто надто деталізувати в кодифікованому законодавчому акті з питань кримінального судочинства терміни, які не є специфічними кримінальними процесуальними поняттями і крім того, слід відмітити, що пристрої для обробки, передавання та зберігання інформації в електронному вигляді (електронної інформації) будуть постійно змінюватися і в

засобом або предметом кримінального правопорушення, чи може бути використана як доказ факту чи обставин, що встановлюються під час кримінального провадження. При цьому пристрої для обробки, передавання та зберігання електронної інформації або їх складові як носії електронної інформації речовими доказами не визнаються. Пристрій для обробки, передавання та зберігання електронної інформації або його складова (складові) може бути визнаний речовим доказом лише у разі, якщо він сам є знаряддям, засобом або предметом кримінального правопорушення, окрім випадків, коли такою ознакою складу кримінального правопорушення виступає інформація, що в ньому міститься, а також у випадку, коли електронна інформація як речовий доказ не може бути копійована без пошкодження чи знищення цього пристрою».

[25] визначивши його як технічні пристрої, призначені для зберігання, обробки та передавання інформації в електронному вигляді за допомогою апаратних і програмних засобів. При цьому зазначається, що цим поняттям, зокрема, охоплюються: інформаційні (автоматизовані, телекомунікаційні, інформаційно-телекомунікаційні) системи; комп'ютери (суперкомп'ютери, мейнфрейми, кластери, сервери, робочі станції, персональні комп'ютери, ноутбуки тощо); комп'ютерна периферія (зокрема, термінали, принтери, сканери, плотери, джерела безперебійного живлення); мобільні термінали систем зв'язку (мобільні телефони, смартфони, планшети та інше); апаратна складова телекомунікаційних та інших комп'ютерних мереж і мережеве обладнання (маршрутизатори, концентратори, комутатори, модеми, мережеві контролери, кабелі тощо); мікропроцесорні системи (наприклад, мікроконтролери та програмовані логічні контролери), а також банкомати й інші стаціонарні платіжні термінали для обслуговування населення.

орбіту кримінального процесу будуть потрапляти все нові і нові пристрої, які будуть містити інформацію в електронному вигляді.

Так, в ISO/IEC 27037:2012, який містить настанови щодо ідентифікації, збору, придбання та збереження цифрових доказів, визначені такі пристрої:[26] [до примітки див. 403]. І при цьому зазначено, що цей список пристроїв є орієнтовним і не є вичерпним.

15.01.2020 року за № 2740 був внесений аналогічний проєкт Закону про внесення змін до КПК та КК України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження).

В ньому, як і в законопроєкті № 9484, інформація в електронному вигляді була віднесена до речових доказів. Крім того, необхідно відмітити намагання авторів проєкту внести ясність у визначення поняття електронний документ шляхом внесення змін до ст.99 КПК. Так, пропонувалося пункт 1 частини другої статті 99 викласти у такій редакції: «1) матеріали фотозйомки, звукозапису, відеозапису та у будь-якій іншій формі зафіксована на матеріальному носії візуальна або аудіальна інформація (у тому числі електронна), а так само електронні документи відповідно до Закону України «Про електронні документи та електронний документообіг»» [217].

Також, як позитивний момент, хочемо відзначити намагання авторів законопроєкту пояснити існування «загадкової» термінології в діючому КПК «відображення електронного документа». Так, пропонувалося частину третю статті 99 викласти у такій редакції: «Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов’язані надати суду оригінал документа. Оригіналом документа є сам

[26] цифрові носії інформації, що використовуються в стандартних комп’ютерах, як-от жорсткі диски, дискети, оптичні та магнітооптичні диски, пристрої даних із подібними функціями; мобільні телефони, персональні цифрові помічники (PDA), персональні електронні пристрої (PED), карти пам’яті; мобільні навігаційні системи; цифрові фото- та відеокамери (включаючи відеоспостереження); стандартний комп'ютер з підключенням до мережі; мережі на основі TCP/IP та інших цифрових протоколів; пристрої з аналогічними функціями, як описано вище.

документ, а оригіналом електронного документа – його електронний примірник відповідно до Закону України «Про електронні документи та електронний документообіг», а також візуальне відображення електронного документа на папері, яке засвідчене в порядку, встановленому законодавством» [217]. Однак, внесення таких змін не вирішувало питання застосування термінології «оригінал», «дублікат», «копія» до інформації в електронному вигляді, актуальність якого розглянемо у наступному підрозділі.

У зв'язку з цим слід констатувати, що недостатнє усвідомлення законодавцем специфіки природи електронних доказів, а також спроби вирішувати проблемні питання їх використання у кримінальному процесі шляхом ситуативного внесення змін та доповнень до кримінального процесуального законодавства, без системного підходу, лише ускладнюють правозастосування. Такий підхід істотно обмежує можливості повноцінного використання інформації в електронному вигляді як доказу у кримінальних провадженнях.

Однією із спроб законодавчо врегулювати використання електронних доказів у кримінальному провадженні був проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» № 4004 від 01.09.2020 р.[27] [до примітки див. 218]. Так, даним проєктом яким було запропоновано доповнити главу 4 «Докази і доказування» параграфом «Електронні докази». Відповідно до пропонованих змін:[28] [до примітки див. 218].

---

[27] у пояснювальній записці до якого вказано два аргументи з приводу необхідності ухвалення відповідного закону: 1) поширеність подання сторонами електронних доказів у кримінальних провадженнях (такий висновок був зроблений з огляду на дані, отримані Верховним Судом після дослідження практики судів першої, апеляційної та касаційної інстанцій); 2) визначення порядку використання електронних доказів у нормативних актах, які регламентують порядок здійснення цивільного, господарського та адміністративного судочинства.

[28] «Електронним доказом є інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. Також законодавець по аналогії до ЦПК, КАС, ГПК визначав перелік електронних доказів «1) електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо); 2) віртуальні активи; 3) веб-сайти, веб-сторінки; 4) текстові, мультимедійні та голосові повідомлення; 5) метадані; 6) бази даних; 7) інша інформація в електронній (цифровій) формі».

А. В. Скрипник, аналізуючи даний законопроєкт, відмітив, що в ч. 1 ст. 100-1 КПК законопроєкту мова йде «про *файли* або *групи файлів,* а вони є вже *носіями інформації.* Якщо законодавець прагне врегулювати процесуальну обробку носіїв, то зміни потребує не лише визначення електронних доказів, але і сама назва – у такому разі вони будуть не доказами, а джерелами доказової інформації» [250, с. 99].

В свою чергу хочемо зазначити, незважаючи на обґрунтованість критики науковців та практиків, які були висловлені в адресу даного законопроєкту, його безсумнівну прогресивність в частині появи нового процесуального джерела – електронні докази.

А.-М.Ю. Ангеленюк також підтримує ідею необхідності визначення в КПК України переліку джерел отримання електронних доказів у кримінальному провадженні, до яких пропонує віднести: «1) цифрові документи або інші електронні докази надані офіційними установами або щодо яких надано доступ до інформації, яка зберігається на сервері; 2) записи автономних систем (камери відео спостереження, реєстратори, інші програмні забезпечення, застосунки, які встановлені на мобільних телефонах, планшетах чи інших електронних пристроях); 3) електронні докази отримані в результаті проведення слідчих (розшукових) дій або негласних слідчих (розшукових) дій; 4) електронні докази отримані в результаті проведення заходів забезпечення або запобіжних заходів; 5) електронні докази отримані в результаті зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису (стаття 245-1 КПК); 6) електронні докази отримані в результаті тимчасового вилучення майна (стаття 168 КПК)» [4, с. 216].

Не заперечуючи прогресивність ідей автора, хочемо зауважити, що ідея класифікації джерел отримання доказової інформації є досить цікавою з наукового погляду, однак, на нашу думку не матиме практичної реалізації. На нашу думку, запропонована класифікація джерел отримання електронних доказів виглядає хаотично, оскільки в ній не прослідкуються єдині критерії поділу. По перше,

змішуються різні підходи. Так, в першому пункті критерієм є суб'єкт, що надає доказ, в другому — конкретне джерело даних, в третьому — спосіб отримання доказів (в результаті слідчих (розшукових) дій або негласних слідчих (розшукових) дій), в четвертому та шостому пункті мова йде про докази отриманні в результаті заходів забезпечення, п'ятому — мова також йде про слідчу дію, в результаті якої отримуються електронні докази. По друге, відсутність логічної структури не дозволяє чітко визначити джерело та правові особливості доказу.

А. В. Ратнова також пропонує внести зміни в КПК України та викласти ч. 2 ст. 99-1 КПК в наступного змісту: до електронних документів можуть належати: текстові документи, фотографії та інші зображення, аудіо- та відео- записи, електронні повідомлення (смс-повідомлення, електронна пошта, голосові повідомлення), кеш-файли, соокіе-файли, вебсайти, дані геолокації та інші відомості в електронній формі [238, с. 71].

Запропоновані автором зміни до кримінального процесуального законодавства, які передбачають віднесення до електронних документів текстових документів, фотографій, аудіо- та відео- записів, електронних повідомлень, кеш-файлів, вебсайтів, даних геолокації та інших відомостей в електронній формі не враховують фундаментальну особливість електронного документа—наявність обов'язкових реквізитів. Ми високо оцінюємо ініціативу авторки щодо удосконалення законодавства, проте вважаємо запропонований підхід не достатньо коректним, оскільки така кваліфікація в КПК України фактично розмиває відмінності між електронними документами та іншими видами електронних доказів. Включення такої норми до законодавства суперечить самій суті електронного документа та створюватиме правову невизначеність.

На нашу думку, кримінальне процесуальне законодавство потребує чіткого розмежування джерел доказів та поділу на «письмові докази» та «електронні докази», що допоможе врахувати особливості їхньої форми існування, оскільки правозастосовна практика вимушена пристосовувати чинний КПК України до потреб сучасності, а «електронні докази» у кримінальних провадженнях

визнаються речовими доказами або документами, що не завжди відповідає правовій природі останніх. Отже, очевидною постає необхідність вдосконалення правового визначення поняття доказів у кримінальному провадженні із урахуванням специфіки інформації в електронному вигляді, а також підтверджує тезу про необхідність виділення електронних доказів як окремого процесуального джерела доказів.

Нами запропоновано внесення змін до КПК України, зокрема в статтю 99, виклавши її в наступній редакції:

Стаття 99. Письмові докази

1. Письмовими доказами є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить текстову, графічну або змішану інформацію, зафіксовану за допомогою письмових знаків, зображення тощо відомості, які можуть бути використані як доказ обставин, що підлягають доказуванню у кримінальному провадженні.

Проведений нами детальний аналіз електронного документа: його властивостей, законодавчого визначення, використання як доказу у судовій практиці та критерії оцінки достовірності дає нами підстави стверджувати, що ключові характеристики електронного доказу — наявність обов'язкових реквізитів, в тому числі електронного підпису не притаманне іншим видам електронних доказів, як то мультимедійні файли, текстові документи чи метадані, які мають іншу природу. Це розмежування є важливим для правильної правової оцінки будь-якої інформації в електронному вигляді у судовій практиці.

Так, аудіо- та відеофайли є одним із найбільш давніх та традиційних видів доказів, що використовувалися у кримінальному процесі. Ще до цифрової епохи звукозаписи на магнітних носіях та кіноплівка застосовувалися для фіксації інформації. Із розвитком технологій, аналогові носії поступилися місцем цифровим форматам, що значно розширилося можливості використання в якості доказів. Аудіо- та відеозаписи, на відміну від письмових, речових доказів, мають звукову та візуальну виразність. Вони дають змогу суду безпосередньо сприймати події у

динаміці, відтворюючи обставини минулого. Саме ця особливість робить інформацію, зафіксовану у звукових та відеоматеріалах, особливо переконливою під час дослідження в якості доказів у судовому засіданні. Однак саме через таку вагомість ці докази потребують ретельної перевірки на достовірність.

Поглянемо на норми п.1 ч.2 ст.99 КПК України, яка визначає, що матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані) відносяться до документів. Ця норма, на нашу думку, демонструє певну нечіткість у співвідношенні понять. Так, звукозапис, відеозапис — це не носій інформації, це сама інформація. Відеозапис, так само як і звукозапис чи фото, є інформацією, яка зафіксована в певній формі, а носієм такої інформації є фізичний об'єкт (диск, флешка, карта пам'яті), на якому збережений цей відеозапис. Отже ця норма змішує поняття: відеозапис, звукозапис, фото як інформаційний зміст та носій інформації як фізичний об'єкт. Таким чином, у поточній редакції ст. 99 КПК України спостерігається концептуальна помилка, і для її виправлення слід розмежувати документи, що містять інформацію та носії інформації. Крім того, якщо подивитися на використання терміну «матеріали» перед переліком «фотозйомки, звукозапису, відеозапису», то про що це говорить? Не про сам запис, а й пов'язані з ним метадані, характеристики? Це не зовсім логічно виглядає. Більш логічно і зрозуміло це виглядає, якщо під «матеріалами» розуміти саме фото, аудіозапис, відеозапис та фізичні носії на яких вони зберігаються.

Отже, на наш погляд, ця норма позбавлена правової визначеності і нами запропоновані зміни до ст. 99 КПК (див. додаток Г).

І в цьому аспекті, варто відмітити, що файл, на нашу думку, не є носієм інформації у традиційному розумінні, а є формою збереження інформації у електронному вигляді. Файл — це структурована одиниця комп'ютерних даних, яка існує у вигляді певного формату (текстовий документ, відео, зображення, база даних тощо). Він не є носієм сам по собі, а лише об'єктом, що міститься на носії інформації. А в свою чергу, комп'ютері дані — це зміст файлу, тобто інформація,

що міститься всередині. Чому це так важливо? Фізичний носій (наприклад, карта пам’яті) може містити сотні файлів, але сам по собі він не інформацією — він лише засіб для її зберігання. Отже, файл — це лише контейнер даних (наприклад, .txt, .jpg, .mp4), який потребує пристрою для зчитування. Ці поняття необхідно розрізняти в юридичному контексті, щоб уникнути плутанини і використовувати термінологію відповідно до її семантичного значення. Комп’ютерних дані (термін використовується відповідно до законодавчо закріпленого в ст. 99 КПК України), то як ми вже зазначали, не є носіями інформації і тим паче матеріальним об’єктом. Комп’ютерні дані можуть виступати електронними доказами у кримінальному провадженні, якщо містять інформацію, яка має значення для справи.

Що стосується метаданих як окремого виду електронних доказів, то вони відіграють ключову роль у правовій оцінці електронних доказів, оскільки містять технічну інформацію про файли та електронні документи: дата, часові позначки, авторство, місце зберігання, історію змін, дані про місцезнаходження, IP адреси та ідентифікатори пристроїв тощо. Розмежовуючи метадані як окремий вид електронних доказів необхідно підкреслити їхню допоміжну функцію у підтвердженні достовірності інших цифрових даних. Фактично метадані можуть посилювати доказову силу інших видів електронних доказів, зокрема електронних документів (дату підписання, авторство, факт внесення змін), мультимедійних файлів (фото, відео, аудіо) — вказуючи на дату й час зйомки, місцезнаходження або пристрій, за допомогою якого створено файл, текстових електронних доказів (повідомлення в месенджерах, соціальних мережах, електронні листи, публікації на вебсайтах, текстові файли у форматах WORD, PDF, TXT, повідомлення в банківських та інших сервісних додатках) — час та дата надсилання або отримання повідомлення може підтвердити хронологію подій; IP адреса або пристрій, з якого надіслано допомагає встановити місцезнаходження або особу користувача тощо.

А. В. Коваленко в своєму монографічному дослідженні «Криміналістичні вчення про збирання, дослідження та використання доказів у кримінальному провадженні» (2024) зазначає, що комп’ютерні дані зберігаються в зашифрованій

формі, призначеній для обробки обчислювальними пристроями комп'ютерної техніки. Вони є нематеріальним об'єктом і можуть досліджуватися тільки після перетворення в аудіовізуальну форму [95 с. 309].

На прикладі, судового рішення ККС ВС від 15.08.2024 р. № 203/94/18,991/2/23 можна бачити, що метадані досліджуються судом та їм надається оцінка як доказам [29] [до примітки див. 200].

В наступному розділі дослідження розглянемо проблеми оцінки належності, достовірності текстових електронних доказів, мультимедійних доказів, а також виклики, які пов'язані з їх використанням. Окрему увагу буде приділено метаданим як самостійному виду електронних доказів, а також як елементу, що підсилює достовірність інших електронних доказів.

2.3. Інтернет як джерело доказової інформації

Теорія передачі інформації між комп'ютерами з'явилася у 1961 році, а починаючи з 80-років минулого століття Інтернет поступово став тим, що зараз називають «всесвітньою мережею» [369].

Відповідно до звіту «Digital 2023: Global Overview Report» («Цифровий 2023: Глобальний оглядовий звіт»), який проведений за участі «DataReportal» спільно з компаніями «Meltwater» і «We Are Social»,[30] [до примітки див. 91].

Що стосується України, то на початок 2023 року в Україні було 28,57 мільйона користувачів Інтернету, тоді рівень проникнення становив 79,2 %. У січні

---

[29] Метадані не є достовірним джерелом інформації про історію маніпуляцій з файлом, оскільки такі можуть змінюватися незалежно від його вмісту. Сторона, що ставить питання про підробку файлів, має навести аргументовані відомості про ознаки фальсифікації записів, спотворення їх змісту чи невідповідність фактичним обставинам. Такі твердження щодо можливого здійснення технічного втручання і редагування записів, порушення їх цілісності, мають спиратися на об'єктивні дані безсумнівного сприйняття таких фактів органами слуху та зору, або переконливо підтверджуватися іншими доказами у справі, або обґрунтовуватися відповідними технічними висновками спеціалістів на засадах змагальності в кримінальному процесі.

[30] кількість осіб, які користуються Інтернетом, соціальними мережами невпинно зростає. Населення світу перевищило 8 мільярдів 15 листопада 2022 р. та досягло 8,01 мільярда на початку 2023 року. Загалом на початку 2023 року мобільними телефонами скористалися 5,44 мільярда людей, що дорівнює 68 відсоткам загального населення світу. Сьогодні в світі налічується 5,16 мільярда користувачів Інтернету, тобто 64,4 % всього населення планети зараз знаходиться в мережі .

2023 року в Україні було 26,70 мільйонів користувачів соціальних мереж, що дорівнювало 74,0 % загального населення (Facebook – 12,85 млн користувачів, YouTube мав 26,70 млн, Instagram – 11,00 млн, TikTok – 13,01 млн, Facebook Messenge охопила 7,75 млн користувачів в Україні, LinkedIn мав 4,30 млн «учасників» в Україні, Twitter в Україні мав 595,9 тис. користувачів). Всього на початок 2023 року в Україні було активно 55,88 мільйонів стільникових мобільних зв'язків, що еквівалентно 154,9 % від загальної кількості населення [91].

Ці дані говорять самі за себе і свідчить, зокрема, про те, що багато людей використовують кілька мобільних з'єднань. Користувачі мобільного Інтернету все частіше використовують свої мобільні телефони для низки онлайн-дій: обмін миттєвими повідомленнями, голосові та відеодзвінки, електронна пошта, соціальні мережі, вебсайти. І цілком зрозуміло, що все це можна використовувати в якості потенційного джерела доказів.

О. О. Торбас у своїй праці, практичному посібнику «OSINT при розслідуванні кримінальних правопорушень», наголошує на важливості використання доказової інформації з відкритих джерел та можливості використання правоохоронними органами відомостей, які можуть бути отримані за допомогою OSINT розслідувань з будь-яких доступних джерел. OSINT (open source intelligence – розвідка відкритих баз даних) – це уніфікований у міжнародній спільноті термін, який можна визначити як розвідку інформації, отриманої із загальнодоступних джерел, яка не потребує таємних методів збору [280, с. 7].

Зарубіжні науковці також наголошують на інформативності електронних джерел доказової інформації, адже звичайна діяльність у сучасному суспільстві залишає кіберслід, який можна використати для реконструкції місцезнаходження людини в певний час, включаючи доступ до її офісу чи дому, її електронні покупки та багато іншого. У деяких ситуаціях цифрові сліди дають нам більше інформації, ніж традиційні сліди [388].

Хочемо відмітити, що SITU Research розробила інструмент для представлення доказів у Міжнародному кримінальному суді, а саме нові засоби

взаємодії з візуальною та просторовою інформацією в залі суду. Ця інтерактивна цифрова платформа була створена у співпраці з Офісом прокурора Міжнародного кримінального суду для полегшення організації, аналізу та представлення доказів, що документують руйнування об'єктів культурної спадщини в Тімбукту, Малі. Поєднуючи геопросторову інформацію, історичні супутникові знімки, фотографії, відео з відкритих джерел та інші форми документації з місця, інструмент був використаний в рамках судового розгляду проти обвинуваченого, пана Ахмада Аль Факі Аль Махді, ймовірного члена збройного угруповання Ансар Дін, якого звинуватили в участі в навмисному знищенні дев'яти мавзолеїв і дверей мечеті в 2012 році. Це перший випадок, коли такий інструмент був використаний у Міжнародному кримінальному суді. Розробка цього інструменту є кроком до нових та все більших застосувань цифрових технологій у судових процесах, спрямованих на притягнення до відповідальності за жорстокі злочини [399].

Як приклад використання інформації з відкритих джерел в якості доказів у практиці ЄСПЛ можна привести справу «Georgia v. Russia (II)» (2021). При прийнятті рішення ЄСПЛ врахував інформацію в електронному вигляді, отриману з відкритих джерел як об’єктивний доказ та посилався на доповідь, опубліковану Американською асоціацією сприяння розвитку науки (AAAS), «Супутникові знімки високої роздільної здатності та конфлікт у Південній Осетії» від 9 жовтня 2008 р. (§ 66, 188, 205) [372].

Крім того, SITU Research розробило новий цифровий інструмент для управління, аналізу та представлення відеодоказів. Багато розслідувань пов'язані з великими обсягами зображень і відеоматеріалів[31] [414].

---

[31] Ця платформа працює з електронними таблицями, збираючи інформацію та факти про кожен об'єкт, як-от джерело, тривалість, тип файлу, геолокацію, хронолокацію, а також теги подій або дій. Кодек постійно вилучає ресурси з доказової бази даних у живий графічно організований інтерфейс користувача. Зовнішня інформаційна панель відображає відповідний просторово-часовий контекст для цих відео - контекст, який присутній, але ледь помітний в електронній таблиці. Інтерфейс користувача поділено на часову шкалу, карту та медіаплеєр. Часова шкала представляє кожен хронолокований ресурс горизонтальною смугою, подібною до програмного забезпечення для редагування відео, а карта, яка підтримувалася Mapbox, представляє кожен геолокований ресурс маркером. Інші функції включають можливість фільтрувати активи за двійковими тегами та шукати їх за буквено-цифровим кодом.

Це вимагає широкого спектру навичок і вміння працювати з різними форматами та типами даних, і при цьому дотримуючись стандартів доказування, визначених національними правовими системами.

В. Школьніков у статті «Правова основа отримання інформації з мережі інтернет у кримінальному провадженні» (2018) вважає, що вироблення єдиного правильного порядку отримання інформації з мережі Інтернет у кримінальному провадженні сприятиме відповідності законодавства всім вимогам, що впроваджує сучасне інформаційне суспільство [364, с. 175]. Також і інші науковці, досліджуючи проблематику огляду вебсторінок, вебсайтів та отримання іншої інформації з відкритих джерел фокусували на цьому свою увагу [97, с. 188].

Цілком очевидно, що не завжди можна отримати фізичний доступ до носіїв інформації в електронному вигляді, інформаційних систем, на яких зберігається така інформація (мова йде про вебсайти, соціальні мережі,тощо, які розташовані за межами України), адже така інформація зберігається на жорстких дисках серверів надавача послуги хостингу, і відповідно неможливо здійснити копіювання інформації та забезпечити підтвердження її автентичності шляхом хешування.

А. Штефан зазначає, що оригіналом вебсайту або сторінки є об’єкт, який містить сукупність даних, доступ до якого здійснюється за його адресою в мережі Інтернет (URL, Uniform Resource Locator) і який зберігається на жорсткому диску (дисках) серверу (серверів) надавача послуг хостингу. Щоб подати до суду оригінал вебсайту чи сторінки, необхідно вилучити з певного сервера жорсткий диск, при цьому доступ до всіх сайтів і сторінок, що містяться на цьому жорсткому диску (дисках), буде тимчасово втрачений. Відтак, виконання такої вимоги не є можливим [365, с. 78; 366, с. 70].

Повністю підтримуємо думку О. О. Торбаса про необхідність використання таких методів збору і збереження інформації з відкритих джерел, щоб мати

можливість під час судового розгляду встановити її достовірність та відповідно ланцюг забезпечення збереження [280, с. 38].

Внаслідок російського вторгнення в 2014 році та повномасштабних воєнних дій на території України з 24 лютого 2022 року, тимчасової окупації окремих територій, правоохоронні органи не мають повноцінного інструмента у проведенні належного досудового розслідування і тому отримання інформації з відкритих інтернет-джерел є важливою доказовою базою у розслідуванні воєнних злочинів, злочинів проти миру та людяності. А для цього потрібні належні стандарти документування інформації з відкритих джерел та процедура належного аналізу, технології роботи слідчих з інформацією з відкритих джерел.

Постає питання чи можна говорити про інформацію з відкритих джерел як один із видів електронних доказів? Якщо так, то за яких умов можна її використовувати як доказ у кримінальних провадженнях?

І в цьому аспекті постає питання щодо «легалізації» інформації, отриманої в результаті проведення OSINT розслідування в кримінальному процесі.

Ми повністю погоджуємося з висловленою думкою про те, що збір доказів у кримінальному провадженні повинен відбуватися в порядку, передбаченому кримінальним процесуальним законодавством, а способи збирання та закріплення доказів мають чітко відповідати тим вимогам, які встановив законодавець адже «можна провести дуже ефективне OSINT розслідування, знайти інформацію, яка підтверджує факт кримінального правопорушення, проте допустити помилки при «введенні» таких даних в кримінальний процес, що зведе нанівець всі зусилля OSINT аналітика» [280, с. 100].

Задля ефективного використання інформації в електронному вигляді, яка знаходиться у відкритому доступі для розслідування правопорушень зі сфери міжнародного кримінального та гуманітарного права у 2020 році Центр прав людини Університету Берклі в Каліфорнії та Офіс Верховного комісара ООН з прав людини розробили рекомендаційний документ – Протокол Берклі 2. Цей Протокол містить базові положення щодо міжнародних стандартів для реалізації онлайн-

розслідування правопорушень. Також у протоколі містяться настанови щодо методів і процедур для збирання, аналізу та зберігання інформації в електронному вигляді, враховуючи певні правові принципи [421].

Працюючи відповідно до цього протоколу, всі учасники кримінального провадження отримують детальні та дієві рекомендації щодо збирання, зберігання, дослідження та використання інформації в електронному вигляді як доказу.

Нами ще раніше висловлена думка, що слідчі, прокурори та судді повинні розуміти технічні аспекти інформації в електронному вигляді, щоб забезпечити їх належну оцінку. Для того щоб інформація з відкритих джерел була прийнята як доказ у суді, необхідно підтвердити її достовірність та ланцюг забезпечення збереження. Автентичність джерела доказової інформації слід підтверджувати за допомогою як зовнішніх, так і внутрішніх маркерів автентичності [259].

«По-перше, коли проводиться аналіз доказів з відкритих джерел необхідно звертати увагу на всі деталі. Проаналізувати атрибуцію (подію, яка викликала появу відповідного джерела), геолокацію, здійснити також технічний аналіз, тобто аналіз метаданних (назва файла, його розмір, дату створення, історію файла). Все дасть можливість проаналізувати ризик викривлення інформації, розміщення неправдивої інформації. Зовнішні маркери автентичності повинні узгоджувати з іншими доказами у кримінальному провадженні. Автентичність джерела може також підтверджуватися показаннями свідків та висновками експерта. І при цьому необхідно звертати увагу на суперечності між показаннями та електронними доказами. Цілком зрозуміло, що інформація з відкритих джерел може бути корисною для відтворення загальної картини події. Однак може мати і доказове значення – доводити або спростовувати обставини, які підлягають доказуванню. А для цього потрібні належні стандарти документування інформації з відкритих джерел та законодавчо визначена процедура належного аналізу, технології роботи слідчих з інформацією з відкритих джерел. Автентичність – це здатність продемонструвати, що цифровий елемент залишається незмінним з моменту його збирання. Це вимагає, щоб цифровий елемент залишався незмінним під час

перебування в архіві або будь-які зміни до нього були задокументовані» [280, с. 53].

В наступному розділі дисертаційного дослідження нами буде надано обґрунтування необхідність закріплення на законодавчому рівні обов'язкової складової при копіюванні інформації — це застосування хешування. Це дасть можливість всім учасникам процесу бути переконаним, що таким чином зафіксована інформація є автентичною. Адже хешинговий алгоритм – це коли доказу присвоюється унікальний набір цифр і його потім неможливо ані змінити ані підробити. І тому ми повністю підтримуємо думку О. О. Торбаса, що під час проведення огляду комп'ютерних даних відповідно до ст. 237 КПК України з подальшим копіюванням таких даних на електронний носій слідчий, дізнавач, прокурор обов'язково в протоколі такого огляду повинна зазначати хеш-суми файлу (файлів), які були скопійовані на такий носій, з якими в подальшому можна буде порівнювати цілісність копій таких файлів [280, с. 116].

«Вивчення комп'ютерних систем або цифрових пристроїв – це криміналістична операція спрямована на пошук доказів, пов'язаних з такими засобами. Процесуальні заходи такого спрямування можуть мати різні назви (обшук комп'ютера, комп'ютерна криміналістична експертиза, комп'ютерний криміналістичний аналіз), як правило їх здійснюють на підставі дозволу, виданого відповідним органом – здебільшого судом» [415, с. 16].

Практика правозастосування дозволяє виділити три способи фіксації електронних доказів, при цьому враховується також можливість фізичного доступу до носія інформації (огляд та фіксація інформації, яка знаходиться в кіберпросторі (мережі Інтернету), огляд та копіювання інформації або створення образу, фізичне вилучення комп'ютерів та інших пристроїв.

В наукових дослідженнях вчені розмежовують огляд електронних документів за місцем їх знаходження: 1) електронні документи на фізичних носіях інформації; 2) електронні документи у вигляді публікацій у мережі Інтернет; 3) електронні документи, розміщені у хмарних сервісах зберігання

інформації [238, с. 122, 184]. Процедури отримання електронної інформації можна поділити на: 1) огляд Інтернет-ресурсів, доступ до електронних інформаційних систем або їх частини яких не обмежується її власником, володільцем або утримувачем або не пов’язаний з подоланням системи логічного захисту (гласна слідча (розшукова) дія); 2) огляд в порядку зняття інформації з електронних інформаційних систем (НСРД) [277, с. 774].

Отже, практикою були вироблені окремі методи фіксації інформації з відкритих джерел для подальшого використання в якості доказової інформації у кримінальному провадженні.

До прикладу можна привести постанову від 09.05.2023 р. (справа № 554/5867/18), в якій ВС ККС не визнав порушення щодо використання інформації, яка була отримана шляхом моніторингу всесвітньої мережі «Інтернет» до внесення відомостей до ЄРДР, оскільки такі дії не були спрямовані на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні, а тому відповідно до ст. 223 КПК України не відносяться до слідчих (розшукових) дій [184]. В той же час суд визнав неналежним доказом відеозапис, отриманий шляхом відеозапису екрану комп'ютера під час відтворення первинного відеозапису [183].

Як доказ була використана інформація з мережі інтернету, яка була отримана в результаті проведення негласної слідчої (розшукової) дії – зняття інформації з транспортних телекомунікаційних мереж [29]. Підставами для звернення з клопотанням до суду про надання дозволу на проведення обшуку була, зокрема, інформація отримана в результаті проведеного аналітичного дослідження відкритих джерел інформації методами OSINT [322; 338; 345].

Аналогічно, слідчий мотивував клопотання про надання тимчасового доступу до речей та документів інформацією, яка була отримана «на основі відкритих джерел (OSINT)» [318; 334].

Отримання доказової інформації з відкритих джерел (відеозаписи були розповсюджені у вільному доступі в мережі інтернет без обмежень у доступі) [162].

Одними із доказів, покладених в основу вироку суду була інформація отримана з відритих джерел (протокол огляд інформації, розміщеної у Всесвітній мережі Інтернет) [30; 35].

Не можемо залишити без уваги і рішення Солом'янського суду м.Києва від 21.02.2025 року у справі №243/7147/23. Так, суд ухвалюючи вирок та визнаючи особу винною у скоєнні кримінального правопорушення, передбаченого 2 ст. 111 КК України, як один із доказів винуватості використав інформацію з відкритих джерел, а саме інформацію, розміщену на сайті «Миротворець». Позицію захисту про недопустимість даного доказу у зв`язку з незахищеністю оглянутої інформації з мотивів відсутності у матеріалах НСРД (фотознімках, відеофайлах) метаданих, суд не прийняв до уваги з мотивів, що метадані є обов`язковим елементом електронного документу, яким протокол огляду не є. Крім того, суд мотивував використання даної інформації тим, що інструменти OSINT можуть використовуватись будь-ким у будь-якій сфері для дослідження інформації [44].

Не заперечуючи можливість використання інформації з відкритих джерел, дозволимо собі не погодитися з думкою суду, що така інформація в електронному вигляді не потребує підтвердженні автентичності. Так, в протоколі проведення процесуальної дії, а в даному випадку це НС(Р)Д фіксується хід і результати такої дії. Звісно, протокол огляду не потребую метаданих, однак в ньому повинні міститься, зокрема, відомості про виготовлені копії інформації, у тому числі комп’ютерних даних та спосіб їх ідентифікації (ч.3 ст.104 КПК України) та крім того, до документів належать складені в порядку, передбаченому КПК України, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії (п.3 ч.2 ст.99 КПК України). В той же час виникає також питання щодо покладення судом на сторону захисту обов'язку доводити незаконність використання програмного забезпечення, створюючи більш сприятливі умови для сторони обвинувачення.

Поділяємо занепокоєння висловлене І. Г. Каланчою у наукових тезах «Результати OSINT як джерело доказів у кримінальному процесі України» щодо

можливості використання як доказів інформації з відкритих джерел без відповідного внесення змін до ст.99 КПК України та вироблення судовою практикою правових позицій щодо використання такої інформації [86, с. 47].

Отже, на наш погляд, використання OSINT-доказів потребує визначення в законодавстві певних стандартів їх процесуального оформлення та оцінки, що говорить про перспективність подальших наукових розвідок.

Необхідно відмітити, що ЗУ «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам» були внесені зміни, зокрема в ст. 237 КПК, в якій передбачили огляд комп'ютерних даних. Так, огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у 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 у паперовій формі) (ч. 2 ст. 237 КПК України) [216].

Однак, вчені висловлюють думки щодо неможливості сприйняття «комп'ютерних даних» безпосередньо суб'єктом розслідування з урахуванням природи інформації, зафіксованої в електронній формі, і навіть самого поняття «комп'ютерних даних», і, «відтворюючи комп'ютерні дані у протоколі огляду, суб'єкт розслідування вже фактично вносить певні зміни в таку інформацію, залишаючи «цифровий слід» (digital footprint)» [64, с. 119].

Погоджуючись з логікою міркувань науковців, хочемо також звернути увагу на конструкцію ч. 4 ст. 99 КПК, з положень якої вбачається, що законодавець визначає, що в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах містяться як комп'ютерні дані, так і інша інформація, тобто фактично відмежовує «комп'ютерні дані». Таке законодавче рішення на нашу думку є нелогічним і суперечить поняттю «комп'ютерні дані», яке міститься в Конвенції з кіберзлочинності.

Професорка О. В. Капліна наголошує на необхідності чіткого законодавчого вирішення змістовного наповнення терміну «комп'ютерні дані» та самої суті такої процесуальної дії як огляд комп'ютерних даних, адже «проведення огляду вмісту папок та файлів, які зберігаються на комп'ютері безумовно пов'язаний з втручанням у приватне життя, що захищається ст. 32 Конституції України та ст. 8 Конвенції про захист прав людини та основоположних свобод»[89, с. 36].

Специфіка об'єкта огляду «комп'ютерних даних» дають підстави для запровадження окремого комплексу тактичних рекомендацій щодо проведення даної процесуальної дії [96, с. 54].

Насамперед, хочемо звернути увагу на те, що нормами ст. 237 КПК не передбачено обов'язковість участі спеціаліста при проведені огляду комп'ютерних даних. Однак, на нашу думку, для забезпечення ефективної фіксації інформації та використання під час судового розгляду виготовленої під час огляду копії інформації, необхідно забезпечити дотримання вимог ч. 4 ст. 99 КПК України щодо залучення спеціаліста, незважаючи на відсутність відповідної вимоги в ст. 237 КПК України.

На нашу думку, огляд інформації, яка міститься у відкритих джерелах є важливим етапом у зборі електронних доказів. Проте однієї лише фіксації таких даних в порядку ст.237 КПК України недостатньо. Основна проблема полягає в тому, що цифровий контент є динамічний, його можна змінити, видалити або зробити недоступним у будь-який момент. Тому необхідно не лише зафіксувати факт наявності відповідної інформації, а й забезпечити її належне збереження та офіційне витребування.

Отже, при відсутності доступу до фізичного носія (наприклад, у випадку фіксації даних з мережі Інтернет) доцільно дотримуватися наступної процедури: 1) фіксація даних шляхом огляду інформації в порядку ст. 237 КПК України з дотриманням вимог ч. 4 ст. 99 КПК України; 2) термінове зберігання даних згідно процедур Будапештської конвенції (ст. 29) з подальшим скеруванням запиту в порядку ст. 548 КПК України. На сьогодні правоохоронними органами також є

можливість використання захищеної платформи зв'язку SIENA (Secure Information Exchange Network Application) для обміну оперативною інформацією в рамках кримінальних проваджень на підставі Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво [233].

І в цьому аспекті повністю підтримуємо думку Н. М. Ахтирської, що для ефективності міжнародного співробітництва під час кримінального провадження щодо збору доказів в електронній формі необхідно вирішення питання приєднання України до Конвенції про захист фізичних осіб під час автоматичної обробки персональних даних (ETS № 108) [104], ратифікації Другого додаткового протоколу до Конвенції про кіберзлочинність [413] і відповідно імплементація в законодавство окремих положень Будапештської конвенції, Першого та Другого додаткового протоколу до Конвенції про кіберзлочинність [7].

Професор І. Г. Богатирьов у статті «Актуальні проблеми запобігання кіберзлочинності в Україні» зазначає, що саме феномен кіберзлочинності з'явився у третьому тисячолітті завдяки системній цілісність і водночас багатогранності суспільного життя з об'єктивною необхідністю використанням сучасних інформаційних технологій (інтернет, комп'ютер, електронні мережі тощо) [22, с. 17].

Враховуючи, що огляд ком'ютерних даних, норма, яка введена в дію не досить давно, і слідчі під час проведення даної С(Р)Д зіштовхуються з труднощами фіксування у протоколі, нами запропоновано алгоритм фіксації даних в протоколі огляду комп'ютерних даних.

Так, протокол огляду комп'ютерних даних повинен містити:

1) дату та час проведення слідчої дії;

2) місцезнаходження, точна адресу, де проводиться слідча дія;

3) номер кримінального провадження;

4) посаду та інші дані, які ідентифікують особу, яка проводить слідчу дію;

5) рішення суду, яке надає дозвіл на проведення такої слідчої дії (ми обґрунтовуємо думку, що для огляду комп'ютерних даних, за виключенням тих, які

знаходяться у відкритому доступі, необхідний судовий дозвіл і це більш детально буде обґрунтовано в наступному підрозділі. Судова практика вказує на те, що слідчі звертаються до суду з клопотанням про надання дозволу на огляд комп'ютерних даних, однак практика вирішення таких клопотань не є однозначною[32] [до примітки див. 312].

Під час судового розгляду кримінального провадження встановлено, що при здійсненні огляду слідчим було фактично здійснено доступ до інформації щодо вмісту повідомлень електронної поштової скриньки, що є різновидом втручання у приватне спілкування, а доступ до такої інформації, відповідно до ст. 264 КПК України відноситься до негласних слідчих (розшукових) дій, і проводиться лише на підставі ухвали слідчого судді відповідного апеляційного суду [347].

6) осіб, які присутні при проведені огляду комп'ютерних даних (спеціаліст, прокурор, потерпілий, його представник, обвинувачений, захисник, інші особи у випадках передбачених КПК;

7) ідентифікаційні ознаки комп'ютерних систем чи інших пристроїв, в яких знаходяться комп'ютерні дані які підлягають огляду, в тому числі і автономні пристрої зберігання даних: внутрішні та зовнішні жорсткі диски (HDD, SSHD, SSD, CD, DVD, SD, microSD, флеш пам'ять тощо). Необхідно зазначати елементи ідентифікації (марка, модель, серійний номер або код IMEI та операційну систему встановлену на пристрої, дату встановлення операційної системи, облікові записи користувачів, мережеві налаштування, код, пароль блокування на мобільному пристрої, ємність зберігання, різні написи, можливі видимі недоліки чи пошкодження;

8) апаратні пристрої та програми, які будуть використані для такого огляду;

---

[32] Слідчий суддя відмовив в задоволенні клопотання слідчого про надання дозволу на проведення огляду комп'ютерних даних, мотивуючи тим, що органом досудового розслідування не наведено достатніх підстав вважати, що доступ до комп`ютерної техніки або відомостей, які можуть у них міститися, неможливо отримати у добровільному порядку шляхом витребування речей, документів, відомостей відповідно до ч. 2 ст. 93 цього Кодексу, або за допомогою інших слідчих дій, передбачених цим Кодексом

Цілком логічно, що огляд комп'ютерних даних може проводитися тільки із застосуванням спеціальних пристроїв та програм, а отже необхідно «вказати в протоколі слідчих дій характеристики апаратних та програмних засобів (тип та параметри операційної системи, серійні номери апаратних та інтерфейсних складових ПЕОМ, MAC-адреси мережевих компонентів тощо)» [127, с. 230]. Здебільшого електронна інформація мережі Інтернет зберігається у вигляді веб-сторінок, які складаються з окремих електронних документів, що містять дані у вигляді тексту, графічних зображень, електронних таблиць, відео тощо і можуть бути переглянуті за допомогою спеціальних комп'ютерних програм – веб-переглядачів (браузерів): Internet Explorer, Mozila Firefox, Google Chrome, Opera та інших [75, с. 25].

9) час початку огляду комп'ютерних даних (обов'язково перевірити часовий пояс, який використовується в системі);

З точки зору електронних доказів системний годинник часто відіграє важливу роль у подіях відміток часу. Наприклад, операційна система використовує дату і параметри часу, щоб анотувати свій запис подій, таких як створення або модифікація файл, тобто метадані файлу, оскільки інформація про дату й час пов'язана із файлом, але не є частиною даних у файлі. Мітки часу також записуються для системних подій, таких як логіни користувачів, зміна паролів і, залежно від призначення пристрою, записані події, такі як кількість кроків, пройдених користувачем. Час і дата інформація, пов'язана з такими подіями, записується у файли системного журналу (журнали подій). Такі журнали часто є важливим джерелом інформації про послідовність подій уявлення про передбачувану конкретну діяльність користувача [408, с. 426].

10) назва файла, який оглядається, розширення файла, тип файла, дата та час створення, дата та час останнього використання, дата та час останньої зміни, розташування, значення хешів;

11) всі зроблені кроки в хронологічному порядку (детальний опис проведених заходів і операцій);

12) посилання на технічний звіт сформований програмними засобами, які використовують для криміналістичного аналіз;

13) опис носія інформації, на який здійснюється копіювання або створюється образ;

Криміналістичну копію можна створити двома способами: як клон (побітова копія вихідного середовища на цільовий носій) або як образ (побітова копія даних із вихідного носія у файл образу на цільовому носієві , як правило може містити метадані [415, с. 20].

Деякі вчені висловлюють думку, що «під час проведення огляду не пов'язаного із доступом до електронних інформаційних систем або їх частини, який обмежується її власником, володільцем або утримувачем або не пов'язаного з подоланням системи логічного захисту, участь спеціаліста є необов'язковою [277, с. 774]. В той же час є протилежні думки щодо обов'язкової участі спеціаліста під час вилучення цифрової інформації з різноманітних накопичувачів зовнішньої пам'яті. Такий підхід обумовлюється тим, що «на практиці існує проблема недостатніх знань слідчих та оперативних кадрів у сфері використання програмних засобів комп'ютерної техніки. Ба більше, наявним є дефіцит напрацьованих методик, які дають можливість правильно та ефективно збирати цифрову інформацію. Складність їх процесуальної оцінки полягає в можливості фальсифікації без залишення видимих слідів проведених маніпуляцій, які на сучасному рівні науки і техніки не завжди можуть бути виявлені» [247, с. 50].

Крім того, умова обов'язкового залучення спеціаліста для копіювання електронної (цифрової) інформації демонструє визнання законодавцем специфічної природи такої інформації та необхідність фахових професійних знань у суб'єкта, який здійснює її збирання [65, с. 42–43].

На нашу думку, для забезпечення ефективної фіксації інформації та використання під час судового розгляду виготовленої під час огляду копії інформації, необхідно забезпечити дотримання вимог ч. 4 ст. 99 КПК України щодо залучення спеціаліста, попри відсутність відповідної вимоги в ст. 237 КПК

України. Відповідно до ч. 4 ст. 99 КПК України, дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а *також копії інформації, у тому числі комп'ютерних даних*, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, *виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа* (курсив наш - І. Смаль). У цьому контексті необхідно зазначити, що сам факт залучення спеціаліста не гарантує відповідність копії інформації в електронному вигляді оригіналу. Спеціаліст, якого залучає сторона обвинувачення, повинен володіти необхідними знаннями та навичками у сфері інформаційних технологій та бути здатним забезпечити такий процес копіювання, який включає перевірку цілісності інформації та її верифікацію. Таким чином, буде дотриманий процесуальний аспект копіювання інформації. Однак, крім процесуального аспекту повинен бути дотриманий і технічний аспект копіювання інформації, який буде гарантувати цілісність та справжність доказової інформації. Серед основних міжнародних стандартів, у яких прямо чи опосередковано визначені основоположні засади роботи із цифровою інформацією, зазвичай виокремлюють такі: ISO/IEC 27037:2012 «Guide for Collecting, Identifying, and Preserving Electronic Evidence» (Керівництво зі збирання, ідентифікації та збереження електронних доказів); ISO/IEC 27041:2015 «Guide for Incident Investigations» (Керівництво з розслідування інцидентів); ISO/IEC 27042:2015 «Guide for Digital Evidence Analysis» (Керівництво з аналізу цифрових доказів); ISO/IEC 27043:2015 «Incident Investigation Principles and Processes» (Принципи та процес розслідування інцидентів); ISO/IEC 27050- 1:2016 «Overview and Principles for eDiscovery» (Огляд і принципи eDiscovery) [404].

Відповідно до наказу від 06.12.2017 р. № 400 «Про прийняття національних нормативних документів, гармонізованих з європейськими та міжнародними нормативними документами, скасування національних нормативних документів, змін до національних нормативних документів в Україні» 01 січня 2019 р. набрав

чинності державний стандарт ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). В цьому стандарті викладені рекомендації, що стосуються діяльності з ідентифікації, збирання, здобуття та збереження цифрових доказів [73].

14) програмні засоби, що забезпечують цілісність скопійованих даних (хешування).Про необхідність закріплення на законодавчому рівні застосування цією процедури підтвердження автентичності скопійованої інформації нами буде досліджено в наступному розділі;

15) опис комп'ютерних систем та цифрових пристроїв, які підлягають упакуванню після огляду;

16) ідентифікаційні дані відеокамери, якщо її використовували під час слідчої дії;

17) час завершенню огляду комп'ютерних даних;

16) підпис слідчого;

17) зауваження та пояснення учасників слідчої дії;

18) зазначення місця, де зберігають докази.

Для отримання відомостей, які не містяться у відкритому доступі, але які мають важливе значення для кримінального провадження можуть бути застосовані механізми Конвенції про кіберзлочинність та процедури міжнародного співробітництва під час кримінального провадження, визначені Розділом IX КПК України.

Після проведення огляду комп'ютерних даних в порядку ст. 237 КПК України та аналізу отриманої інформації можливо визначити місця перебування провайдера, адміністратора інформаційної системи, місця знаходження сервера тощо. Що в свою чергу дасть можливість скерування до центрального уповноваженого органу відповідної іноземної держави, який відповідає за надсилання та відповідь на запити про взаємну допомогу запиту про термінове збереження комп'ютерних даних, які зберігаються в порядку ст. 16 Конвенції про

кіберзлочинність. Запит має стосуватися відомостей, що не отримані під час огляду комп'ютерних даних, але які мають значення для кримінального провадження. За результатами скерування даного запиту центральний уповноважений орган відповідної іноземної держави (при дотриманні вимог та процедур Конвенції про кіберзлочинність) забезпечить зберігання даних про які вказано в запиті. Після дотримання такої процедури можливо направити до уповноваженого органу відповідної іноземної держави запит про міжнародну правову допомогу в порядку ст. 551 КПК України для отримання даних, що збережені за результатами попередньо описаної процедури. За умови дотримання належної правової процедури відповідь компетентного органу іноземної держави міститиме запитувані стороною обвинувачення відомості, що збережено.

Висновки до розділу 2

Аналіз теоретичних та практичних питань, пов'язаний з дослідженням видів електронних доказів у кримінальному процесі, дозволив дисертанту зробити наступні висновки:

1. У межах розділу здійснено аналіз наукових підходів до класифікації електронних доказів, запропонованих вітчизняними дослідниками. На основі дослідженого матеріалу розроблено авторську класифікацію електронних доказів із виокремленням релевантних критеріїв, що враховують їх походження, форму, змістовну природу та процесуальні особливості, а саме : 1) за формою існування; 2) за способом формування; 3) за технічним середовищем існування. Доведено теоретичне та практичне значення класифікації електронних доказів, оскільки саме вона сприяє адаптації кримінального процесу до умов цифрової епохи, формуванню єдиних стандартів доказування з врахуванням процесуальних особливостей їх збирання, збереження, дослідження та оцінки.

2. Досліджено поняття електронного документа як на законодавчому рівні, так і в науковій доктрині. Проаналізовано погляди українських учених щодо

правової природи електронного документа, а також практику його використання у судових рішеннях у контексті співвідношення з поняттям електронного доказу. Встановлено, що на практиці ці терміни нерідко вживаються як синоніми, що не відповідає їх змістовному наповненню та викликає труднощі у правозастосуванні.

3. Проведений нами детальний аналіз електронного документа: його ознак, законодавчого визначення, використання як доказу у судовій практиці та критерії оцінки достовірності дає нами підстави стверджувати, що ключові характеристики електронного документа—наявність обов'язкових реквізитів, в тому числі електронного підпису не притаманне іншим видам електронних доказів, як то мультимедійні файли, текстові документи чи метадані, які мають іншу природу. Це розмежування є важливим для правильної правової оцінки будь-якої інформації в електронному вигляді у судовій практиці.

4. Проаналізовані наукові підходи та судова практика щодо можливості використання інформації з відкритих джерел (зокрема, з використанням OSINT методів) у кримінальному провадженні дозволили акцентувати увагу на необхідності підтвердження автентичності, достовірності та цілісності такої інформації. Зазначено, що така інформація може мати доказове значення лише за умови її використання у сукупності з іншими доказами, що відповідає вимогам належності, допустимості та достовірності.

5. Огляд інформації, яка міститься у відкритих джерелах є важливим етапом у зборі електронних доказів. Проте однієї лише фіксації таких даних в порядку ст.237 КПК України недостатньо. Основна проблема полягає в тому, що цифровий контент є динамічний, його можна змінити, видалити або зробити недоступним у будь-який момент. Тому необхідно не лише зафіксувати факт наявності відповідної інформації, а й забезпечити її належне збереження та офіційне витребування.

Отже, при відсутності доступу до фізичного носія (наприклад, у випадку фіксації даних з мережі Інтернет) доцільно дотримуватися наступної процедури: 1) фіксація даних шляхом огляду інформації в порядку ст. 237 КПК України з дотриманням вимог ч. 4 ст. 99 КПК України; 2) термінове зберігання даних згідно

процедур Будапештської конвенції (ст.29) з подальшим скеруванням запиту в порядку ст. 548 КПК України. Для забезпечення ефективної фіксації інформації та використання під час судового розгляду виготовленої під час огляду копії інформації, необхідно забезпечити дотримання вимог ч. 4 ст. 99 КПК України щодо залучення спеціаліста, незважаючи на відсутність відповідної вимоги в ст. 237 КПК України.

РОЗДІЛ 3
ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ПРОЦЕСІ КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО ДОКАЗУВАННЯ

3.1 Зняття показань технічних приладів та технічних засобів у кримінальному процесі

Збирання доказів у кримінальному провадженні є важливим етапом досудового розслідування кримінальних правопорушень. Інформація в електронному вигляді, яка може бути доказом у кримінальному провадженні, часто утворюється в результаті її фіксування приватними особами, так і в автоматичному режимі технічними приладами та технічними засобами, що мають функцію фото-кінозйомки, відеозапису [261].

Дослідження правової природи показань технічних приладів та технічних засобів як доказу, що з'являється в результаті слідчої (розшукової) дії, передбаченої ст. 245-1 КПК України та аналіз правозастосування сприятиме виробленню доктринальних рекомендацій. Всі ці питання є досить актуальними і потребують ґрунтовного дослідження та законодавчого вирішення.

Для реалізації завдань кримінального провадження (ст. 2 КПК України) кримінальний процесуальний закон встановлює процедуру збирання доказів, визначає вичерпний перелік процесуальних джерел доказів (ст. 84, 298-1 КПК України), вказує на необхідність встановлення належності на допустимості при визнанні відомостей доказами та оцінку доказів з точки зору належності, допустимості, достовірності. Недопустимість обґрунтування обвинувачення особи у вчиненні злочину доказами, які одержані незаконним шляхом, закріплена в статті 62 Конституції України [108].

Практична реалізація такої засади кримінального провадження як законність полягає в неухильному додержанні вимог Конституції України, КПК України, міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, вимог інших актів законодавства (ст. 9 КПК України) [113].

Варто зазначити, що питання стосовно процесуальних джерел доказів, передбачених чинним КПК України, порядок визнання доказів недопустимими нині не становлять безпосередній предмет нашого дослідження, проте вони є дотичними і безпосередньо пов'язані з практичними аспектами збирання та закріплення електронних доказів. Тому, враховуючи обсяг дисертаційного дослідження та не виходячи за межі предмета дослідження, в цьому параграфі зупинимося лише на більш проблемних питаннях, які, на наш погляд, викликають найбільший науковий інтерес і вирішення яких сприятиме як правильному розумінню, так і належному правозастосуванню електронних доказів.

У контексті дослідження проблематики «електронних доказів» та обґрунтування підстав виділення їх в окреме процесуальне джерело [263], а також обґрунтування думки щодо неможливості визнання доказами відомості (фактичні дані), отримані не з процесуального джерела або не в порядку передбаченому КПК, слід звернути увагу на появу нового джерела доказів у кримінальному процесі: показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису. Таке джерело доказів запроваджено виключно у кримінальних провадженнях щодо кримінальних проступків (ст.298-1 КПК України).

З прийняттям Закону України від 15.03.2022 р. № 2137-IX «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» з'явилася норма закону, яка визначає процесуальний порядок отримання фактичних даних із такого процесуального джерела доказів, як показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису [216], а саме джерело доказів – дещо раніше [214].

Отже, відповідно до ч. 2 ст. 84 КПК України процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів, а ст. 298-1 КПК України визначає, що процесуальними джерелами доказів у кримінальному

провадженні про кримінальні проступки, також є пояснення осіб, результати медичного освідування, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису [113].

Законодавець розширяє систему процесуальних джерел доказів, доповнюючи її джерелами, що можуть бути використані під час здійснення досудового розслідування кримінальних проступків. Деякі науковці, зокрема, В. М. Тертишник досить категорично висловилися з приводу появи «нових процесуальних джерел», так науковець вважає, що приписи ч. 2 ст. 298-1 КПК України не відповідають конституційному концепту допустимості доказів, викладеному в ст. 62 Конституції України [276, с. 220].

Схожа позиція і М. Я. Никоненка, який вважає, що «при розширенні кола джерел доказів втрачаються самі ознаки системності» [137, с. 164].

Цікавими є результати опитування практикуючих юристів щодо доцільності виділення своєрідних процесуальних джерел доказів у кримінальних проступках (див. додаток Б). Як ми бачимо, думки респондентів розділилися майже порівно, що, на нашу думку, свідчить про наявність як аргументованих підстав на користь такого законодавчого рішення, так і обґрунтованих сумнівів щодо її практичної доцільності. Така ситуація свідчить про дискусійність питання та потребу у теоретичному осмисленні.

З пояснювальної записки до проєкту ЗУ «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за «гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 р[33] вбачається, що …[до примітки див. 216].

---

[33] дана норма була введена в дію з метою швидкого, повного і неупередженого розслідування кримінальних проваджень, сприяння посиленню можливості органів досудового розслідування щодо розкриття справ «по гарячим слідам» та не потребує судового контролю. Але при цьому хочемо акцентувати увагу на наступному. В законопроєкті мова йшла про технічні прилади та технічні засоби з автоматичною функцією фото-, кінозйомки, відеозапису «запровадження слідчої (розшукової) дію як зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, *розташованих в публічно доступних місцях* (курсив наш - І. Смаль)

Також можливість здійснення даної С(Р)Д без судового контролю обґрунтовувалося відсутністю навіть потенційної можливості порушення прав фізичних осіб під час такої слідчої дії з посиланням на норми ч. 1 ст. 307 ЦК України, відповідно до якої встановлено, що згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку припускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру [220].

Правова природа даної процесуальної дії хоч і викликала інтерес науковців, але є майже не дослідженою в теоретичному, а тим паче практичному аспекті.

Досліджуючи правову природу зняття показань технічних приладів і технічних засобів, насамперед нас цікавить «результат» такої С(Р)Д — показання технічних приладів та технічних засобів як потенційне процесуальне джерело доказів. Варто перш за все, звернути увагу на термінологію «зняття показань», яка застосована законодавцем для даної С(Р)Д. В юридичній літературі з цього приводу вже мають місце публікації. Не вдаючись до їх критичного аналізу, вважаємо за можливе висловити власний погляд щодо процесуального наповнення цієї категорії. З позиції дотримання правил формальної логіки доречно звернути увагу не лише на зовнішню мовну оболонку понять і категорій, а й дотримання законів логіки при формуванні таких понять та виправданість їх використання у відповідних нормах права [120, с. 123].

Спершу, звернемося до аналізу смислового навантаження слова «показання», яке відповідно до академічного тлумачного словника української мови – це дані вимірювальних приладів (про температуру, тиск, погоду і т. ін.) [255, с. 9]. Однак, як його використовувати в розрізі кримінальних процесуальних відносин? Як вбачається з норми статті 245-1 КПК України зміст даної слідчої дії полягає у копіюванні інформації, яку зафіксували технічні прилади та технічні засоби, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, а отримана інформація є не чим інакшим як документом (ст. 99 КПК України визначає, що до документів відносяться, зокрема, матеріали фотозйомки,

звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані)). Вочевидь, незрозуміла логіка появи такого виду доказів як « показання технічних приладів і технічних засобів» і тим паче виділення його в окреме джерело.

Так, В. С. Новожилов, А. С. Зозуля переконані, що поява такого джерела доказів як показання техприладів та техзасобів є нічим інакшим як калькуванням з ч. 1 ст. 251 КУпАП [138, с. 78].

Важко не погодитися з тим, що технічні прилади і технічні засоби при своєму функціонуванні продукують не стільки «показання», скільки «дані», «інформацію» [138, с. 78]. Так, ст. 251 КУпАП визначає,[34] [100].

Що саме може належати до технічних приладів, технічних засобів, з яких можуть бути зняті такі показання? На думку О. В. Капліної до технічних приладів та технічних засобів, з яких можуть зняті показання, можуть належати автомобільні відео-реєстратори, безпілотні літальні апарати, призначені для виконання польоту без пілота на борту та здійснення фото- або кінозйомки чи відеозапису; технічні прилади та засоби (портативні відеореєстратори) якими оснащені підрозділи НП з метою здійснення автоматичної фото- і кінозйомки чи відеозапису; стаціонарні системи, які встановлюються в публічно доступних місцях та призначені для здійснення фото- і кінозйомки, відеозапису з метою охорони публічної безпеки чи власності, безпеки дорожнього руху, громадського порядку, здійснення фіксування правопорушень [87, с. 358].

[34] що фактичні дані (докази) можуть встановлюватися, зокрема, показаннями технічних приладів та технічних засобів, що мають функції фото- і кінозйомки, відеозапису, у тому числі тими, що використовуються особою, яка притягається до адміністративної відповідальності, або свідками, а також працюючими в автоматичному режимі, чи засобів фото- і кінозйомки, відеозапису, у тому числі тими, що використовуються особою, яка притягається до адміністративної відповідальності, або свідками, а також працюючими в автоматичному режимі або в режимі фотозйомки (відеозапису), які використовуються при нагляді за виконанням правил, норм і стандартів, що стосуються забезпечення безпеки дорожнього руху, безпеки на автомобільному транспорті та паркування транспортних засобів.

ЗУ «Про Національну поліцію» від 2 липня 2015 року № 580-VIII[35] містить норму... [до примітки див. 231]. Окрім згадки у ЗУ «Про Національну поліцію» мова про технічні прилади та засоби йде і в ст. 14-2 КУпАП [100].

Детальне термінологічне визначення технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису міститься в Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису, затвердженої Наказом МВС України від 18.12.2018 р. № 1026 [227].

Зазначена Інструкція, до речі, не поширюється на здійснення працівниками поліції фото- і кінозйомки, відеозапису процесуальних дій відповідно до вимог статті 107 КПК України, НСРД, оперативно-розшукових заходів, застосування в системі фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі відповідно до вимог постанови у сфері забезпечення безпеки дорожнього руху в автоматичному режимі відповідно до вимог постанови Кабінету Міністрів України від 10.11.2017 р. № 833 «Про функціонування системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі» [234].

Ця Інструкція розмежовує автомобільну та стаціонарну систему технічних приладів і технічних засобів фото- і кінозйомки, відеозапису, дає визначення «безпілотного літального апарату», «відеореєстратора» (пристрій, призначений для запису, зберігання та відтворення відеоінформації) та «портативного відеореєстратора» (пристрій, призначений для запису, зберігання та відтворення відеоінформації, технічні характеристики та особливості конструкції якого дають змогу закріпити його на форменому одязі поліцейського). До речі, в ній є згадка

---

[35] яка має назву застосування технічних приладів, технічних засобів та спеціалізованого програмного забезпечення (ст. 40), якою визначено, що такими приладами, зокрема, можуть бути фото- і відеотехніка, у тому числі техніка, що працює в автоматичному режимі, технічні прилади та технічні засоби з виявлення та/або фіксації правопорушень. Містить також поняття «інформація, отримана за допомогою фото- і відеотехніки, технічних приладів і технічних засобів», «матеріали фото- і кінозйомки, відеозапису.

про електронний носій інформації, що використовується для зберігання цифрової інформації (карта пам'яті або флеш-карта).

В Постанові КМ України «Про функціонування системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі» від 10.11.2017 р. згадується про технічні засоби (прилади контролю) [234].

Проведений нами аналіз ст. 245-1 КПК України вказує на те, що до технічних приладів, технічних засобів, з яких можуть бути зняті такі показання можна віднести будь-які прилади та засоби, які мають функцію фото-, кінозйомки, відеозапису і такий запис може здійснюватися як в автоматичному режимі, так і не в автоматичному режимі. Отже, фактично таким технічним приладом може бути і мобільний телефон, адже він має функцію фотозйомки та відеозапису. Цьому є підтвердження, уточнення міститься в нормі цієї статті (в тому числі і в автоматичному режимі). Тому дана слідча дія дає можливість отримувати докази, які раніше слідство отримувала шляхом витребування або добровільного надання (прикладом може бути правова позиція викладена у постанові ВС від 31.03.2021 р. (справа № 333/1539/16-к) щодо можливості отримання доказів шляхом їх добровільного надання слідству) [167].

На думку українського ученого В. М. Дубаса запровадження даної слідчої дії стало розширенням процесуальних можливостей слідчого, прокурора в здобутті доказів, хоча аналіз даної норми свідчить про її низьку кореляцію зі ст. 8 ЄКПЛ [74, с. 131].

Отже, можна дійти висновку, що показання технічних приладів і технічних засобів, що мають функції фото і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, які визначені самостійним процесуальним джерелом доказів у кримінальному провадженні щодо кримінальних проступків, є не чим іншим, як одним із видів електронних доказів. Аналіз наведених положень та правозастосувальної практики дає підставу стверджувати, що ці всі технічні прилади й технічні засоби зберігають інформацію в електронному

вигляді [260, с. 329–330]. Таку думку висловлюють також і інші науковці, зазначаючи, що процесуальна дія зняття показань техприладів і техзасобів полягає в копіюванні візуальної чи аудіовізуальної цифрової (електронної) інформації, а також, інших похідних метаданих з оригінального носія інформації на окремий носій інформації [138, с. 79].

На обґрунтування нашої позиції щодо необхідності викладення ст. 245-1 КПК в іншій редакції вважаємо за необхідне наголосити, що основоположний принцип, який забезпечує верховенство права – це принцип правової визначеності. Враховуючи мету для досягнення якої ця норма створювалася – підвищення ефективності досудового розслідування «за гарячими слідами», необхідно створити таку правову норму, яка б дійсно виконувала ту функцію, на яку розраховував законодавець та надавала можливість використовувати в якості доказу скопійовану в результаті даної слідчої дії інформацію в електронному вигляді.

У контексті такого елементу допустимості доказів як належний процесуальний порядок отримання доказів необхідно зазначити, що правозастосовна практика йде по шляху констатації необхідності застосування ст. 86 КПК України за умови коли такі процесуальні порушення прямо та істотно порушують права і свободи людини та/або надають підстави для сумніву у достовірності отриманих фактичних даних, які не видалося за можливе усунути в ході судового розгляду, що порушення належної правової процедури само по собі не веде до недопустимості доказів, а лише фундаментальних прав і свобод особи [283].

В цьому ж рішенні суд посилається на абз. 5 п. 3.2 мотивувальної частини рішення Конституційного Суду № 12-рп/2011 від 20.10.2011 р., яка визначає, що обвинувачення у вчиненні злочину не може бути обґрунтоване фактичними даними, одержаними в незаконний спосіб, а саме: з порушенням конституційних прав і свобод людини і громадянина; *з порушенням встановлених законом порядку,*

засобів, джерел отримання фактичних даних (курсив наш - І. Смаль); не уповноваженою на те особою тощо [241].

Аргументуючи висловлену думку, доцільно також згадати і правову позицію ВС, який у своєму рішенні від 14.03.2023 р. (справа № 135/638/21) [182].

В дисертаційному дослідженні "Інститут допустимості доказів як гарантія ухвалення законного та обґрунтованого вироку" (2015) В. В. Тютюнник зазначає, що законність отримання доказу включає в себе наступні критерії: 1) належний суб'єкт отримання доказу; 2) фактичні дані мають бути отримані тільки з джерел, перерахованих у законі;3) доказ повинен бути отриманий з додержанням правил проведення процесуальної дії, в ході якої отримано доказ; 4) під час отримання доказу повинні бути дотримані всі вимоги закону щодо фіксування ходу та результатів слідчої дії [242, с. 302; 281, с. 71]. Ці положення не викликають заперечень, і по суті, мають самоочевидний характер, адже відображають базові принципи кримінального процесуального доказування. Ми не просто з цим погоджуємося— це покладено в основу нашого підходу до аналізу С(Р)Д зняття показань технічних приладів та технічних засобів.

В судових рішення ВС від 11.07.2023 р. (справа №257/368/19) [188] та від 13.06.2023 р. (справа №520/2703/17) [187] також висловлена правова позиція щодо оцінки доказів з погляду допустимості.

В основі встановлених кримінальним процесуальним законом правил допустимості доказів лежить концепція, відповідно до якої в центрі уваги суду повинні знаходитися права людини і виправданість втручання в них держави незалежно від того, яка саме посадова особа обмежує права [156].

Важко не погодитися з висловленою думкою. В той же час рішення ВП ВС від 31.08.2022 р. (справа № 756/10060/17) розділило правників на два протилежні табори.

Частина правників стверджує, що порушення належної правової процедури само по собі не веде до недопустимості доказів і вважають, що визнаватися

недопустимими докази можуть тільки у випадку істотного порушення фундаментальних прав і свобод людини.

Однак є і протилежні думки правників, які стверджують, що Верховний Суд своєю постановою фактично розширив сферу застосування ст. 87 КПК, замінивши нею ст. 86 і поширивши необхідність оцінки істотності порушення прав на всі докази, навіть у випадках порушення порядку їх отримання ст. 87 КПК не може підміняти інші статті, зокрема й ст. 86, оскільки вона регулює лише один випадок недопустимості доказів – отримання внаслідок істотного порушення прав, тим часом як ст. 88 та 88-1 КПК регулюють інші випадки, як і ст. 86, яка регулює питання допустимості чи недопустимості доказів, залежно від дотримання порядку їх отримання, а не порушення прав під час їх отримання. «Навіщо взагалі встановлювати процедури проведення розслідування, якщо їх дотримуватись, очевидно, не обов'язково, принаймні якщо права порушуються не істотно? Адже можна було просто написати, що слідчі можуть збирати докази як завгодно, аби тільки не порушувались права людини… істотно» [119].

До речі, С. Кунянський в своїй статті «Що не так з поглядами Верховного Суду на допустимість доказів: досліджуємо за допомогою методу чесного читання» висловив думку, що одне із завдань кримінального провадження – застосування до кожного належних правових процедур. Всі норми КПК мають інтерпретуватися на розвиток, а не всупереч, зокрема, цьому завданню. І приходить до висновку, що недопустимими є докази: 1) недопустимість яких прямо встановлена законом (ч. 2, 3 ст. 87, ст. 88, 88-1 КПК); 2) отримані внаслідок істотного порушення прав та свобод людини (ч. 1 ст. 87 КПК); 3) отримані з порушенням порядку, встановленого КПК (ч. 1 ст. 86 КПК) [117].

Не заперечуючи важливість духу закону, оскільки він відображає його мету і ціль, вважаємо, що буква закону також є важливою, адже, закон повинен бути зрозумілим та конкретним, щоб уникнути спотикання при його застосуванні.

Частина 1 ст. 87 КПК визначає, що недопустимими є докази, отримані внаслідок *істотного порушення прав та свобод людини* (курсив наш - І. Смаль),

гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок істотного порушення прав та свобод людини [113].

В то же час в ч.2, 3 ст.87 КПК мова йде про безумовний обов'язок суду визнати недопустимими докази отримані в результаті істотного *порушення прав людини і основоположних свобод* (курсив наш - І. Смаль), тобто прав гарантованих Конвенцією про захист прав людини і основоположних свобод. Отже мова йде, зокрема, про докази, які хоча й отримані у порядку, встановленому КПК, але все одно мають визнаватися недопустимими.

Відповідна правова позиція міститься і у рішенні Верховного Суду «Критеріями допустимості доказів є: належне процесуальне джерело *(ч. 2 ст. 84 КПК містить вичерпний перелік процесуальних джерел доказів, який розширеному тлумаченню не підлягає)* (курсив наш - І. Смаль); належний суб`єкт збирання доказів (докази можуть бути зібрані тільки тими суб`єктами, які згідно з нормами КПК мають на це право); належна процесуальна форма *(встановлений КПК порядок здійснення кримінального провадження в цілому і проведення окремих процесуальних дій*) (курсив наш - І. Смаль). Суд звертає увагу на те, що кримінальне процесуальне законодавство містить критерії, за якими порушення встановленого КПК порядку проведення окремих процесуальних дій є істотним і призводить до визнання доказів недопустимими (частини 2 та 3 ст.87 КПК). Перелік діянь, які передбачені у ст. 87 КПК як підстави для визнання фактичних даних недопустимими як докази, не є вичерпним і становить собою порушення фундаментальних гарантій, що дає певний орієнтир для визначення змісту поняття «істотне порушення» у випадках, які не підпадають під цей перелік» [158].

М. С. Городецька констатує важливість дотримання процедури кримінального процесуального порядку в цілому та забезпечення прав учасників під час провадження зокрема [58, с. 402].

Повертаючись до аналізу ст. 245-1 КПК України, варто зазначити, що наукові дискусії викликало питання можливості проведення даної слідчої дії у кримінальних провадженнях як щодо злочинів, так і кримінальних проступків. Так, І. Гловюк та В. Завтур вважають, що ця слідча (розшукова) дія може проводитися як у кримінальних провадженнях щодо злочинів, так і щодо проступків, незважаючи на те, що в статті 245-1 КПК України там не згадується дізнавач [49].

Але тоді, на нашу думку, виникає логічне питання до законодавця: навіщо було виокремлювати результати даної процесуальної дії в межах проваджень про кримінальні проступки як окреме процесуальне джерело у ст. 298-1 КПК України?

Дещо іншою у цьому сенсі є позиція, що джерела доказів визначені ст.298-1 КПК можуть використовуватися щодо злочинів тільки на підставі ухвали слідчого судді [275, с. 132].

Зокрема, А. М. Соцький висловив аналогічну думку[36] [до примітки див. 266, с. 385–386]. Науковець при цьому зазначає, що редакція ст. 245-1 КПК України потребує доопрацювання, оскільки з даної норми вбачається, що дана слідча (розшукова) дія може проводитися тільки на підставі постанови слідчого (прокурора), тобто дізнавач не вправі її проводити [266, с. 385].

І. П. Зінковський висловив думку що зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису має ознаки слідчої (розшукової) дії; застосовне в обох формах досудового розслідування [78, с. 162].

Проте, з нашого погляду, вирішення цього питання вимагає необхідності виділення та аналізу двох аспектів. Перший аспект стосується правомірності проведення слідчої (розшукової) дій зняття показань технічних приладів та

---

[36] « показання технічних приладів і технічних засобів, що мають функції фото, кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису визнаються процесуальними джерелами доказів виключно при розслідуванні кримінальних проступків, а проводити таку слідчу дію може тільки дізнавач, а при розслідуванні злочинів дозволяється тільки на підставі ухвали слідчого судді, яка постановляється за клопотанням прокурора та приходить до висновку про необхідність ч. 2 ст. 84 КПК України доповнити новим джерелом доказів: показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису»[226, с. 385–386].

технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису у кримінальному провадженні щодо злочинів. Відповідно до конструкції ст. 245-1 КПК України дана С(Р)Д натепер може проводитися як у кримінальних провадженнях щодо кримінальних проступків, так і в кримінальних провадженнях щодо злочинів. По-перше, вказана стаття композиційно розміщена в главі 20 КПК, що присвячена питанням С(Р)Д дій. По-друге, такий висновок ґрунтується на положеннях ст. 40, 40-1 та ст.300 КПК, відповідно до якої для досудового розслідування кримінальних проступків дозволяється знімати показання технічних приладів і технічних засобів у провадженнях щодо вчинення кримінальних проступків, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису.

Ч. 2 ст. 84 КПК України визначає вичерпний перелік процесуальних джерел доказів. Показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису є джерелом доказів у кримінальному провадженні про кримінальні проступки (ст. 298-1 КПК України) і можуть бути використані у кримінальному провадженні щодо злочину тільки на підставі ухвали слідчого судді, яка постановляється за клопотання прокурора. Для нас логіка законодавця є незрозумілою. Як можна використовувати як процесуальне джерело доказів показання технічних приладів і технічних засобів, отримані слідчим в порядку ст. 245-1 КПК? Деякі науковці висловлюють думку, що такого роду докази можуть використовуватися й при розслідуванні злочинів (як різновид такого джерела доказів як документ) [14, с. 219].

Результатами здійснення процесуальної дії, передбаченої ст. 245-1 КПК, є документи як процесуальні джерела доказів, а сама ця дія за правовою природою є різновидом витребування речей і документів, що передбачене в ч. 2 ст. 93 КПК як спосіб збирання доказів незалежно від форми досудового розслідування [138, с. 85].

Відповідаючи на можливі заперечення опонентів, що в результаті проведення даної слідчої дії отримуються документи, які є процесуальними джерелами доказів

у кримінальних провадженнях щодо злочинів, поставимо питання наступним чином. Отже, потрібно проводити розмежування по суб'єкту отримання доказу? Якщо дізнавач проводить С(Р)Д в порядку ст. 245-1 КПК, то він отримує показання технічних приладів і технічних засобів, а якщо слідчий проводить аналогічну С(Р)Д – то документи?

Вчені А. П. Бегма, Г. В. Муляр, О. С. Ховпун вважають, що метою законодавця є розмежування джерел доказів, які можуть бути використані в доказуванні злочинів, а які – кримінальних проступків та звертають увагу відсутність чіткого законодавчого врегулювання питання «що саме ми можемо використовувати, формуючи доказову базу в кримінальних провадженнях» [12, с. 367].

Ми повністю поділяємо позицію науковців щодо необхідності вдосконалення законодавчого регулювання С(Р)Д , передбаченої ст.245-1 КПК України. Це дійсно є перспективним напрямом подальших наукових розвідок, оскільки окремі аспекти залишаються спірними й потребують чіткого нормативного врегулювання. Разом із тим, у межах даної дисертаційної роботи, з огляду на обмежений обсяг дослідження, не вбачається можливим зосередитися на розробленні та обґрунтуванні конкретних законодавчих змін у цьому напрямку.

Повернемося до другого аспекту, який стосується можливості проведення даної С(Р)Д до внесення відомостей до ЄРДР. Так, для з'ясування обставин вчинення кримінального проступку до внесення відомостей до ЄРДР може бути знято показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису (п. 3 ч. 3 ст. 214 КПК України). Тоді як бути з тим, що ч. 4 ст. 245-1 КПК України зазначає, що постанова слідчого, прокурора про зняття показань технічних приладів та технічних засобів повинна містити найменування кримінального провадження та його реєстраційний номер. Цікавою є думка вченого щодо необхідності розмежування застосування за темпоральною ознакою: до внесення у ЄРДР знімати показання технічних приладів і технічних засобів у провадженнях щодо

вчинення кримінальних проступків, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису за ст. 300 КПК України (яка процедуру такого зняття не регламентує), а після внесення відомостей до ЄРДР, керуючись ст. 245-1 КПК України, здійснювати слідчу (розшукову) дію – зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису у порядку, передбаченому цією статтею [78, с. 162].

Можливо виділити і третій аспект, який стосується ролі слідчого судді при вирішенні питання щодо можливості використання процесуальних джерел доказів, визначених ст. 298-1 КПК України у кримінальному провадженні щодо злочину.

Як відомо, до повноважень слідчого судді належить здійснення судового контролю за дотримання прав, свобод і інтересів осіб у кримінальному провадженні у порядку, передбаченому КПК України. Тобто, можна говорити про те, що в ч. 2 ст. 298-1 КПК України констатовано про неможливість використання у кримінальному провадженні щодо злочинів процесуальних джерел визначених ч. 1 ст. 298-1 КПК України без відповідної ухвали слідчого судді, однак в процесуальному законодавстві не встановлений порядок розгляду такого клопотання прокурора. На наш погляд, повинна бути в процесуальному законодавстві норма, яка б регламентувала порядок розгляду таких клопотань та крім іншого, містила положення щодо можливість відмови у задоволенні такого клопотання, якщо прокурор не доведе законність отримання такого доказу та необхідність його використання у кримінальному провадженні щодо злочину. Адже судовий контроль повинен містити оцінку дотримання прав, свобод і інтересів осіб при проведенні, зокрема, такої С(Р)Д як зняття показань.

Таким чином, можна погодитися з думкою вчених А. П. Бегми, Г. В. Муляра, О. С. Ховпуна, що невідповідність вказаних норм щодо джерел доказів викликає певну правову колізію та потребує уточнення [12, с. 367].

Однією з гарантій забезпечення прав і законних інтересів учасників кримінального провадженні є чітка регламентація діяльності суб’єктів

кримінального процесу. Наявність колізій у кримінальному процесуальному законодавстві приводить до появи неоднозначної практичної діяльності. Повністю розділяємо позицію науковців, які вважають, що показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису не можуть бути використані у кримінальному провадженні щодо злочину, окрім як на підставі ухвали слідчого судді, яка постановляється за клопотанням прокурора. Таким чином, висловимо обґрунтовані сумніви щодо можливість використання як доказів фактичних даних отриманих в результаті «зняття показань» у кримінальних провадженнях щодо злочинів, які першочергово були внесені в ЄРДР з правовою кваліфікації як злочини, а не кримінальні проступки. Тоді, в свою чергу, фактичні дані отримані з порушенням встановлених законом порядку, засобів, джерел отримання не можуть бути доказами.

Навіть вибірковий аналіз судової практики застосування судами приписів ст. 245-1 КПК України дозволяє стверджувати, що суди по різному тлумачать положення цієї статті у сенсі можливості застосування показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису як джерела доказів у кримінальному провадженні щодо злочинів. Як вбачається з судової практики слідчий суддя відмовляє в задоволенні клопотання слідчого про надання тимчасового доступу до речей та документів у кримінальних провадженнях щодо злочинів мотивуючи тим, що копії відеозапису, що здійснено в публічно доступному місці необхідно отримувати в порядку передбаченому ст. 245-1 КПК України на підставі постанови прокурора [310; 311; 314; 323; 325; 340].

З ухвали слідчого судді вбачається, що накладено арешт на оптичний компакт-диск, на якому містяться відеозаписи з камери відеоспостереження, який на підставі постанови слідчого про зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису було отримано в порядку ст. 245-1 КПК України.

Дана ухвала виносилася у кримінальному провадження внесеному в ЄРДР за ознаками злочину [306; 316].

Клопотання про тимчасовий доступ до речей та документів у кримінальному провадженню за ч. 1 ст. 286 КК (кримінальний проступок) задоволено з мотивів, що отримання тимчасового доступу до речей та документів, а саме до відеозаписів з камер відеонагляду у вказаний вище спосіб, не суперечить вимогам ст. 245-1 КПК України [336].

Відмовлено дізнавачу у задоволенні клопотання про тимчасовий доступ до речей та документів, оскільки не надано жодних відомостей, які б давали обґрунтовані підстави вважати, що дізнавач вживав заходів для отримання зазначених відеозаписів у особи, яка ними володіє, та відсутність обґрунтування труднощів їх отримати у визначений КПК України спосіб, в порядку, передбаченому ст. 245-1 КПК України [343].

За результатами аналізу більше ніж 60 судових рішень, можна сказати, що здебільшого суди вважають, що ст.245-1 КПК України може застосовуватися як в кримінальних провадженнях щодо злочинів так і кримінальних проступків.

Як приклад протилежної судової практики можна привести наступні судові рішення. Вироком суду відеозапис був визнаний недопустимим доказом з обґрунтуванням, що він виданий свідком, тобто здобутий стороною обвинувачення всупереч вказаного імперативного порядку визначеного ст. 245-1 КПК без наявності постанови слідчого чи прокурора. Сторона обвинувачення не спростувала належними доказами посилання обвинуваченого про фальсифікацію відеозапису [36]. Тобто, в даному судовому рішенні суд зазначає про обов'язок саме сторони обвинувачення доводити достовірність доказу який вона надає і не перекладає такий обов'язок на сторону захисту[37] [див. до примітки 302]. В іншій

[37] В ухвалі Пустомитівського районного суду Львівської області від 01.02.2024 р (справа №450/4548/23) суд зазначив про безпідставність доводів захисника щодо недопустимості як доказу протоколу зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису та матеріального носія, на якому містяться відео-файли з підстав порушення ч.5 ст.245-1 КПК України, оскільки спеціаліст та слідчий були відсутні при копіюванні власником інформації з відповідних приладів [253]

судовій справі (№211/3934/22) клопотання про визнання недопустимими доказів за відсутності протоколу зняття показань в порядку ст. 245-1 КПК не задоволено з обґрунтуванням, що є протокол огляду відеозаписів наданих на підставі постанови слідчого[38] [33; до примітки див. 45]. На нашу думку, такі дії виходять за межі порядку проведення слідчої дії, визначеної ст.245-1 КПК України.

Аналіз судової практики крізь призму порушеної проблеми дозволяє зробити висновок про можливість виникнення парадоксальної ситуації, яка за діючого регулювання нормами КПК України не може бути належним чином вирішена. Як у кримінальних провадженнях внесених у ЄРДР з правовою кваліфікацією як злочини можна використовувати «показання технічних приладів і технічних засобів…, як належне процесуальне джерело? В цьому контексті вважаємо за необхідне обґрунтувати необхідність внесення змін до КПК України. Як уже неодноразово нами зазначалося, використання електронних доказів у кримінальних провадженнях потребує вироблення особливих процесуальних правил та стандартів. Дотримання законності неможливо без існування належної законодавчої регламентації.

Таким чином, на підставі аналізу кримінального процесуального законодавства України та наукових підходів до розуміння поняття та сутності зняття показань технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису можна зробити висновок, що для того, щоб фактичні дані стали доказами вони мають набути властивості допустимості. А саме, вони мають бути отримані належним суб’єктом доказування, належним способом збирання доказів та з належного джерела доказів. Збирання доказів за допомогою дослідження інформації в електронному вигляді потребує вироблення особливих процесуальних правил та стандартів, які б

---

[38] З вироку Тернопільського міськрайонного суду Тернопільської області від 27.12.2023 року справа № 607/16549/23 вбачається, що слідчий під час проведення С(Р)Д в порядку ст.245-1 КПК України перейшов за посиланням, яке вказане у відповіді на запит, на хмарне сховище Google Drive, і в файловому каталозі цього хмарного сховища знайшов та скачав до пам`яті персонального комп`ютера, а надалі провів збереження та запис на оптичний диск відеозаписи.

враховували особливості «електронних доказів». Відсутність законодавчо закріпленого єдиного підходу до отримання електронних доказів на практиці приводить до неналежної фіксації, вилучення та оцінки.

Хоча в межах нашого дослідження не ставилося за мету розроблення окремого законопроєкту, однак окремої уваги потребує термінологічне визначення, що вжите в статті 245-1 КПК України. Вважаємо, що результат даної С(Р)Д полягає в отриманні інформації в електронному вигляді, що зафіксована технічними приладами та технічними засобами в автоматичному режимі і тому ми пропонуємо зміни до ст. 245-1 КПК України, зокрема в частині необхідності термінологічного уточнення —замість «зняття показань технічних приладів та технічних засобів» використовувати поняття «отримання електронних даних з технічних приладів та технічних засобів» та до ст.3 КПК України, доповнивши її визначенням терміна «електронні дані» — це інформація в електронному вигляді, яка придатна для сприйняття людиною після обробки автоматичними програмними засобами (див. додаток Г).

3.2. Інваріантність понять «оригінал», «дублікат», «копія» в нормативному регулюванні та правозастосовній практиці

Питання щодо використання понять «оригінал», «дублікат», «копія» у контексті електронного документа та електронних доказів є одним з найбільш дискусійних. Погляди як науковців так і практиків є досить різними і цьому, на нашу думку, сприяє відсутність чіткого визначення даних категорій як у кримінальному процесуальному законодавстві, так і в профільному законі «Про електронні документи та електронний документообіг». На цьому наголошує також і А. В. Скрипник, досліджуючи категорії «оригінал», «дублікат», «копія» у контексті цифрової інформації [250, с. 104].

Поглянемо на ці поняття з точки зору теоретичних поглядів, нормативного закріплення та практичних напрацювань.

Як ми зазначали в розділі 1 принциповими відмінностями традиційних доказів від електронних є середовище їх існування. І саме відмінності аналогового й електронного середовищ існування впливає на досліджувані категорії, що найбільш яскраво проявляється у кожній з двох можливих форм існування електронного документа: статичній (під час зберігання у пам'яті) і динамічній (під час зчитування збережених сигналів) [250, с. 106–107]. Так, деякі науковці стверджують, що електронні документи за стадіями виготовлення також як і паперові можна поділити на оригінали, дублікати, копії та виписки [237, с. 45; 352, с. 207].

Інформація в електронному вигляді, яка безпосередньо записується у процесі проведення слідчих дій є оригіналом. Інформація, яка копіюється на інші носії, вже не є оригіналом – вона називається копією [110, с. 70].

Таким чином, оригінал електронного доказу – це фактично документ, який створений першим і до якого не вносилися зміни. Копія цього документа – це документ, який створений пізніше і до якого вносилися зміни, пов'язані тільки з його копіюванням.

А. В. Скрипник у своєму дисертаційному дослідженні приходить до висновку, що оригінали, дублікати і копії можуть існувати у цифровому середовищі; вказані категорії (оригінал, дублікат, копія) є актуальними лише для динамічної форми існування документу (під час зчитування), у той час як у статичній (під час зберігання) конфігурація фізичних даних на машинних носіях на цифрову інформацію не впливає [250, с. 109].

Цивіліст О. Ю. Гусєв до визначення оригіналів електронних доказів застосовує три підходи: матеріалістичний, компонентний та інтерперсональний. Відповідно до першого підходу поняття оригіналу електронного доказу слід вважати беззмістовним, якщо електронними доказами визнається лише інформація, а не форма її вираження. Відомості доказового характеру не можуть існувати окремо від матерії, використання терміна «копія» стосовно електронних доказів

видається некоректним, отже відповідно є недоречним вживання терміну «оригінал» до об’єкта, з якого не можна зробити «копію» [62, с. 100, 106].

Тобто, науковець фактично заперечує існування поняття «оригінал» по відношенню до електронних доказів.

Другий підхід з погляду О. Ю. Гусєва дозволяє за певних обставин встановити оригінальність електронного доказу на підставі його реквізитів [62].

Такий підхід, на нашу думку, можна застосувати до електронного документа, поскільки відповідно до нормативних документів, а саме Закону «Про електронні документи та електронний документообіг», такий документ має обов’язкові реквізити.

А третій, з погляду дослідника – пов’язує можливість визначення оригіналів електронних доказів із особистим ставленням учасників справи до них. На думку автора такий підхід проявляється у формулюванні законодавцем ч. 3 ст. 99 КПК [62, с. 100, 106].

Отже, О. Ю. Гусєв пропонує відмовитися від вживання терміна «оригінал» стосовно електронних доказів узагалі. Винятки можливі лише для норм, присвячених таким формам цифрових даних, які можуть мати обов’язкові реквізити, а саме для електронних документів [62, с. 106].

Вживання термінів «оригінал», «дублікат» і «копія» стосовно електронних доказів є умовним вважає С. Й. Гонгало [51, с. 96].

Аналогічно міркує і А. Ю. Каламайко, зазначаючи про відсутність поняття «оригіналу» електронних засобів доказування в силу повної ідентичності електронних копій. В контексті електронних засобів доказування неможливо вести мову про «оригінал» у звичному розумінні, оскільки всі електронні копії є ідентичними [84, с. 61–62]. Або навпаки, Ю. С. Павлова озвучує думку про відсутність поняття копій електронних доказів [146, с. 107].

Інші дослідники, С. О. Чорний, О. І. Антонюк розрізняють копію електронного доказу, під якою пропонують розуміти «створений електронними (цифровими) засобами або відтворений візуально на папері примірник

електронного доказу, що відповідає оригіналу та засвідчений у встановленому законом порядку» [359, с. 87].

На думку О. Ю. Гусєва навіть копія з копії електронного документа може вважатись оригіналом [62, с. 99].

Оригіналом електронного доказу буде об’єкт, первинно створений у відповідному середовищі, його електронними копіями – примірники, створені шляхом відтворення оригіналу об’єкта. Тобто, оригіналом є об’єкт, який містить виражену в ньому інформацію та первинні метадані, пов’язані з його створенням і використанням, копією – об’єкт, який відтворює виражену в оригіналі інформацію та може частково відтворювати первинні метадані й одночасно містить власні, незалежні від первинних метадані. Таким чином, електронні докази характеризуються наявністю їх оригіналів та електронних копій, які розмежовуються за їх метаданими, вважає А. Штефан [366, с. 68].

Деякі автори, наголошуючи на умовності виокремлення оригіналу та копію по відношенні до електронних доказів пропонують визнавати усі екземпляри електронного документа оригіналами, які відрізнятимуться лише датою створення.

Зокрема, А.-М. Ангеленюк висловлює думку щодо допустимості копії електронного доказу виготовленої без участі спеціаліста якщо відсутні ознаки втручання з метою зміни відомостей після моменту виготовлення копії. При цьому вчена вважає, що копія електронного доказу не може бути допустимим доказом факту чи обставин, на доведення яких вона надана, якщо відомості, які вона містить не підтверджується іншими доказами, визнаними допустимим» [4, с. 217].

Уявляється, все ж слід критично поставитися до ідей автора, оскільки вони не позбавлені недоліків, адже складно уявити яким чином буде встановлюватися відсутність ознак втручання.

Після висвітлення поглядів залишається враження того, що кожен з них не позбавлений раціонального зерна. Проте для правозастосування є неприйнятною полярність думок. Спробуємо обміркувати викладене попередньо.

З позицію закону де юре звернемося до законодавства, яке регулює надання у кримінальному провадженні як доказу електронного документа.

Однак, перед цим хочемо наголосити, що не будь-який електронний документ може бути доказом в кримінальному процесі. По-перше, електронний документ повинен містити в собі інформацію (відомості), які встановлюють наявність чи відсутність обставин, що мають значення для кримінального провадження та підлягають доказуванню. По-друге, він повинен містити в собі інформацію, яка зберігається на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет), що дає можливість доступу до такої інформації в будь-який момент. По-третє, електронний документ повинен бути отриманий з дотриманням процесуальних правил збирання доказів [141, с. 123].

Стаття 99 КПК України визначає, що процесуальним джерелом доказів є оригінал документа. Оригіналом електронного документа є його відображення, якому надається таке ж значення як документу.

Отже, законодавець оригіналом електронного документа вважає його відображення, однак при цьому не конкретизує форму такого відображення.

Погоджуємося з думкою А. В. Скрипника, який зазначає «власне суперечність полягає у такому: якщо розуміти під відображенням форму представлення цифрової інформації, доступну для сприйняття людиною змісту, то випливає, що оригінал електронного документа: а) є аналоговим, тобто доступний для безпосереднього сприйняття людиною; б) не є єдиним. Описана неузгодженість дозволяє поставити під сумнів доцільність запровадження категорії «оригінал електронного документа» у такому вигляді» [250, с. 102].

Візуальною формою подання електронного документа є відображення даних, які він містить, і таке відображення може бути двома способами (ч. 4 ст. 5 Закону України «Про електронні документи та електронний документообіг»):

1) електронними засобами у формі, придатній для приймання його змісту людиною;

2) на папері у формі, придатній для приймання його змісту людиною (ч. 4 ст. 5 Закону України «Про електронні документи та електронний документообіг») [223].

Як ми вже зазначали, досліджуючи правову природу електронного доказу і його характерні властивості, головною відмінністю електронного документу від традиційного є відсутність жорсткої прив'язки до матеріального носія і відповідно можливість існувати на декількох носіях одночасно та миттєво передаватися по комунікаційним каналам зв'язку.

Аналіз норм Закону України «Про електронні документи та електронний документообіг» дає нам підстави стверджувати, що у разі зберігання електронного документа *його автором* (курсив наш - І. Смаль) на кількох електронних носіях інформації або надсилання його декільком адресатам, то кожний із його примірників вважається оригіналом електронного документа.

На нашу думку, яка в подальшому буде обґрунтована більш детально, електронний документ створений автором є його оригіналом, навіть у випадку його існування на різних матеріальних носіях, однак якщо під час проведення слідчих (розшукових), негласних слідчих (розшукових) дій чи під час тимчасового доступу до речей і документів здійснюється копіювання такого документа, то мову можна вести про копію електронних доказів, в тому числі і електронного документа, а не його оригінал.

Стаття 8 Закону України «Про електронні документи та електронний документообіг» від 22. 05. 2003 р. № 851-IV хоч і має назву «Правовий статус електронного документа та його копії» фактично не розкриває зміст поняття щодо статусу копії електронного документа.

Також хочемо звернути увагу в цьому аспекті на те, що законодавець визначає оригіналом електронного документа електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або

підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги» [223].

В зв'язку з цим постає питання чи можна категорії «оригінал», «копія», «дублікат» в їхньому традиційному значенні поширювати на інформацію в електронному вигляді, електронні докази.

Так, в розділі 1, досліджуючи ознаки електронних доказів, одними з характерних нами було виділено мобільність, трансльованість, відсутність прив'язки до конкретного матеріального носія, які свідчать про те, що цифрові об'єкти можуть існувати в декількох місцях одночасно.

У загальному розумінні оригінал – це «те, що є основою для відтворення, копіювання, переробки» [254, с. 744], копія – «точне відтворення чого-небудь, що цілком відповідає оригіналові» [253, с. 283]; дублікат, другий примірник документа, що має таку саму юридичну силу, як і оригінал [23, с. 50].

Національний стандарт із діловодства та архівної справи ДСТУ 2732:2004 під оригіналом документа розуміє його примірник, який першим набуває юридичної сили [70].

Відповідно до пункту 3.10 ДСТУ 2732:2004 копія (документа) – це документ, що містить точне знакове відтворення змісту чи документної інформації іншого документа і в окремих випадках деяких його зовнішніх ознак [70].

Дублікат оригіналу (службового документа) – повторно оформлений службовий документ для використовування, замість втраченого чи пошкодженого оригіналу, що має таку саму юридичну силу [70].

Сучасний міжнародний стандарт у сфері електронного документообігу ISO 12651-1:2012 визначає оригінал електронного документа як електронне зображення (цифрове представлення цього документа), що використовується для створення дублікатів [402].

Звичайно терміни «копія» і «дублікат» не є синонімічними. Разом з тим, слід зазначити, що КПК у ч. 4 ст. 99 надає автономне визначення поняття «дублікат документа» як документа, виготовленого таким самим способом, як і його оригінал.

Однак, на нашу думку таке визначення не можна застосувати до інформації в електронному вигляді, адже її не можна виготовити «таким самим способом» як і був виготовлений оригінал, оскільки такий документ буде містити інші метадані, про що ми поговоримо далі.

Отже, на нашу думку, оригіналом електронного документа є інформація в електронному вигляді створена, збережена, направлена *її автором* (курсив наш - І. Смаль), яка має обов'язкові реквізити, в тому числі електронний підпис автора або електронний підпис і печатку.

Утім, якщо дізнавач, слідчий, прокурор, спеціаліст, який залучається до певної слідчої дії здійснює копіювання файла на інший носій, то це буде копія електронного документа. Це не може бути оригіналом електронного документа, а тим паче його дублікатом. Оригіналом електронного документа може бути тільки електронний документ при наявності обов'язкового реквізиту – підпису (це може бути електронний підпис автора, кваліфікований електронний підпис, удосконалений електронний підпис). На наше переконання дублікат електронного документа, як і будь-якого документа повинна виготовити саме та особа, яка створила оригінал, але і в даному випадку такий документ не можна назвати дублікатом, оскільки він матиме, як ми вже зазначали інші метадані.

Щодо можливості використання копії електронного доказу (копії інформації в електронному вигляді) то законодавець визначає наступні умови.

Як вбачається з конструкції ч. 4 ст. 99 КПК України для того щоб копія інформації, в тому числі комп'ютерних даних (в новій редакції закону) могли бути використані як докази, повинні бути дотримані три умови. По- перше, така інформація повинна бути виготовлені прокурором, слідчим (дізнавачем). По-друге, такі докази повинні бути виготовлені обов'язково із залученням спеціаліста. І по-третє, визнані судом як оригінал доказу. Необхідність визнання судом оригіналом копії інформації фактично є правовою фікцією (лат. - вигадка, вимисел) – прийом, за допомогою якого в статті закону неіснуючий факт оголошується існуючим і

набуває юридичного значення [24, с. 902], в цьому ми повністю погоджуємося з думкою науковця А. В. Скрипника [250, с. 107].

Крім того, з даної норми права (ч.4 ст.99 КПК України) можна зробити також наступні висновки: в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах міститься як інформація, так і комп'ютерні дані. З п. 1 ч. 2 ст.99 КПК прослідковується наступний висновок: комп'ютерні дані – це носії інформації. Такими ж носіями інформації законодавець вважає матеріали фотозйомки, звукозапису, відеозапису. Також в в даній правовій нормі мова йде і про носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії (п. 3 ч. 2 ст. 99 КПК).

Наразі проаналізуємо норми кримінального процесуального законодавства, в яких йде мова про виготовлення копій інформації.

Стаття 168 КПК містить норму, яка передбачає виготовлення слідчим чи прокурором копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста[113].

Про *зняття копії інформації* (курсив наш - І. Смаль) мова також йде в ч. 1 ст. 159 КПК, яка передбачає зняття копії інформації, що міститься в електронних інформаційних систем, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку при застосування такого заходу забезпечення кримінального провадження як тимчасовий доступ до речей і документів [113]. Зі змісту цієї статті вбачається, що копіювання такої інформації здійснюється *без обов'язкової участі спеціаліста* (курсив наш - І. Смаль).

В ч. 5 ст. 245-1 КПК України мова йде про копіювання відповідних записів показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису. Таке копіювання може здійснюватися такими способами: а) у присутності слідчого,

прокурора шляхом самостійного копіювання особою, яка є власником або володільцем відповідних приладів та засобів; б) копіювання такою особою за участю спеціаліста відповідних записів на носії, які надаються слідчим, прокурором; в) надання таких копій на носіях, особи, яка є власником або володільцем відповідних приладів та засобів.

Детальний аналіз такої слідчої дії як зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапис був зроблений нами у підрозділі 3.1, однак зауважимо стаття 245-1 КПК України передбачає залучення спеціаліста тільки за необхідності.

І в цьому контексті, постає питання щодо можливості використання копії інформації отриманої без участі спеціаліста в порядку ч. 5 ст. 245-1 КПК та ч. 1 ст. 159 КПК в якості процесуального джерела доказу (документа), адже ч. 4 ст. 99 КПК визначає, що тільки *копії інформації виготовлених* слідчим, прокурором *із залученням спеціаліста* визнаються судом *як оригінал документа* (курсив наш - І. Смаль) .

Також копії документів можуть бути отримані в результаті проведення НС(Р)Д (ст. 256 КПК). В нормах даної статті зазначено, що аудіо- або відеозаписи, фотознімки, інші результати, здобуті за допомогою застосування технічних засобів, вилучені під час їх проведення речі і *документи або їх копії* (курсив наш - І. Смаль*)* можуть використовуватися в доказуванні на тих самих підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового розслідування. А саме ст. 99 КПК передбачає підстави прийняття як доказів документів: надається оригінал документа; дублікат документа; копія інформації виготовлена прокурором, слідчим із залученням спеціаліста. До речі, під час проведення негласних слідчих (розшукових) дій копії такої інформації виготовляються оперативним співробітником.

Досить цікаво викладена норма ст. 257 КПК про те, що *отримана інформація* (курсив наш - І. Смаль) може бути використана в іншому кримінальному

провадженні; що *передання інформації* (курсив наш - І. Смаль), яка була одержана внаслідок проведення НС(Р)Д, здійснюється тільки через прокурора. Зрозуміло, що на практиці для того, щоб передати *таку інформацію* (курсив наш - І. Смаль), необхідно здійснити її копіювання на інший носій, адже інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (відповідно до Закону України «Про інформацію» та ст. 200 ЦК України) [230; 254].

Як показує наш практичний досвід, клопотання прокурора, яке подається слідчому судді в порядку ст. 257 КПК, взагалі не містить інформації про порядок виготовлення копії такої інформації, підтвердження порядку такого копіювання не надається також і в судовому засіданні під час розгляду кримінального провадження.

Також в аспекті дослідження понять «оригінал», «копія», «дублікат» необхідно звернути на появу ще одного поняття, як то «примірник». Так ч. 3 ст. 106-1 КПК містить норму «матеріали досудового розслідування, що містяться в інформаційно-телекомунікаційній системі досудового розслідування, передаються, їх копії чи *примірники* (курсив наш - І. Смаль) надаються в електронній формі, а за рішенням слідчого, дізнавача, прокурора, слідчого судді, суду, які їх передають чи надають, - у паперовій формі» [113].

Фактично законодавець веде мову про копію та примірник матеріалів досудового розслідування, але при цьому не зазначає яким чином буде підтверджена їх автентичність і що таке «примірник» в контексті матеріалів кримінального провадження.

Частина 4 ст. 106-1 КПК є ще одним прикладом правової фікції. Визнаються оригіналами документів (до речі, якщо в ч. 4 ст. 99 КПК зазначено, що це «визнання оригіналом документа» робить суд, то дана норма не визначає хто ж все таки «визнає оригіналом» наступні документи: документи, підписані, погоджені в інформаційно-телекомунікаційній системі досудового розслідування з використанням кваліфікованого електронного підпису; *примірники* (курсив наш - І.

Смаль) документів, підписані, погоджені в інформаційно-телекомунікаційній системі досудового розслідування з використанням кваліфікованого електронного підпису *в електронній формі* (курсив наш - І. Смаль); *примірники* (курсив наш - І. Смаль) документів, підписані, погоджені в інформаційно-телекомунікаційній системі досудового розслідування з використанням кваліфікованого електронного підпису *в паперовій формі* (курсив наш - І. Смаль) [113].

Прикметним є те, що ч. 5 ст. 106-1 КПК має відсилку до законодавства щодо електронних документів та електронного документообігу в частині, коли обіг електронних документів у кримінальному провадженні не врегульований КПК. Але як ми зазначали вище, ЗУ «Про електронні документи та електронний документообіг» навпаки містить норму, яка для підтвердження автентичності копію відсилає до іншого законодавства «електронна копія електронного документа засвідчується у порядку, встановленому Законом України "Про електронну ідентифікацію та електронні довірчі послуги".

«Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством» (ч. 6 ст. 7 ЗУ «Про електронні документи та електронний документообіг») [223]. На нашу думку, ця норма як раз є посилом для законодавця ввести в КПК відповідні норми щодо визначення процедури для підтвердження справжності документа, тобто його автентифікації.

Нам незрозуміло навіщо вигадувати таку складну конструкцію з визнанням оригіналом документів. На нашу думку, більш логічно, доцільно і зрозуміло було б визначити в процесуальному кодексі можливість надання не тільки оригінала інформації в електронному вигляді, але і її копії. Однак, при цьому необхідно надати чітке визначення в КПК, що таке оригінал електронного документа, що таке його копія, а враховуючи, що електронний документ є тільки одним із видів електронних доказів також надати загальне визначення цього поняття. І відповідно необхідно в КПК ввести норму, яка б визначала яким чином повинна підтверджуватися відповідність копії оригіналу .

З проведеного анкетування вбачається: 37 % респондентів вважають за необхідне подання саме оригіналу носія інформації в електронному вигляді, із них 42 % суддів, 28 % прокурорів, 43 % слідчих (дізнавачів), 20 % адвокатів; 39 % респондентів вважають за можливе подання копії інформації в електронному вигляді; 40 % вважають за необхідне подання копії такої інформації, але виготовленої спеціалістом (Додаток Б, питання 13).

Незрозумілим також, на нашу думку, викладення ч. 4 ст. 99 КПК саме в такій редакції, а саме як може вплинути на «оригінальність» такої інформації якщо її виготовить саме слідчий, прокурор, але із залученням спеціаліста.

Також з конструкції ч. 4 ст. 99 КПК вбачається, що законодавець визнає, що електронний документ крім інформації містить ще і комп'ютерні дані, а враховуючи різноплановість цих понять (Закон України «Про електронні документи та електронний документообіг» визначає дані як інформацію, яка подана у формі, придатній для її оброблення електронними засобами (ст. 1); можна стверджувати, що у законодавця немає чіткого розуміння, що є фактично носієм інформації, а також що він розуміє під поняттям «комп'ютерні дані» і як на практиці повинні розмежовуватися ці категорії. Щодо поняття «комп'ютерні дані» нами це більш детально досліджувалося в розділі 1.

Як ми зазначали вище на розгляді у ВР знаходиться законопроєкт «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» № 4004 від 01.09.2020 р. (з розгляду не знятий), в якому пропонується внести окрему главу щодо електронних доказів [219]. З наукової точки зору буде корисним звернутися до аналізу положень, які регулюють питання щодо «оригіналу», «дублікату» та «копії» електронних доказів.

Так, ч. 3 ст. 100-1 КПК (у редакції проєкту) встановлює, що сторони кримінального провадження, потерпілий, представник юридичної особи щодо якої здійснюється провадження зобов'язані надати суду електронний доказ в *оригіналі або в електронній копії* без порушень його цілісності та справжності [219].

На нашу думку, така альтернативність є виправданою, оскільки по-перше, визначена процесуальним законом вимога щодо подання оригіналів електронних доказів не в усіх випадках має дійсне практичне значення; по-друге, подання оригіналів електронних доказів не в усіх випадках є можливим. Однак, в даній нормі законопроєкта процесуально не визначено критерії, на підставі яких можна було б установити, оригіналом чи копією є той або інший електронний доказ [110, с.70]. Пропозиції, які містяться в даному законопроєкті є недостатньо чіткими, зрозумілими і однозначними, а отже не відповідають принципу верховенства права. Крім того, не визначено як буде підтверджуватися відсутність порушення цілісності та справжності, щоб у сторін кримінального провадження, потерпілого, представника юридичної особи щодо якої здійснюється провадження не виникало жодних сумнівів.

Відповідно до ч. 4 ст. 100-1 КПК (у редакції проєкту) оригіналом електронного доказу є *його відображення*, якому надається таке ж значення, як процесуальному джерелу доказів [219]. Таке формулювання по-перше, ставить під сумнів, що електронний доказ є процесуальним джерелом доказу (хоча ч.2 ст. 84 законопроєкту електронні докази відносить до процесуального джерела доказів) і по-друге, ця норма знову залишає поняття «відображення електронного доказу»,яке є доволі спірним та невизначеним.

Одночасно у ч. 6 ст. 100-1 КПК (у редакції проєкту) зазначається про те, що копія електронного доказу, виготовлена слідчим, прокурором із залученням спеціаліста, визнається судом як оригінал електронного доказу [219]. Тобто, фактично як і у чинному КПК залишається правова фікція «визнання судом копії електронного доказу оригіналом». І крім копії електронного доказу, суд визнає оригіналом ще й копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як електронний доказ (ч. 2 ст. 100-1 КПК проєкту) [219].

Варто зауважити, що в ч. 3 ст. 100-1 КПК проєкту містить поняття електронний доказ в електронній копії, в той же час ч.7 цієї ж статті говорить про копію електронного доказу.

Незрозумілими залишаються також і питання: що ж варто вважати носієм «інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах» [250, с. 102].

С. В. Собур вважає, що законодавець розглядає поняття «матеріальні носії» як більш широке та включає до його змісту поняття «електронні носії» [264, с. 44–48].

А. В. Скрипник вважає найбільш вдалим такий терміновжиток: машинні носії, накопичувані цифрових даних, носії для збереження цифрових даних, носії цифрових даних – для позначення технічних засобів, призначених для передачі цифрових сигналів у часі і просторі; носій цифрової інформації – для позначення файлу [250, с. 82].

У вітчизняному законодавстві також вживається термін «електронні носії». Так в ч. 1 ст. 13 Закону України «Про електронні документи та електронний документообіг» зазначено: «Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації» [223]. Поняття «електронні носії» не конкретизується.

Фахівці експерти відмічають, що найбільш універсальним способом зберігання цифрової інформації є файл. Копіювання файлів здійснюється за допомогою операційної системи. З точки зору судової експертизи відео-, звукозапису копія могла вважатися дублікатом, якщо б вона могла відповідати таким умовам: це повинна бути точна цифрова репродукція всіх інформаційних об'єктів, що зберігаються на оригінальному матеріальному носієві; юридичне походження наданої цифрової репродукції [269, с. 166].

Необхідно розуміти, що самі по собі дані (комп'ютерні чи електронні) не можуть бути документами. Ці дані не можуть існувати окремо від матеріального

носія інформації (жорсткого диску, флеш-носія і т.п.), на якому вони зафіксовані. Тобто, документами необхідно вважати не відомості (дані), а носії інформації у різних формах, на яких ці дані зафіксовані, вважає О. П. Метелев [126, с. 93].

Ми можемо погодитися з такою точкою зору науковця при умові, що таким носієм інформації буде визнаний файл.

З погляду А. В. Скрипника утворюється цифрова тріада: носій цифрових даних (машинний носій) – джерело цифрового доказу (носій цифрової інформації – файл) – цифровий доказ (інформація) [251, с. 111–112].

В свою чергу А. Ю. Каламайко стверджує, що електронний документ має специфічну природу (не матеріальну, а електронну), відповідно й носій електронного документа має свої особливості, що потрібно враховувати при вивченні всіх його складових елементів, у тому числі й носія [84, с. 53].

Досить цікавим є диференційований підхід А. В. Скрипника, який передбачає виділення цифрових оригінала, дубліката і копії. На його думку, цифровий оригінал – а) для електронного документа – файл з електронним підписом; б) для іншої цифрової інформації – файл, створений найпершим з представлених, до якого не вносилися зміни, не пов’язані із його створенням [250, с. 117].

Погоджуючись з вищенаведеним підходом, який на нашу думку є достатньо логічним, чіткий як з точки закону, який застосовується де факто, так і de lege ferenda – з точки зору закону, прийняття якого бажане, все ж таки не вважаємо логічним визначення поняття дубліката. Так, А.В.Скрипник під дублікатом розуміє « файл, створений пізніше за оригінал, але зміни до якого були внесені тільки у зв’язку з копіюванням» [250, с. 117].

Для електронного документа, на нашу думку, ця категорія позбавлена смислу: якщо документ міститиме електронний підпис, то це оригінал; якщо ні, то це копія, а не дублікат, поняття «дублікат» не може бути застосовано також і до електронних доказів. Адже дублікат, як ми вже зазначали, – це повторно оформлений документ замість втраченого чи пошкодженого оригіналу, що має таку

саму юридичну силу [70]. Тобто цілком логічно і зрозуміло, що дублікат може виготовити тільки особа яка створила оригінал такого документа. Тому, на нашу думку, існування поняття дублікат позбавлене смислу не тільки до електронних документів, а й до інших видів електронних доказів.

Про можливість надання суду дублікатів протоколів процесуальних дій, а також матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі електронних), виготовлених слідчим, прокурором із залученням спеціаліста, стверджується у постанові ВС від 15.01.2020 р. (справа № 161/5306/16-к) [159].

Щодо застосування поняття «дублікат» до протоколів процесуальних дій ми вважаємо це цілком логічним як до паперового документа, адже такий документ виготовляється, однак до скопійованих файлів звукозапису, відеозапису чи інших електронних доказів логічно застосовувати поняття «копія». Принциповим є сам механізм: дублікат виготовляється його автором, а файл копіюється на інший носій.

ВС в постанові від 15.01.2020 р. справа № 161/5306/16-к зазначає, що «терміни «копія» і «дублікат» не є синонімічними. Разом з тим, слід зазначити, що КПК у частині 4 статті 99 надає автономне визначення поняття «дублікат документа» як документа, виготовленого таким самим способом, як і його оригінал. Отже, для точного використання даних термінів у кримінальній процесуальній діяльності термін «копія документа» слід визначати за пунктом 3.10 ДСТУ 2732:2004, а термін «дублікат документа» – за частиною 4 статті 99 КПК» [159].

Не заперечуючи висновки суду, що поняття «копія» і «дублікат» не є синонімічними, наступні міркування суду, на нашу думку, є не зовсім логічними і ми не можемо з ними погодитися (незрозуміло чому необхідно застосовувати саме такий підхід для визначення що таке копія, а що таке дублікат документа: в одному випадку керуватися ДСТУ, а в іншому нормами кримінального процесуального закону). Якщо слідувати буквальному тлумаченню ч. 4 ст. 99 КПК, то для того щоб стверджувати, що це дублікат електронного документа, то його необхідно *виготовити* (курсив наш - І. Смаль) у точно такий спосіб як виготовляв його автор

документа. «Виготовити у такий самий спосіб», тобто зробити ті самі дії, які робив автор цього документа.

Під цифровою копією А. В. Скрипник розуміє а) скопійований файл без підтвердження автентичності (без хешсуми) б) електронне або паперове відображення змісту файлу (принтскрин, роздруківка тощо) [250, с. 117].

На нашу думку, логічно і більш обґрунтовано до інформації в електронному вигляді використовувати поняття оригінал та копія, адже коли здійснюється копіювання інформації в електронному вигляді, то її зміст не змінюється, однак змінюються дані, що стосуються дати, часу створення копії документа, тобто до файла, який містить відповідну інформацію вносяться зміни, які пов’язані тільки з його копіюванням.

А. А. Барабаш, Д. І. Клепка доходять висновку, що електронні документи, які не посвідченні ЕЦП, можуть вважатись електронними документами, однак не будуть вважатись оригіналами таких документів у розумінні цього Закону України «Про електронні документи та електронний документообіг» [9, с. 32]. На нашу думку, якщо електронний документ не містить підпису, то це фактично не електронний документ, а один із видів електронних доказів.

Як ми вже зазначали в першому розділі нашої роботи одними із ознак електронних доказів є те, що вони містять метадані. Про це також говорить А. Ю. Каламайко та Ю. С. Павлова [84, с. 98; 144, с. 7].

Для терміну метадані немає єдиного формального визначення. Навпаки, існують різні визначення цього терміну. Метадані – інформації технічного характеру, яка закодована всередині файлів [84, с. 50]. Метадані – довідкова структурована інформація, що описує, роз'яснює, дає змогу ідентифікувати, спрощує використання та управління набором даних [228]. Метадані цифрового об’єкта – інформація, яка фіксується в автоматичному режимі у зв’язку із створенням та використанням певного об’єкта. Метадані описують характеристики об’єкта, дату і час його створення чи внесення змін у нього, інші відомості про об’єкт [366, с. 67].

Досить слушною і корисною для формування практики є думка науковців інших країн. Метадані – це вмонтована в тіло цифрових даних інформація про самі дані. Їх особливістю є те, що вони мають латентний характер: зазвичай, метадані не відображаються на екрані дисплея і, таким чином, не відтворюються, коли інформацію з екрана роздруковують на папері [405, с. 33].

Для прикладу, програми-редактори текстових документів автоматично створюють і фіксують відомості про автора, час створення і внесення змін та інше. А метадані з електронної пошти, наприклад, можуть поінформувати, чи створювались резервні копії листів, коли листи були надіслані, прочитані тощо. Як уже зазначалося, кожна копія електронного документа може вважатися оригіналом. У цьому випадку є ризик зіштовхнутися з проблемою, що такі «оригінали» можуть не мати потенційно корисних у доказуванні метаданих, які містяться лише в первісному електронному примірнику [409, с. 173].

Електронні копії цифрових даних звісно мають метадані, але вони не є копією метаданих первісного файлу, а цілком новими відомостями, що з’явилися в момент копіювання і характеризують лише обставини обробки та зберігання самої копії. Унаслідок цього суб’єкти судового пізнання не можуть почерпнути важливої для доказування інформації, тобто повинно існувати процедура підтвердження ідентичності відповідного електронного доказу. Ми не ведемо мову в даному випадку про електронний документ, тому що підтвердженням його ідентичності буде електронний підпис. Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису [223]. «Особливу увагу варто звернути на цілісність й автентичність електронних доказів з позиції їх надійності та достовірності. Цей процес охоплює перевірку точності використовуваних криміналістичних інструментів, проведення порівнянь хеш-значень для забезпечення цілісності даних, перевірку метаданих для встановлення часової шкали та цілісності файлів. Для підвищення надійності висновків може знадобитися незалежна перевірка експертами» [240, с. 63].

Найбільш ефективним засобом встановлення тотожності копії і оригіналу є визначення логічного атрибуту – контрольної суми (хешу, хеш-коду, хеш-суми) [250, с. 106; 280, с. 114; 353, с. 258].

У світлі вказаних тенденцій питання, пов'язані з хешуванням електронних доказів, набуватимуть все більшого значення для судової практики, адже з вказаними питаннями нерозривно пов'язані питання оцінки автентичності електронних доказів, їх належності та допустимості. За даними ЄДРСР ККС ВС вже ухвалено низку постанов, в яких йшла мова про необхідність хешування для підтвердження автентичності електронних доказів [206; 189; 193].

«Питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень» [171].

Що ж таке хеш-сума і яке вона має значення для встановлення ідентичності відповідного електронного доказу?

Контрольна сума – це певне значення ,яке обчислюється на основі набору даних із застосуванням одного із математичних (криптографічних) алгоритмів, які використовуються для перевірки цілісності даних при їх передачі або збереженні[39] [до примітки див. 110, с. 70; 349, с. 9].

Під час фіксації даних здійснюється копіювання інформації, створюється побітова (фізична) копія, повна копія, часткова побітова копія, файлова (логічна) копія і т.п. Для забезпечення технічного аспекту процесу копіювання інформації

---

[39] О.Кравченко, К.Макарук зазначають що «одним із способів підтвердження цілісності та незмінності електронної інформації під час її зберігання, перезапису, перенесення та передавання каналами зв’язку є обчислення та перевірка контрольної суми файлів. Контрольна сума (CRC-сума, хеш-сума) – це деяке значення, що розраховане за набором даних шляхом застосування певного алгоритму і використовується для перевірки цілісності даних під час їх передачі або зберігання. Перевірка файлів методом обчислення контрольної суми, також відома як хешування, – це процес підтвердження того, що файл, завантажений на комп’ютер, ідентичний вихідному файлу. Здійснюючи хешування одного і того самого файлу, завжди отримують однаковий рядок символів у хеші за умови, що жоден біт цього файлу не змінився. Але якщо файл принаймні несуттєво відрізняється від оригіналу (наприклад, у файлі з’явився новий символ пробілу), контрольна сума буде зовсім інша .

доцільно застосовувати ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» Стандарт розрізняє процеси виготовлення фізичної або порозрядної копії (образу) електронного носія інформації та копії окремого електронного файлу [73].

Отже, під «хешем» слід розуміти свого роду маркер цілісності файлу, підтвердження відповідності копії оригіналу і таке підтвердження можливе без проведення експертних досліджень, адже для кожного файлу генерується унікальна, притаманна виключно йому, хеш-сума і навіть мінімальна зміна інформації генерує зовсім інше значення хеш-суми. Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством (ч. 4 ст. 7 Закону №851-IV) [183].

На нашу думку, ця норма закону дає підстави стверджувати, що у КПК України повинна бути закріплена норма про порядок підтвердження цілісності та автентичності електронного доказу.

ЗУ «Про електронну ідентифікацію та електронні довірчі послуги» від 05.10.2017 № 2155-VIII, визначає, що автентифікація – це електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних (ст. 1) [225].

Яким чином правозастосовна практика «пристосовує» чинний КПК України до потреб сучасності, можна побачити на прикладі проведеного аналізу судових рішень. На нашу думку, саме судова практика дає поштовх до вдосконалення правового визначення поняття доказів у кримінальному провадженні із урахуванням специфіки інформації в електронному вигляді і відповідно необхідності нормативного закріплення спеціального режиму її використання в якості доказу. А підтвердженням актуальності питання «оригіналу», «копії» електронного доказу в рамках даної роботи свідчить відсутність єдності у наукових поглядах, так і наявність суперечливої судової практики.

Використання поняття «оригінал», «копія» в судових рішеннях

Так, Постановою Верховний Суд колегією суддів Третьої судової палати ККС від 11 березня 2020 р. (справа № 149/745/14) підтверджено позицію суду про визнання недопустимими як докази протоколів про проведення негласної слідчої (розшукової) дії аудіо-, відеоконтролю особи з посиланням на ч. 3 ст. 99 КПК щодо необхідності надання оригіналу документа [160].

Прикметно, що через два місяці ВС в складі цієї ж колегії (Постанова ВС від 20 травня 2020 року справа N 585/1899/17) виносить протилежне рішення з мотивацією, що всі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення [163; 164; 165 ; 171; 206].

Питання ідентифікації електронного документа як оригіналу можуть бути вирішені або повноважною особою, яка його створила або, за наявності підстав, шляхом проведення спеціальних судових досліджень [178; 181; 165; 169; 172; 175; 176].

“Ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив`язки до конкретного матеріального носія [41; 166; 174; 183; 186; 185, див. додаток В].

Отже, ми можемо бачити усталену практику ВС щодо визнання копій файлів оригіналами, з обґрунтування такої правової позиції положеннями Закону України «Про електронні документи та електронний документообіг».

Однак є і рішення ВС (Постанова ВС від 01.09.2022 справа № 736/2398/18), в яких суд погоджується, що були підстави для визнання аудіофайла недопустимим доказом та зазначає, що це не суперечить усталеній судовій практиці щодо оцінки копії електронного документа, створеного відповідно з оригіналу цього документа з додержанням процедури, передбаченої кримінальним процесуальним законом (фактично не було доказів, що копія зроблена з оригінала) [170].

В іншій справі колегія суддів ВС не погодилася з такими висновками місцевого суду, які підтримав апеляційний суд щодо не підтвердження оригінальності копій відеозапису. Одним із мотивів було, що сторона захисту не зверталася з клопотанням про витребування та дослідження в судовому засіданні первинних носіїв інформації, отриманої за результатами НСРД, для порівняння змісту електронних документів з таких носіїв з тими, що зберігаються на носіях, наданих суду як додатки до протоколів НСРД; відсутність будь-яких об`єктивних даних про те, що носії інформації, долучені до протоколів про проведення НСРД, містять електронні документи, створені не під час здійснення цих НСРД [177].

Термінологія, що використовується в судових рішеннях

Незважаючи на те, що в кримінальному процесуальному законодавстві відсутня термінологія «електронний доказ» в судових рішеннях використовують даний термін для позначення: відеофайла, який містився на диску, та був визнаний постановою слідчого електронним доказом [38].

Аналогічно і в інших судових рішеннях використовується термінологія «електронні докази» [34; 42; 43; 290; 292; 301]; «електронний доказ електронний носій (DVD-R-диск)» [46]; «електронні докази, які знаходяться на жорсткому диску та складаються із файлів», «197 одиниць електронних доказів» [291].

Цікава аргументація міститься і в ухвалі Київського апеляційного суду від 09.02.2023 р. (справа № 759/16863/16-к)[40] [до примітки див. 299].

Способом фіксації електронного доказу буде створення його електронної копії, найчастіше це відбувається у вигляді скріншота»; «скріншоти відеозапису… могли б бути копіями електронних доказів, якби стороною обвинувачення… разом

---

[40] той факт, що наявні в справі *фото- та відеоматеріали не є первинними….* (курсив наш - І. Смаль), тобто, не виходять з першої точки, а ідентифікаційні ознаки носіїв, на яких зберігаються дані відомості в матеріалах даних, не завжди співпадають з тими, які в протоколі …, слід оцінювати ці матеріали як *електронні копії фото- та відеоматеріалів»* (курсив наш - І.Смаль). З посиланням на Закон України «Про авторське право і суміжні права», а саме поняття електронна (цифрова) інформація суд зазначає, будь-яка *інформація в цифровій формі* (курсив наш - І. Смаль) на будь-яких веб-сайтах чи комп'ютерних програмах у вигляді статей чи переписки може використовуватися *як електронний доказ* (курсив наш - І. Смаль) у суді відповідно до закону.

із скріншотами до суду були надані власні оригінали відеозапису» [300, див. додаток В].

Таким чином, ми можемо бачити використання практиками термінології «електронні докази», «копії електронних доказів», «електронний носій». Також мова йде про скріншот як спосіб фіксації електронного доказу та необхідною умовою його використання є його посвідчення відповідно до Національного стандарту ДСТУ 4163:2020 «Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів» [72].

В касаційній скарзі захисник вказує на недопустимість як доказів відеозаписів, посилаючись на те, що дані електронні докази не мають електронного підпису, що відповідно до положень частин 1, 4 ст. 7 Закону України «Про електронні документи та електронний документообіг», а також рішення ВП ВС від 14.02.2019 р. (справа № 9901/43/19) свідчить про їх не оригінальність, а також недопустимість [173].

У вироку від 15.02.2022 № 559/762/19 Млинівський районний суд Рівненської області виснував «паперова копія електронного доказу скріншотів сторінок у соціальних мережах не є письмовим доказом, оскільки такі роздруківки не засвідчені в установленому ЗУ "Про електронні документи та електронний документообіг" порядку» [39].

Представник потерпілого заявив, що електронні докази належним чином не завірено і з такими доводами погодився суд (Ухвала ВАКС від 17.02.2023 Справа № 991/667/23) [289].

У вироку від 12.02.2024 № 756/14896/21 Оболонський районний суд м. Києва, обґрунтовуючи свою позицію надав власне визначення електронних доказів,[41] [до примітки див. 40].

---

[41] яке фактично відтворює поняття електронних доказів інших процесуальних кодексів та вважає, що можливість застосування електронних доказів випливає зі змісту ст. 84 КПК України, яка не передбачає вимог до форми доказів. Основним критерієм віднесення доказів до електронних є їхня форма - електронна (цифрова) форма, а також орієнтовний перелік тих електронних доказів, подання яких може мати місце під час розгляду провадження.

Адвокатом у справі № 707/146/17 заявлено клопотання про призначення експертизи відео-, звукозапису відеофайлів, ухвалою від 01.07.2021 ВАКС відмовлено в задоволенні клопотання з підстав, що не надано доказів щодо підробки та/або монтажу відеофайлів [288]. Аналогічно ВАКС мотивував свою позицію і у вироку від 09.11.2023 № 991/5570/20 [32].

Наша позиція, сформована на основі аналізу законодавства, полягає в тому, що якщо відсутність хешування ставить під сумнів автентичність електронного доказу, суду слід задовольнити заяву адвоката про призначення відповідної експертизи, особливого якщо цей доказ є ключовим для прийняття рішення, адже це у підсумку може вплинути на справедливість судового розгляду. І призначення такої експетризи може бути єдиним способом встановлення достовірності такого доказу.

В ЄДРСР можна знайти досить велику кількість ухвал однотипного змісту, в яких суд, з посиланням на норми ст. 7 ЗУ «Про електронні документи та електронний документообіг», обґрунтовує необхідність обов'язкового реквізиту електронного документу та зазначає, що оригіналом електронного документа вважається електронний примірник документа з обов`язковими реквізитами, у тому числі з електронним підписом автора [293–298].

На нашу думку, це пов'язано з тим, що на практиці при роботі з інформацією в електронному вигляді стає цілком очевидним, що окрім електронних документів, яким притаманні обов'язкові реквізити, в тому числі електронний підпис автора, існують ще й інші види електронних доказів.

Перевірка достовірності електронних доказів, тому числі і електронних документів, є складним і проблемним питанням. Адже достовірність доказів фактично залежить від дотримання процедури їх збирання та фіксації. Цей

Оптичний диск з відеозаписом (відеофайлом) є самостійним джерелом доказу, похідним від інформації, що було зафіксовано відеореєстратором в електронному вигляді у виді файлу, що свідчить про те, що записаний на оптичний диск - носій інформації електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа [36].

очевидний факт підтверджується також і результати опитування практикуючих юристів (Додаток Б, питання 18).

Отже, можемо зробити висновок, що існування електронних доказів в специфічному середовищі, обумовленому використанням певних технічних засобів чи пристроїв та програмного забезпечення не дозволяє поширювати категорії «оригінал», «дублікат» і «копія» у їхньому традиційному значенні на електронні докази. Також для визначення цих категорій є важливою така ознака електронних доказів як відсутність тісного зв'язка з матеріальним носієм електронної інформації, отже вони можуть зберігатися одночасно на декількох матеріальних носіях, а також в хмарному середовищі. Не можна залишити поза увагою й ті проблеми, що виникають у судовій практиці, оскільки копіювання файлів без належного технічного супроводу може негативно неабияк впливати на доказову цінність інформації. І як підтверджує судова практика в задоволені клопотань сторони захисту щодо призначення експертних досліджень для підтвердження автентичності копії оригіналу, як правило, суди відмовляють з посиланням на правові позиції ВС, які в свою чергу місять положення щодо необхідності такої автентифікації.

На наш погляд як науковця, правові позиції ВС, про які ми зазначали вище [163–165; 171; 178; 206] враховують правову природу електронних доказів, а саме можливість існування на різних матеріальних носіях і бути ідентичним за змістом.

Однак цю ідентичність, на наш погляд, в обов'язковому порядку повинна підтвердити особа, яка зберігла файл (носій інформації) на іншому матеріальному носієві, тобто слідчий, дізнавач, прокурор або спеціаліст, якщо слідча(розшукова), негласна слідча(розшукова) дія, тимчасовий доступ до речей, документів проводилися за його участі. Частина 2 ст. 92 КПК України визначає, що обов`язок доказування належності і допустимості доказів покладається на сторону, що їх подає[113]. Тобто сторона обвинувачення повинна підтвердити за допомогою обчислення контрольної суми файлу або каталогу з файлами (CRC-суми, hash-суми) відповідність копії оригіналу. А достовірність електронного документа

повинно підтверджуватися цифровим підписом. Адже ч.3 ст.104 КПК визначає, що протокол процесуальної дії в обов'язковому порядку повинен містити інформацію про виготовлені дублікати документів, а також копії інформації, у тому числі комп'ютерних даних, *та спосіб їх ідентифікації* (курсив наш - І. Смаль) [113]. У випадку відсутності хеш кода в обов'язковому порядку призначається стороною обвинувачення експертиза, яка повинна підтвердити відповідність копії оригіналу. І в даному випадку допустимість доказу може заперечуватися за відсутності підтвердженого хешування або експертного дослідження.

Ще раз звернемо увагу на норму Закону України «Про електронні документи та електронний документообіг» – «Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством» (ч. 4 ст. 7 Закону) [223].

На нашу думку, ця норма закону дає підстави стверджувати, що у кримінальному процесуальному кодексі повинна бути закріплена норма про порядок підтвердження цілісності та автентичності електронних доказів, і, зокрема, електронного документа. Не лише теоретичні висновки, а й матеріали судової практики підтверджують, що у багатьох випадках не існує обґрунтованої потреби у поданні до суду оригіналів електронних доказів, а цілком достатнім є надання їх копій. І в цьому аспекті ми повністю підтримуємо думку М. І. Демури, Д. І. Клепки, І. О. Крицької про те, що «первинним критерієм допустимості використання цифрової інформації та її носіїв у кримінальному процесі як засобу доказування обставин, що мають значення для кримінального провадження, має бути наявність технічних можливостей підтвердити автентичність такої інформації» [66, с. 298].

3.2. Електронні докази та забезпечення права на приватність в контексті ст.8 ЄКПЛ.

Право на приватність є фундаментальним право людини, закріпленим в Загальній декларації прав людини ООН, Міжнародному пакті про громадянські й політичні права, а також в низці інших міжнародних і регіональних угодах.

Приватність тісно пов'язана з людською гідністю й іншими базовими цінностями демократичного суспільства. Так, у ст. 12 Загальної декларації прав людини проголошено захист особистого і сімейного життя, таємниці кореспонденції [77]. Ст. 17 Міжнародного пакту про громадянські і політичні права гарантує захист від свавільного чи незаконного втручання у особисте та сімейне життя, таємницю кореспонденції [129].

За міжнародними нормами одним із елементів права на приватність є право на таємницю кореспонденції.

В ст. 8 Конвенції про захист прав людини і основоположних свобод визначено, що «кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції» [105].

Отже, таємниця кореспонденції є складовою права на приватне життя, як одне з основоположних прав людини, закріплене як на національному, так і на міжнародному рівнях.

Право на повагу до «кореспонденції» у розумінні статті 8 § 1 ЄКПЛ має на меті захистити конфіденційність спілкування у широкому переліку різних ситуацій. Нові технології також підпадають під сферу дії статті 8, зокрема дані зі смартфона/планшета та/або його дзеркальної копії («Saber v. Norway» 2020, § 48; «Särgava v. Estonia», 2021), електронні повідомлення (електронні листи) («Copland v. the United Kingdom», 2007, § 41; «Bărbulescu v. Romania [GC]», 2017, § 72); використання Інтернету («Bărbulescu v. Romania [GC]», 2017, § 81 та «Copland v. the United Kingdom», 2007, §§ 41–42), і дані, що зберігаються на комп'ютерних серверах («Wieser and Bicos Beteiligungen GmbH v. Austria», 2007, § 45), включаючи жорсткі диски («Petri Sallinen and Others v. Finland», 2005, § 71) та дискети («Iliya Stefanov v. Bulgaria», 2008, § 42) [398].

В окремій думці судді Gerald Fitzmaurice у справі справі «Golder v. the United Kingdom» (1975) констатовано, що термін «кореспонденція» є менш широким, ніж спілкування і тому було б неправильно ототожнювати поняття «кореспонденція» з поняттям «спілкування» [374].

У рішенні у справі «Klass and Others v. Germany» (1978) ЄСПЛ уперше дав розширене тлумачення терміну «кореспонденція», зазначивши, що телефонні розмови охоплюються поняттями «приватне життя» і «кореспонденція» за змістом п. 1 ст. 8 Конвенції і в подальшому ЄСПЛ ще більше розширив тлумачення терміну кореспонденція («Malone v. the United Kingdom», 1985) [376; 377].

В українському законодавстві можемо виділити такі аспекти приватності: тілесна приватність (ст. 28 Конституції України), територіальна приватність (ст. 30); комунікаційна приватність (ст. 31); інформаційна приватність (ст. 32 Конституції України) [108].

В рамках нашого дисертаційного дослідження нас більш цікавить комунікаційний аспект приватності. Так, приватність спілкування гарантована Конституцією України (ст. 31) [108].

Тобто, конституційні гарантії права на приватність поширюється на такі об’єкти: 1) листування; 2) телефонні розмови; 3) телеграфна кореспонденція; 4) інша кореспонденція. Отже, з конституційних норм вбачається, що «листування» та «кореспонденція» є окремими об’єктами захисту.

Аналогічно, в ст. 163 КК України об’єктом кримінального правопорушення є право на таємницю листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер [111].

А в кримінальному процесуальному законодавстві окремими об’єктами захисту є «приватне життя» і таємниця спілкування (ст. 7, 14, 15 КПК) [113].

Інтерес до права на приватність істотно посилився в другій половині XX століття у зв’язку зі стрімким розвитком інформаційних технологій. За останні десятиліття Інтернет перетворився на один із основних засобів комунікації, а технологічний прогрес набув безпрецендентних темпів. Щороку мільйони нових користувачів приєднуються до цифрового простору, що підсилює актуальність захисту приватності.

На нашу думку, очікування суспільства щодо конфідеційності спілкування є досить актуальним, враховуючи яку важливу роль відіграє електронна пошта,

спілкування в соціальний мережах у приватному житті кожної людини. Збережені повідомлення електронної пошти, повідомлення в месенджерах є досить інформативні.

Не ставлячи за мету дослідити всі аспекти втручання у право на приватність у кримінальному провадженні, спробуємо з'ясувати найбільш проблемні питання [258]. Потреба у цьому зумовлюється необхідністю формування чіткого уявлення про місце та роль електронних доказів. Без формулювання чіткої теоретичної концепції з даного питання доволі складно виробити рекомендації практичного характеру.

При розкритті даної тематики в першу чергу звернемо увагу на такі ознаки інформації в електронному вигляді як значний обсяг інформації, яка може зберігатися на певному носієві, адже ця інформація може накопичуватися не один рік. В мобільному телефоні можна отримати інформацію про спілкування в різних соцмережах, збережені паролі, смс повідомлення, контакти як в телефоні, так і в електронній пошті, месенджерах, геотеги, медіафайли, записи особистого характеру. Майже в кожному мобільному пристрої, комп'ютері існують спеціальні програми, як то «Приват 24», «Ощадбанк» «Монобанк», які дозволяють керувати банківськими рахунками (проводити відповідні транзакції, брати кредити, робити вклади тощо).Отже, через дані пристрої слідчий фактично може отримати доступ до фінансових операцій, тобто банківської таємниці. А, наприклад, через програму Helsi до медичної документації. Постає питання чи можна отримувати всю цю інформацію без судового дозволу?

Також необхідно враховувати можливість доступу до такої інформації не безпосередньо на самому носієві, а через віддалений доступ. Все це дає підстави вважати, що у слідчого (дізнавача), прокурора може з'явиться необмежена кількість інформації, яка взагалі не має відношення до кримінального провадження, але яка має відомості приватного характеру. І в цьому контексті необхідно піднімати питання забезпечення прав людини щодо захисту таємниці приватного життя та кореспонденції.

Забезпечення прав і свобод людини є конституційним обов'язком держави. Органи досудового розслідування, прокуратура, суд, забезпечуючи швидке, повне, неупереджене розслідування і судовий розгляд повинні також забезпечити дотримання прав і свобод людини. Дотримання балансу, пропорційності втручання в сферу прав і свобод людини, справедливої рівноваги між інтересами судочинства та загальними завданнями кримінального провадження – найбільш гостро знаходить свій прояв у питанні меж втручання у приватне спілкування під час збирання доказів та дотримання прав на повагу до приватного, сімейного життя та кореспонденції під час входження в «електронний» простір особи.

У контексті досліджуваної проблематики звернемося до Резолюції A/HRC/RES/32/13 Ради ООН з прав людини, яка декларативно підкреслює, що права, які належать людям офлайн, мають захищатися і у мережі Інтернет [417].

Без сумніву порядок такого втручання повинен мати чітку урегульованість нормами кримінального процесуального законодавства.

А. В. Скрипник також наголошує на проблемі неконтрольованого втручання у сферу прав людини коли це стосується отримання інформації з електронних носіїв [251, с. 156]. На це звертають увагу також і інші науковці [66, с. 297].

С. Р. Тагієв обґрунтовано акцентує увагу на проблемі необмеженого доступу суб'єктів, що здійснюють досудове розслідування, до інформації, що міститься на електронних носіях [273 с. 6].

Така інформація може стати складовою доказової бази лише за умови її виявлення, вилучення, дослідження та процесуального закріплення із дотриманням прав людини та з урахуванням захисту персональних даних вважають Г. Авдєєва та Е. Живуцька-Козловська. [1, с. 129–130; 262].

До прикладу приведемо також рішення ЄСПЛ у справі «Saber v. Norway» (2020), в якому Суд виснував [42] [до примітки див. 380].

---

[42] «пункт 2 статті 8 Конвенції вимагає, щоб відповідний закон був «сумісним з принципом верховенства права». У контексті обшуків і виїмок національне законодавство повинно забезпечувати певний захист особи від свавільного втручання в її права за статтею 8. Таким чином, національне законодавство має бути достатньо чітким у своїх формулюваннях, щоб дати громадянам адекватне уявлення про обставини та умови, за яких органи державної

За своїм змістом право особи на таємницю кореспонденції пов'язане з поняттям приватного життя людини і безумовно є елементом її приватності.

Незважаючи на наявність вагомого наукового здобутку, присвяченого проблемі, що пропонується для аналізу та розв'язання, досі залишається поле для полеміки з багатьох питань, пов'язаних з втручанням у «електронний простір» людини під час провадження досудового розслідування та судового розгляду кримінальних проваджень. Саме комплексне дослідження різних аспектів цього правового явища уможливить визначити найбільш доцільний та збалансований напрям коригування чинного кримінального процесуального законодавства в контексті забезпечення конституційних та конвенційних прав людини щодо втручання у право на приватність і забезпечення швидкого, повного, неупередженого розслідування і в свою чергу забезпечення права на справедливий судовий розгляд. Такий підхід, з нашого погляду, дозволить глибше і всебічніше дослідити правову природу електронних доказів у кримінальному процесі.

Збирання доказів, в тому числі і електронних доказів, може здійснюватися у кримінальному провадженні шляхом проведення слідчих (розшукових) дій: обшуку (ст. 234 КПК України); огляду (ст. 237 КПК України); зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису (ст. 245-1 КПК України); здійснення заходів забезпечення кримінального провадження: тимчасового доступу до речей і документів (ст. 159 КПК України); тимчасового вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку (ст. 168 КПК України); шляхом проведення негласних слідчих (розшукових) дій відповідно до глави 21 КПК України: зняття інформації з інформації з електронних комунікаційних мереж (ст. 263 КПК України); зняття інформації з електронних інформаційних систем (ст. 264 КПК України);

влади мають право вдаватися до будь-яких таких заходів. Крім того, обшук і виїмка є серйозним втручанням у приватне життя, житло і кореспонденцію і, відповідно, повинні ґрунтуватися на особливо чіткому «законі». Важливо мати чіткі, детальні правила з цього питання».

установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України) і т. д.[113].

Переважна більшість С(Р)Д та НС(Р)Д, пов'язаних з обмеженням конституційних прав і свобод особи, можуть проводитися тільки при наявності ухвали слідчого судді. Правові приписи, що закріплені в ч. 3 ст. 233 та ст. 250 КПК України надають можливість проведення таких дій за відсутності ухвали слідчого судді за умови подальшого судового контролю.

Питання щодо встановлення балансу інтересів правоохоронних органів та права людини на повагу до приватного, сімейного життя, житла та кореспонденції у визначенні того, чи існує «достатня підстава» для проведення обшуку є хоч і не новим, але залишається актуальним і на даний час, про що свідчить неоднозначна судова практика.

В КПК України зустрічається формулювання «достатня підстава», «наявність достатніх підстав вважати», «оцінка доказів з точки зору достатності та взаємозв'язку» як один із стандартів доказування.

На нашу думку, для встановлення наявності «достатніх підстав» не має потреби в детальному аналізі аргументів «за» і «проти». Достатньо встановити, що певні факти та обставини вказують на існування підстав, які будуть «достатніми» для переконання дізнавача, слідчого, прокурора у необхідності чи можливості проведення певної слідчої дії, застосування заходів забезпечення кримінального провадження, тощо.

Погоджуємося з висловленою думкою І. А. Тітка, що застосування кримінальних процесуальних норм з оцінними поняттями вимагає від правозастосовника детального аналізу всіх обставин справи, уникаючи абстрактних, шаблонних мотивувань. Особливу увагу слід приділяти індивідуалізації норми з оцінним поняттям стосовно розгляду кожного окремого випадку, оскільки, незважаючи на схожість певних ситуацій, вони не можуть бути ідентичними [278, с. 156].

З цього приводу абсолютно точно зазначала і О. В. Капліна, що зміст правової норми, яка містить оцінне поняття, є невизначеним, а це значно знижує її інформаційне та ціннісно-орієнтувальне значення. До того ж вчена підкреслює, що правозастосовники в процесі оперування оцінними поняттями опиняються у складнішій ситуацій, пов'язаній із потребою адекватного тлумачення в рамках закону та відповідно до волі законодавця, що через наявність суб'єктивіського підходу може спричинити появу юридичних колізій, порушення законності тощо [88, с. 34].

ЗУ «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам» від 15.03.2022 р. № 2137-IX внесені зміни до КПК України, зокрема до ст. 236 КПК [216].

Ч. 6 ст. 236 КПК України оперує також поняттям «достатньої підстави». Так, за наявності «достатньої підстави» вважати, що на комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, міститься інформація, що має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити: 1) пошук комп'ютерних даних; 2) виявлення комп'ютерних даних; 3) фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку.

Тобто, законодавець зазначає, що якщо в ухвалі слідчого судді не надано дозвіл на виявлення комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, а слідчий, прокурор виявив доступ чи можливість доступу до них, то саме наявність оцієї «*достатньої підстави*» (курсив наш - І. Смаль) надає право здійснити активні, цілеспрямовані дії по пошуку комп'ютерних даних та їх фіксацію. Тоді повертаємося до абзацу першого частини 6 ст. 236 КПК, яка надає право слідчому, прокурору під час проведення обшуку «долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється їх відкрити чи зняти

(деактивувати) систему логічного захисту або обшук здійснюється за відсутності осіб, зазначених у частині третій цієї статті». І в цьому аспекті згадаємо ч. 5 ст. 236 КПК України «Обшук на підставі ухвали слідчого судді повинен проводитися в обсязі, необхідному для досягнення мети обшуку». Таким чином, ми доходимо до логічного висновку, що якщо обшук за твердженням законодавця повинен проводитися в обсязі, необхідному для досягнення мети такого обшуку, а мета такого обшуку повинна чітко і неоднозначно міститися в ухвалі слідчого судді, то «долати системи логічного захисту» слідчий, прокурор може тільки в тому випадку, якщо в ухвалі слідчого судді надавався дозвіл на пошук конкретної інформації, комп'ютерних даних.

А тепер звернемо увагу на конструкцію абзацу другого частини шостої ст. 236 КПК: «виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку» [280], і як ми можемо бачити мова йде про надання дозволу на виявлення «комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку» , а не комп'ютерних даних, пошук яких можливий при наявності двох складових: виявлення доступу чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку; наявності достатніх підстави вважати, що *інформація* (курсив наш - І. Смаль) що на них міститься має значення для встановлення обставин у кримінальному провадженні.

Таким чином, в нас виходить замкнуте коло, яке не дає «чіткості закону» і воно буде існувати до тих пір, поки законодавець не визначить як джерело доказів «електронні докази» та окремі процесуальні правила для отримання в якості доказу інформації в електронному вигляді. Адже в даній статті мова йде про «комп'ютер», а що ми розуміємо під даним терміном ми детально визначали в розділі 1 нашого дисертаційного дослідження, як фізичний об'єкт і про інформацію в електронному вигляді, яка за сукупності певних умов може бути доказом (електронним).

На нашу думку, встановлення «достатньої підстави» слідчий, прокурор повинен переконливо «пояснити», а це можливо шляхом чіткого обґрунтування у протоколі обшуку і подальшого судового контролю.

Як відомо, стандарт доказування «достатня підстава» досить давно використовується у англосаксонській системі права. Так, у Четвертій поправці до Конституції США зазначається, що:[43] [до примітки див. 419].

Достатня підстава», або в іншій інтерпретації «ймовірна причина», «розумна підстава» (probable cause), є одним зі стандартів доказування у кримінальному провадженні, який раніш за все отримав свій прояв на практиці та закріплення у законодавстві держав англосаксонської системи права. Зміст стандарту доказування «достатня підстава» та коло рішень, які приймаються на підставі відповідного стандарту доказування у кримінальному провадженні, є різними у державах англосаксонської та континентальної системи права [143, с. 104].

Цілком зрозуміло, що огляд вмісту електронного носія інформації проводиться не тільки з метою виявлення збережених файлів, а й з метою фіксації листування, яке міститься в смс та інших повідомленнях.

Перевірка практичного правозастосування цієї норми свідчить про низку існуючих проблем. Хоча, на перший погляд, вказана норма закону є зрозумілою і не дає підстави для подвійного тлумачення. Вбачається певна невідповідність європейським стандартам якості закону, адже в ч. 6 ст. 236 КПК України визначення «щодо яких є достатні підстави вважати» вказують на занадто широку свободу дискреції. А в свою чергу, високий ступінь втручання у право на приватність покликаний, щоб закон встановлював низку правових гарантій пропорційності такого втручання.

---

[43] «право осіб на їхню недоторканність, а також їхнього житла та документів проти необґрунтованого обшуку та виїмки (конфіскації) не повинно бути порушене, жодне рішення не може бути прийняте не інакше, як на підставі достатньої підстави (ймовірної причини), скріпленої присягою (клятвою) або письмовою заявою (підтвердженням) з докладним описом місця обшуку; особи, яка розшукується та предметів, для виявлення яких проводиться обшук» [368].

Враховуючи мету даної слідчої дії необхідно, щоб все таки закон достатньо чітко визначав межі такої дискреції слідчого, прокурора, щоб забезпечити дотримання прав і свобод від свавільного втручання.

На думку автора дискусійним є також питання, пов'язані з оглядом інформації, яка міститься в пам'яті телефонів, планшетів, ноутбуків і т.п. без відповідного дозволу суду. Адже при такому огляді відбувається втручання у конституційні та конвенційні права учасників кримінального процесу та інших осіб на таємницю листування, телефонних переговорів, оскільки таємниця спілкування є одним із загальних засад кримінального провадження [263, с. 229].

На мобільному телефоні будь-якої особи міститься особиста переписка з іншими людьми в СМС-повідомленнях, соціальних мережах, наприклад у «Ватсап», «Телеграм», «Вайбер» тощо. «Активні пошуки в телефоні інформації» є фактично його обшуком і повинен бути судовий контроль за пропорційністю втручання у приватне життя та кореспонденцію. Адже слідчий «шукає» в ньому інформацію без обмеження в часі і без обмеження обсягу і змісту інформації.

В межах процедури розгляду клопотання про надання дозволу на проведення відповідної слідчої(розшукової) дії здійснюється судовий контроль законності обмеження прав і свобод, необхідності, тобто чи є таке втручання у права і свободи людини виправданим для досягнення мети та відповідно оцінює пропорційність такого втручання.

Поглянемо на законодавчі норми. Клопотання слідчого про обшук в житлі чи іншому володінні повинно, крім іншого, містити обґрунтування, що обшук є пропорційним заходом втручання ***в особисте та сімейне життя особи*** (курсив наш - І. Смаль)(п. 5 ч. 5 ст. 234 КПК). Тобто, слідчий суддя повинен при прийнятті рішення оцінити пропорційність втручання в особисте та сімейне життя особи. Отже мова не йде про оцінку пропорційності втручання в кореспонденцію. Постає питання чому? На нашу думку, норми, що регулюють обшук не враховують, що електронна пошта, листування в соціальних мережах є окремим об'єктом захисту,

визначеним ст. 8 Конвенції. Адже питання щодо втручання у кореспонденцію в нашому КПК вирішується тільки шляхом проведення негласних слідчих дій.

І в цьому контексті доречно привести результати опитування 1289 практикуючих юристів. Так, 75 % суддів, 74 % прокурорів, 63 % слідчих (дізнавачів), 100 % адвокатів висловили думку про необхідність поширення поняття «кореспонденція» на листування в застосунках для обміну повідомленнями, електронній пошті (Додаток Б).

Ще одним питанням, яке належить до вказаної проблематики є огляд інформації, яка міститься в електронних пристроях, вилучених під час затримання особи. На сьогодні у даному питанні не досягнуто єдності як серед науковців, так і в судовій практиці, що, на наш погляд, надає йому актуальності в аспекті наукового осмислення.

В дисертаційному дослідженні А. Скрипник зазначає, що затримання особи і особистий обшук здійснюються з метою запобігти злочинові чи його перепинити (ч. 3 ст. 29 Конституції України), а не з метою зібрати докази чи зберегти доступ до їх процесуальних джерел. «Логіка «автоматичного співобмеження прав» (вилучили – можемо оглянути / обмежили право власності – можемо обмежити й інші права) несумісна з принципами верховенства права і законності» [250, с. 136].

Викладаючи власне бачення на вказане питання, вважаємо за необхідне звернути увагу на низку нормативних положень та окремі реалії практики правозастосування, на які слід зважати принаймні при визначенні відправних позицій законодавчого врегулювання.

Так, відповідно до ч. 1, 2 ст. 168 КПК України кожен хто законно затримав особу, в порядку, передбаченому ст. 207, 208, 298-2 цього Кодексу може тимчасово вилучити майно. Тимчасове вилучення майна може здійснюватися також під час обшуку, огляду [113].

При затриманні осіб вилучаються речі, в тому числі і пристрої, які містять інформацію в електронному вигляді. Частіше всього це мобільні телефони, планшети, смарт-годинники. Оскільки мобільний телефон, крім інформації щодо

викликів, містить великий об’єм іншої інформації в електронному вигляді, то чи можливо проводити огляд такої інформації без дозволу суду? Для нас очевидна відповідь – ні. Ми вважаємо, що повинен бути судовий дозвіл на обшук і саме обшук, а не огляд такого пристрою, і в судовому рішенні повинно бути обов’язково зазначено яку саме необхідно знайти інформацію, за який період.

На нашу думку, не можна ототожнювати інформацію, яка міститься на таких пристроях з самим пристроєм як фізичним об’єктом. У разі виявлення електронного носія інформації в ході особистого обшуку затриманого необхідно після фізичного вилучення такого пристрою отримати судове рішення щодо обшуку електронного носія інформації. Адже для того щоб втручання у право на повагу до приватного життя і кореспонденції відповідало закону та було необхідним в демократичному суспільстві воно повинно супроводжуватися адекватними та ефективними гарантіями проти зловживань.

Огляд інформації, яка міститься в мобільних телефонах, на перший погляд, здійснюється «відповідно до закону», тобто має певне підґрунтя в кримінальному процесуальному кодексі. Однак, КПК України не містить спеціальних положень для обшуку та вилучення комп’ютерних даних.

На нашу думку, необхідно розглянути питання доцільності зміни парадигми у вирішенні питань отримання інформації в електронному вигляді, яка міститься в телефонах, комп’ютерах, інших пристроях в аспекті дотримання ст. 8 ЄКПЛ.

Аргументацію на користь зміни парадигми кримінального процесуального законодавства та запровадження судового контролю під час втручання у приватне спілкування, яке включає в себе і кореспонденцію, підсилюють результати опитування суддів, прокурорів, слідчих, дізнавачів та адвокатів (Додаток Б).

Ч. 2 ст. 264 КПК України визначає, що не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов’язаний з подоланням системи логічного захисту [113].

Характерно, що в правозастосовній практиці є непоодинокі факти, коли слідчі звертаються до суду з клопотаннями про дозвіл на проведення огляду мобільного телефону, незважаючи на наявність згоди власника (володільця інформації) на проведення огляду, вважаючи, що без дозволу суду дана слідча дія буде проведена з порушенням конституційних норм[44] [до примітки див. 303].

Ухвалою слідчого судді Заводського районного суду м. Миколаєва від 09.06.2020 р (справа № 487/378/19) надано доступ до інформації, яка міститься на мобільних телефонах підозрюваного, мотивуючи свою позицію, зокрема, тим , що відповідно до п. 6 ч. 1 ст. 162 КПК України особисте листування особи та інші записи особистого характеру належать до охоронюваної законом таємниці, яка міститься в речах і документах [313]. Аналогічно вирішувалося питання у інших справах [329].

Існує також протилежна практика, коли отримавши доступ до мобільного телефону шляхом його тимчасового вилучення на підставі ухвали слідчого судді, слідчі фактично крім опису зовнішніх ознак телефону оглядають інформацію і інші персональні дані власника телефону, які міститься у пам’яті пристрою. В процесі огляду підбираються паролі до електронних пристроїв, що можна порівняти з обшуком. Вивчення судової практики свідчить про те, що дослідження інформаційного змісту електронних носіїв інформації відбувається як правило шляхом огляду. Однак, інформація, яку потрібно дослідити може знаходитися за межами вільного доступу. Для її пошуку необхідно здійснювати цілеспрямовані пошуки в віртуальному середовищі, що має місце тільки при проведені обшуку. Комп’ютер під час роботи може відображати процеси, які відбуваються станом на зараз (тобто показують які операції виконує комп’ютер), кеш (де дані тимчасово

[44] Так, слідчий суддя Бабушкінського районного суду м. Дніпропетровська (справа № 932/268/20) ухвалою від 17.01.2020 р надав тимчасовий доступ до речей та документів в порядку ст.160 КПК України, а саме до особистого листування та інших записів особистого характеру, зокрема, фотографій, відеозаписів, аудіозаписів, які містяться у мобільному телефону, вилученому під час обшуку. Зі змісту ухвали вбачається, що підозрюваний на досудовому слідстві давав згоду слідчому на проведення огляду його телефонів.

зберігаються), мережеві з'єднання і виявляти будь-які дані, що зберігаються в пам'яті. Пам'ять може містити паролі, ключі шифрування чи розшифровані програми [415, с. 13].

В той же час звернення до релевантної судової практики демонструє діаметральність думок серед правозастосовників[45] [до примітки див. 32].

Тобто, фактично суд констатував, що на законодавчому рівні відсутня процедура отримання інформації з мобільних телефонів. Про це також зазначає і О. П. Метелев «КПК не дає чіткої відповіді, чи необхідно отримувати ухвалу суду на проведення обшуку мобільного телефону або іншого цифрового пристрою затриманого. У ст. 14 КПК передбачено, що втручання в таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування можливе лише на підставі судового рішення. З огляду на вищевказані суперечності процесуальних норм, стає незрозумілим, якою з них повинен керуватись правоохоронець, здійснюючи вивчення вмісту мобільного телефону під час особистого обшуку затриманого [125, с. 179].

С. Р. Тагієв, М. С. Пузирьов, С. В. Івашко ставлять цілком логічне запитання щодо доцільності тлумачення норм судом, коли мова йде про тимчасове обмеження конституційних прав громадян [274, с. 458].

В цьому контексті хочемо наголосити, що одним із правила подолання законодавчих прогалин є застосування аналогії права, що знайшло нормативне закріплення в ч. 6 ст. 9 КПК і зводиться до наступного: у випадках, коли положення КПК не регулюють або неоднозначно регулюють питання кримінального

---

[45] Так, ВАКС, ухвалюючи вирок 09.11.2023 у справі № 991/5570/20 виснував «Втручання у приватне спілкування в нетаємний спосіб, яким є огляд, копіювання вмісту карт пам`яті телефонів, жорстких накопичувачів ноутбуків, зовнішніх накопичувачів чи інших електронних носіїв інформації, при виконанні ухвали про тимчасовий доступ до речей та документів, виявлених під час обшуку або вилучених в результаті такого обшуку, регламентується іншими нормами КПК, ніж статті 258 (загальні положення про втручання у приватне спілкування) та 264 (зняття інформації з електронних інформаційних систем) КПК. Враховуючи, що вилучення телефону та отримання інформації з нього відбувалося у нетаємний спосіб, то орган досудового розслідування не перевищив межі дозволеного. У даному випадку детектив не мав отримувати дозвіл на проведення негласних слідчих (розшукових) дій для отримання інформації із телефону. Щодо подальшого огляду пристрою процесуальне законодавство не містило чіткої норми як діяти слідчому органу для отримання таких даних».

провадження, застосовуються загальні засади кримінального провадження, визначені ч. 1 ст. 7 КПК. Так, під час кримінального провадження кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування і втручання у таке спілкування можливе лише на ***підставі судового рішення*** **(**курсив наш - І. Смаль) у випадках, передбачених цим Кодексом, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети (ст. 14 КПК) [113].

Відмовляючи у задоволенні клопотання захисту щодо визнання недопустимим протокол огляду мобільного телефону без відповідного дозволу суду у справі № 127/13972/17, апеляційна палата ВАКС в ухвалі від 08.12.2023 року використала наступне обґрунтування[46] [до примітки див. 286; 31, п. 483–485; 284–286]; [47] [до примітки див. 161].

Таким чином, з правової позиції ВС, яка викладена в даній постанові вбачається, що огляд змісту мобільного телефону, листування без відповідного рішення суду є законним, якщо такий телефон не захищений паролем.

Водночас ч. 1 ст. 258 КПК України визначає, що ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді. Відповідно до п. 4 ч. 4 ст. 258 КПК втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що воно є приватним [113].

---

[46] «проведення огляду наявного на вилучених під час обшуку технічних пристроях особистого листування осіб, яке відбулось у минулому, і яке не має підстав проводити в умовах таємності та негласності, не є видом НСРД і не потребує попереднього отримання дозволу слідчого судді у порядку, передбаченому Главою 21 КПК для здійснення зняття інформації з електронних інформаційних систем, як і не потребує дозволу слідчого судді на тимчасовий доступ до речей і документів. Аналогічна мотивація суду і у вироку ВАКС від 27.03.2023 року (справа № 317/2973/18) ,ухвалах Апеляційної палати ВАКС від 16.01.2023 року (№ 991/6636/22), від 10 квітня 2023 року (справа № 991/2346/23).

[47] ВС у постанові від 09.04.2020 р. у справі № 727/6578/17 виснував, що зняття інформації з електронних інформаційних систем або їх частин можливе без дозволу слідчого судді, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Зі змісту ухвали вбачається, що інформація, яка малася в телефоні була досліджена слідчим шляхом включення телефону та огляду текстових повідомлень.

В наукових колах висловлюються думки, які ми повністю розділяємо, що відсутність паролю для доступу до інформації на електронному пристрої не свідчить про те, що доступ до такої інформації не обмежується її власником, володільцем або утримувачем, так як і як незамкнені двері до будинку не свідчать про надання власником добровільної згоди на проникнення до житла [362, с. 109]. Крім того, постає також питання чи законним буде доступ до носія електронної інформації, яка захищена за допомогою біометричного захисту, якщо слідчі органи мають доступ до відбитків пальців власника телефону, який вони отримали законним шляхом (наприклад при проведенні дактилоскопії). Аналогічно постає питання щодо ідентифікація по рисам обличчя. Якщо піднести телефон до обличчя і розблокувати. Чи це законно? Це можна порівняти з ситуацією, якщо підозрюваний закрився в приміщенні, то поліція має право зайти без його згоди, якщо є відповідна ухвала суду. Але зі свідком це неможливо, якщо він не дав згоди, адже свідка не можна змусити надавати докази.

На нашу думку, не можна застосовувати таку градацію щодо доступу до інформації на мобільному телефоні чи іншому пристрої у залежності від наявності чи відсутності паролю. Отже, ми вважаємо, що навіть наявність ухвали слідчого судді на проведення обшуку житла, в якій надавався дозвіл на вилучення електронних пристроїв, не дає право на втручання у право на приватне життя та право на кореспонденцію без подальшого судового контролю.

Слід звернути увагу на практику місцевих, апеляційних судів щодо процесуального вирішення питання огляду інформації, яка містить в мобільних телефонах, які вилучені органами досудового розслідування під час проведення обшуку чи затримання. Судова практика вирішує це питання в різні процесуальні способи: *1) шляхом надання доступу до речей та документів і відповідно до*

інформації, яка міститься на мобільних телефонах (ст. 163 КПК)[48] [до примітки див. 333; 342]; [49] [до примітки див. 315].

Судовим рішенням надано тимчасовий доступ (можливість ознайомитися та зробити копії) до інформації на мобільному телефоні, а саме до мобільних застосунків «Telegram», «WhatsApp», «Viber», «Signal» та смс-повідомлень, журналів вхідних та вихідних дзвінків, контактів, які містилися станом на час початку проведення обшуку [317; 319]; надано дозвіл на тимчасовий доступу до речей і документів, а саме мобільного телефону вилученого під час особистого обшуку [339]; Ухвала про надання тимчасового доступу до інформації, що міститься на носіях інформації мобільного телефону, вилученого в ході обшуку [309; 321; 332]; надано тимчасовий доступ до інформації, яка зберігається у мобільному телефоні, який добровільно виданий під час огляду місця події [344]; надано тимчасовий доступ до особистого листування та іншої інформації, яка міститься у мобільних телефонах та ноутбуках яка містилася станом на момент початку обшуку з можливістю ознайомитися та зробити копії такої інформації [305; 320].

2) шляхом зняття інформації з електронних інформаційних систем (ст. 264 КПК);[50][до примітки див. 346]; слідчим суддею Нікопольського міськрайонного

---

[48] Так, ухвалою слідчого судді Саксаганський районний суд м. Кривого Рогу від 19.02.2020 р. (справа № 214/2400/19) надано доступ до мобільного телефону, однією з підстав для надання інформації є посилання на те, що власник мобільного телефону відмовляється надати його в добровільному порядку ; слідчим суддею надано дозвіл до інформації наявної в листуваннях за допомогою месенджерів «Instagram», «Telegram», «Viber», «Facebook», «WhatsApp», доступ до яких здійснюється з мобільного телефону добровільно наданого потерпілою та іншої інформації, що міститься у ньому.

[49] Ухвалою слідчого судді Заводського районного суду м.Миколаєва від 25.04.2024 справа №487/2640/24 надано тимчасовий доступ до інформації, яка міститься у мобільних телефонах, які вилучені в ході обшуку з наступним мотивуванням «слідчим суддею враховано те, що здобути необхідну для досудового розслідування інформацію іншим шляхом, окрім як звернення до слідчого судді із цим клопотанням про надання дозволу на тимчасовий доступ до речей і документів та отримання останнього, є неможливим, оскільки зміст інформації мобільних терміналів, системних блоків, становить охоронювану законом таємницю. Копіювання інформації, що міститься у телефонах та сім-картці оператора мобільного зв`язку слідчим самостійно не є можливим в силу того, що абзац другий ч. 2 ст. 168 КПК України дозволяє копіювати інформацію виключно із інформаційних (автоматизованих) систем, телекомунікаційних систем, інформаційно-телекомунікаційних систем, а не з мобільних терміналів, які в силу їх функціональної приналежності, можуть містити охоронювану законом таємницю».

[50] Ухвалою слідчого судді Харківського апеляційного суду від 26.09.2023 р. (справа № 818/5052т/23) надано дозвіл на проведення негласної слідчої (розшукової) дії – зняття інформації з електронних інформаційних систем вилученого в ході проведення огляду мобільного телефону. Відомостями, які необхідно отримати за допомогою

суду Дніпропетровської області ухвалою від 21.12.2023 р. (справа № 182/5113/23) відмовлено в задоволенні клопотання про надання тимчасового доступу до речей і документів, до інформації, яка зберігається в мобільному телефоні, який було виявлено та вилучено під час обшуку в автомобілі з підстав, що фактично ставиться питання про втручання у приватне спілкування, шляхом зняття інформації з інформаційних систем, що врегульовано ст. 258, 264 КПК України та відноситься до негласних слідчих дій [327]; суд визнав недопустимим доказом протокол огляду, оскільки слідчим було фактично здійснено доступ до інформації щодо вмісту повідомлень електронної поштової скриньки, що є різновидом втручання у приватне спілкування, а доступ до такої інформації, відповідно до ст. 264 КПК України відноситься до негласних слідчих (розшукових) дій, і проводиться лише на підставі ухвали слідчого судді відповідного апеляційного суду [308; 324; 326; 337; 347]; слідчий звернувся з клопотання про надання тимчасового доступу до інформації у формі листування, історії дзвінків, історії переписки месенджерами, в додатках для смартфонів та персональних комп'ютерів на мобільному телефоні, який було вилучено в ході затримання підозрюваного в порядку ст. 208 КПК України, під час проведення особистого обшуку. Слідчий суддя відмовив в задоволенні клопотання з підстав, що це відноситься до повноваження слідчого судді апеляційного суду [330; 335].

3) відмова у задоволенні клопотань про надання тимчасового доступу до інформації на мобільному телефоні;

Слідчий суддя відмовив у задоволенні клопотання з мотивів, що телефон, доступ до якого просить надати слідчий, було вилучено під час особистого обшуку та ухвалою слідчого судді на нього накладено арешт. Відтак телефон є речовим

вказаної негласної слідчої (розшукової) дії є листування власника (володільця) мобільного телефону щодо планування вчинення кримінального правопорушення, контакти осіб, із якими власник (володілець) мобільного телефону планував вчинити злочин, відомості про власника (володільця) мобільного телефону, інформація про номер мобільного телефону (телефонів) SIM-карт, які знаходяться у мобільному телефоні, а також інші будь-які фактичні дані, що свідчать про протиправну злочинну діяльність. В інший спосіб отримати відомості про злочин та особу, яка його вчинила, не вбачається можливим, оскільки інформація, яка міститься у мобільному телефоні обмежена власником. Встановлений строк два місяці.

доказом та правомірно зберігається у сторони обвинувачення, підозрюваним надано дозвіл на огляду телефонів та паролі до нього. За вказаних обставин відсутня необхідність отримання ухвали слідчого судді для доступу до телефону [304].

При дослідженні судової практики з окресленої тематики нами була здійснена вибірка рішень місцевих судів різних регіонів і прикметно, що навіть після одного із останніх рішень ККС ВС від 09.04.2024 р., в якому ВС висловив категоричну позицію щодо порядку дослідження інформації, яка міститься в мобільних телефонах, місцеві суди фактично приймають рішення, які не узгоджуються з правовими позиціями ВС. Так, ВС у справі № 369/4929/19 виснував, що якщо сторона обвинувачення отримала телефон в своє володіння на підставі законно проведеного обшуку під час затримання особи, то дослідження змісту інформації, яка міститься на ньому, не потребує попереднього дозволу на це володільця телефону або слідчого судді, оскільки такий огляд інформації, що міститься в телефоні, очевидно не становить собою негласне втручання у приватне спілкування, передбачене § 2 Глави 21 КПК, положення глави 15 КПК також не можуть бути застосовані до такої ситуації (у даному випадку телефон після його вилучення знаходився у володінні сторони обвинувачення, тому вимога надати самій собі доступ до нього суперечило б здоровому глузду [197].

Дозволимо собі не погодитися з таким висновком суду, адже той факт, що мобільний телефон знаходиться у сторони обвинувачення жодним чином не означає, що інформація, яка в ньому міститься, перестає бути «приватною».

Нашу точку зору поділяють і інші судді, що можемо побачити з ухвали слідчого судді Голосіївського районного суду міста Києва в ухвалі від 09.05.2024 р. (справа № 752/3651/24),[51] [до примітки див. 307]. Аналогічний правовий висновок міститься і в інших судових рішеннях [328; 341].

---

[51] відмовляючи у задоволенні клопотання про тимчасовий доступ до речей та документів, а саме: особистого листування (в повідомленнях «What's App» «Viber» та «Telegram» та інших наявних додатках), фото-, відео галереї, телефонної книги та іншої інформації/відомостей в мобільних додатках, які містяться на належному підозрюваному мобільному телефоні, зазначив, що розгляд клопотань, щодо втручання у приватне спілкування, не належить до

Думається, що першочерговими орієнтирами в пошуку відповідей на поставлені питання на сьогодні можуть служити як окремі положення КПК, так і напрацювання судової практики, а саме місцевих суддів.

Варто зазначити, що кримінальне процесуальне законодавство формувалося фактично до появи сучасних технологій і цілком зрозуміло, що правові норми не враховують специфіки інформації в електронному вигляді, яка може використовуватися як доказ. Поява нових способів комунікації з використанням електронних технологій приводить до необхідності адаптації права як регулятора суспільних відносин до таких змін. І така адаптація законодавства повинна відбуватися якомога швидше, щоб уникнути правового вакууму у регулюванню відповідних відносин.

На нашу думку, проєкт закону України від 31.08.2020 р. № 4004 «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів», який так і не був розглянутий ВР є свідченням того, що законодавець намагається усунути законодавчі прогалини, правовий вакуум у регулюванні доступу до інформації, яка міститься в електронних інформаційних системах або їх частинах і яка не підпадає під регулювання главою 21 КПК. Законопроєкт передбачає, зокрема, нову редакцію ч. 2 ст. 264 КПК України «Пошук, виявлення і фіксація відомостей, що містяться в електронних інформаційних системах або їх частинах, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов’язаний з подоланням системи логічного захисту, є слідчою (розшуковою) дією, яка проводиться на підставі постанови прокурора, слідчого» [219], що на наше переконання суперечить засадам кримінального провадження, а саме ст. 31 КПК України та ч. 2 ст. 14 КПК України та може привести до порушення конституційного права, яке передбачає, що втручання у таємницю спілкування можливе лише на підставі судового рішення.

повноваженнь слідчого судді місцевого загального суду. Аналогічний правовий висновок міститься і в інших судових рішеннях.

Високий ступінь втручання у право на приватність покликано, щоб закон встановлював низку правових гарантій пропорційності такого втручання і відповідно відсутність гарантій від зловживань у вигляді судового контролю може становить порушення ст. 8 Конвенції[52] [до примітки див. 384, п. 49].

На нашу думку, процесуальне законодавство необхідно доповнити нормами, які б визначали можливість проведення обшуку електронного носія інформації як окремої слідчої дії. І такий дозвіл на проведення обшуку повинен бути тільки з дозволу суду. Зважаючи на вказане, вбачається за необхідне переосмислити існуючий на сьогодні законодавчий підхід стосовно цього питання та внести відповідні нормативні корективи до КПК України [див. додаток Г].

Нами вироблені наукові положення з питань використання інформації в електронному вигляді у доказовій діяльності у кримінальному провадженні, а також розроблено пропозицій щодо вдосконалення процедур обшуку носіїв електронної інформації для забезпечення прав на повагу до приватного життя та кореспонденції крізь призму європейських стандартів та сучасних вітчизняних наукових концепцій. Адже чинне законодавство України в частині збирання доказової інформації (в тому числі шляхом проведення НСРД) має відповідати підходам, закладеним у Конвенції.

У справі «Funke v. France» (1993, заява № 10828/84) ЄСПЛ підкреслює необхідність того, щоб «втручання в права можна було б визнати пропорційними поставленій законній меті», а «законодавство і практика передбачали достатні й ефективні гарантії проти зловживань». Про це Суд заявляє також у справі

---

[52] Так, у рішенні по справі «Волохи проти України» («Volokhy v. Ukraine», 2006) ЄСПЛ було висловлено наступну позицію «у національному законодавстві має існувати засіб правового захисту від свавільного втручання державних органів у право на повагу до приватного життя, приватності житла і кореспонденції... Ризик такої свавільності є особливо очевидним в умовах, коли повноваження виконавчої влади здійснюються таємно... Оскільки здійснювані на практиці заходи таємного спостереження за обміном інформації є закритими для їх ретельного аналізу з боку осіб, яких це стосується, або з боку громадськості загалом, надання правової дискреції органам виконавчої влади у вигляді необмежених повноважень було б несумісним з принципом верховенства права. Отже, закон має з достатньою чіткістю визначати межі такої дискреції, наданої компетентним органам, і порядок її здійснення, з урахуванням законної мети даного заходу, щоб забезпечити особі належний захист від свавільного втручання».

«Imakayeva v. Russia» (2006, заява № 7615/02). У справі «Bykov v. Russia» (2009, заява № 4378/02) ЄСПЛ нагадав, що наявність справедливих процедур з розгляду питання про прийнятність доказів набуває ще більшого значення тоді, коли предметом спору є «надійність доказів» [282, с. 137].

Як Суд зауважив у справі «Malone v. the United Kingdom» (1984), стаття 8 § 2 Конвенції «не лише посилається на національне законодавство, але й стосується якості закону і вимагає, щоб він відповідав верховенству права» [377].

Так, підсумовуючи та додатково аргументуючи власні міркування, наведемо позицію, висловлену з даного питання науковцями, а також результати опитування 1289 практикуючих юристів.

Параграф 2 глави 21 КПК України містить загальні положення та порядок проведення НС(Р)Д, пов’язаних із втручанням у приватне спілкування. Застосування негласних методів на сьогодні є цілком правомірним і неоспорюваним способом збирання інформації стороною обвинувачення за умови наявності системи процесуальних гарантій дотримання прав, свобод та інтересів осіб, щодо яких здійснюється такий захід [362, с. 46].

А. В. Шило в дисертаційному дослідженні звертається до питання отримання інформації з вилученої електронної техніки (персональних комп'ютерів, ноутбуків, смартфонів, телефонів тощо) та константує, що є нелогічним застосування НСРД як зняття інформації із транспортних телекомунікаційних мереж, адже, дана слідча дія передбачає «перехоплення» інформації в «онлайн» режимі і не стосується статичних електронних даних, якими є sms, електронні листи, повідомлену у різного роду месенджерах тощо [362, с. 108].

Повністю підтримуємо позицію А. В. Шило, що «наявність ухвали слідчого судді про дозвіл на обшук під час проведення якого вилучено електронний пристрій або ухвали про накладення арешту на електронний пристрій, вилучений у власника при затриманні, ще не надає права на вилучення інформації, що міститься на такому пристрої. Інформація у даному випадку є окремим об'єктом, який не слід ототожнювати з її фізичним носієм – електронним пристроєм [362, с. 109].

Продовжуючи цю логіку, відмітимо, що інформація про приватні сторони життя особи може рівною мірою міститися як в доказах, отриманих під час проведення НСРД, так і в матеріалах, отриманих шляхом гласних засобів збирання доказів.

А. В. Шило, розвиваючи думку про необхідність отримання судового дозволу для дослідження інформації з мобільного телефона, ноутбука чи іншого пристрою, зазначає, що втручання до змісту інформації на такому пристрої, можливе на підставі ухвали слідчого судді про надання тимчасового доступу до речей та документів [363, с. 176].

М. І. Демура, І. Д. Клепка, І. О. Крицька обґрунтовують позицію про необхідність адаптації досвіду окремих країн до вітчизняного кримінального процесуального законодавства щодо запровадження правила «закритого контейнеру», яким би передбачався двоступеневий судовий контроль за обмеженням права особи на таємницю спілкування при у порядку тимчасового доступу до цифрової інформації шляхом ознайомлення з нею та її копіювання [66, с. 297].

В той же час дослідники висловлюють і протилежні думки. Так, наприклад, в науковій статті С. І. Перепелиця, досліджуючи питання забезпечення права на приватне життя та кореспонденцію, зробив висновок, що відповідно до діючих процесуальних норм «слідчий суддя суду першої інстанції має право давати дозвіл на відшукання і вилучення приватних комп'ютерів та смартфонів, однак втручання в приватне спілкування осіб можливе лише на підставі ухвали слідчого судді апеляційного суду» [151, с. 77].

Повністю підтримуємо думку А. В. Скрипника про необхідність запровадження такої слідчої (розшукової) дії як цифровий обшук (пошук комп'ютерних даних, ознайомлення з ними, їх дослідження), адже це повністю відповідає сутності процесуальної дії, яка передбачає активний цілеспрямований вплив на віртуальне середовище [250].

Враховуючи вищенаведену аргументацію та підсумовуючи розгляд даного питання, на наш погляд, варто констатувати наступне.

Технології на основі Інтернету кардинально змінилися і відповідно повинно суттєво змінитися регулювання у національному законодавстві з врахуванням практики ЄСПЛ, є базові вимоги, які випливають із європейського законодавства і судової практики, а саме те, що будь який збір даних повинен мінімізувати об'єм даних які збираються чи зберігаються (аналіз на необхідність та пропорційність) і це стосується не тільки комунікацій, а й інших даних, наприклад кореспонденції. Отже, резюмуючи, зазначимо, що ухвала про дозвіл на обшук житла чи іншого володіння особи не є тим рішенням суду, що дає право на втручання у право на кореспонденцію та право на приватне, сімейне життя, гарантоване ст. 8 Конвенції, що має місце під час вилучення інформації з телефонів, комп'ютерів та інших пристроїв під час обшуку. Таким чином, національний закон не містить чітких та зрозумілих положень того, яким чином відбувається процедура вилучення та дослідження вмісту телефону, а також гарантій від свавілля. Якщо отримати кримінально значиму інформацію неможливо у відкритому доступі, а особа не надає дозволу на отримання такої інформації добровільно, слідчий повинен звернутись з відповідним клопотанням до слідчого судді. Ані ухвала про обшук, ані ухвала про арешт мобільного телефону не надає автоматичний дозвіл на доступ до наявної в ньому інформації, оскільки у жодному із зазначених рішень не досліджується питання щодо законності, необхідності та пропорційності таких дій.

Запропонуємо власне бачення нормативного врегулювання дослідження інформації в електронному вигляді з забезпечення прав людини на повагу до приватного життя та кореспонденції.

Яким чином можна отримати відомості з мобільного телефону чи комп'ютера, не оглянувши його повного змісту? В будь-якому якому випадку слідчому чи прокурору доводиться переглядати увесь зміст інформації, що міститься у пристроях, щоб відібрати докази, які мають значення для кримінального провадження. Серед такої інформації, можуть бути відповідно і

відомості що стосуються приватного, сімейного життя, така інформація може також підпадати під визначення «кореспонденція». Тобто, під час проведення обшуку (ч. 6 ст. 236 КПК України) вже відбувається втручання в права гарантовані ст. 8 Конвенції, навіть без вилучення відповідних пристроїв. Чи може відбуватися доступ до інформації, яка має ознаки приватності без порушення стандартів статті 8 Конвенції? На нашу думку, можна запропонувати таку модель поведінки агентів держави, коли функції слідчого і особи, яка здійснює перегляд такої інформації в електронному вигляді будуть розділені (це може бути експерт). Особа, яка буде здійснювали перегляд, не повинна бути зацікавленою в результатах. Відповідно, коли є певний масив інформації, слідчий має позначити мету, задля якої збирається інформація. Технічний експерт має передивитися весь вміст, але обрати і зафіксувати лише те, що має значення для справи. Окремо має бути контроль за інформацією, розголошення якої не допускається (журналістські джерела, адвокатська таємниця, таємниця нарадчої, тощо). Відібрана в такий спосіб інформація має пройти контроль слідчого судді до того як буде передана слідчому для використання у кримінальному провадженні в якості доказу. В такому випадку буде забезпечено і законність (в контексті забезпечення гарантій щодо невтручання у приватне, сімейне життя та кореспонденцію) і пропорційність такого втручання. Це може бути як один із можливих варіантів дотримання ст. 8 ЄКПЛ під час входження в «електронний простір».

Як додатковий аргумент приведемо рішення ЄСПЛ у справі «Yuditskaya and others v. Russia» (2015), в якому Суд виснував про необхідність дотримання процедур фільтрації якщо це стосується електронних даних, які зберігалися на комп’ютерах, що були вилучені слідчим під час обшуку [386].

На противагу цьому рішенні у справі «Case of Sérvulo & Associados – Sociedade de Advogados, RL and others v. Portugal» (2015) Суд постановив про відсутність порушення ст. 8 Конвенції.[53] [до примітки див. 382].

[53] Заявники скаржилися на обшук та вилучення комп'ютерних файлів та електронних повідомлень у комп'ютерній системі в їхніх офісних приміщеннях, що, як Суд зазначив (п. 75), становило втручання в їхнє право на повагу до їхньої

Що стосується втручання у приватне спілкування шляхом проведення НСРД постає також питання чи може становити проблему з погляду ст. 8 Конвенції відсутність у державі механізму захисту прав «випадкових жертв», які «постраждали» від прослуховування телефонних розмов. Обвинувачений може під час судового розгляду оспорювати хоч якось правомірність втручання у приватне спілкування (хоча і в даному випадку не має механізму захисту у випадку порушення ст. 8 Конвенції), що не скажеш про інших осіб. Так, ст. 253 КПК містить норму «Особи, конституційні права яких були тимчасово обмежені під час проведення негласних слідчих (розшукових) дій, а також підозрюваний, його захисник мають бути письмово повідомлені прокурором або за його дорученням слідчим про таке обмеження»[113]. Фактично при прослуховування телефонних розмов відбувається втручання у приватне життя не тільки підозрюваного, але й необмеженого кола осіб. Правового захисту таких осіб фактично не має. Вони не можуть захистити свої права ні в кримінальному процесі, ні в цивільному тим паче. Закріплення в ст.253 КПК вимоги про повідомлення осіб, щодо яких проводилися негласні слідчі (розшукові) дії має гарантувати право на оскарження таких дій.

В цьому аспекті звернемося до рішення ЄСПЛ у справі «Plechlo v. Slovakia» (2023)[54] [до примітки див. 378].

Рішення ЄСПЛ у справі «Contrada v. Italy (no. 4)» (2024) також має надзвичайно важливе значення в контексті зміни парадигми національного

«кореспонденції» у розумінні ст. 8 Конвенції. Суд вважає, що, незважаючи на обсяг ордерів на обшук і виїмку, гарантії, надані заявникам для запобігання зловживанню, свавіллю та порушенню професійної таємниці адвокатів, зокрема, нагляд слідчого судді, доповнений втручанням голови апеляційного суду відповідно були належними та достатніми. Таким чином, обшук і вилучення комп'ютерних документів та електронних повідомлень, які оскаржувалися в цій справі, не становили непропорційного втручання в законну мету, що переслідувалася (п. 119).

[54] В цій справі заявнику було відмовлено у перегляду законності ордеру на прослуховування телефонних розмов з огляду на його статус особи яка випадково постраждала від такого прослуховування. Держава втрутилася в його право на повагу до приватного життя та кореспонденції, записавши розмови в рамках кримінальної справи, яка його не стосувалася. За результатами дослідження цих розмов почалося розслідування вже щодо самого заявника. І він не міг ані отримати доступу до тих перемовин, ані оскаржити рішення, що санкціонує прослуховування, оскільки не мав статусу в оригінальній справі. В цій справі заявник не був фігурантом кримінальної справи, а був «випадковою жертвою» прослуховування. Суд встановив, що втручання у право заявника на повагу до його приватного життя і кореспонденції не супроводжувалося адекватними та ефективними гарантіями проти зловживань. Отже, воно не відповідало закону для цілей пункту 2 статті 8 Конвенції (п. 50).

кримінального процесуального законодавства щодо можливості оскаржень ухвал слідчих суддів про НСРД (ретроспективно), в тому числі особами, які не є підозрюваними чи обвинуваченими у кримінальному провадженні, однак чиї права були обмежені під час проведення НСРД та встановлення чітких та дієвих механізмів відшкодування шкоди. Заява стосувалася законності перехоплення телефонних розмов заявника та обшуку його житла і приміщень. Заявник скаржився на необґрунтоване втручання в його права, передбачені статтею 8, і на відсутність ефективного судового контролю за цими заходами, які були призначені в рамках провадження, в якому він не брав безпосередньої участі [373].

«Суд доходить висновку, що італійське законодавство не містить адекватних та ефективних гарантій захисту від ризику зловживань осіб, до яких застосовується захід перехоплення, але які, не будучи підозрюваними у причетності до злочину або обвинуваченими у вчиненні злочину, залишаються поза межами судового провадження. Зокрема, не передбачено можливості для таких осіб звернутися до судового органу з метою отримання ефективного перегляду законності та необхідності такого заходу і, за необхідності, отримання відповідного судового захисту» (п. 95). «Суд вважає, що італійське законодавство не відповідає вимозі щодо "якості закону" і не здатне обмежити "втручання" тим, що є "необхідним у демократичному суспільстві"» (п. 96) [373].

В рамках нашого дослідження викликає інтерес і рішення у справі «Wieser and Bicos Beteiligungen GmbH v. Austria» (2007) з точки зору аналізу законності та пропорційності[55] [до примітки див. 385].

---

[55] З фабули справи вбачається, що був проведений обшук на підставі ухвали суду у приміщенні адвокатів. У цій справі заявники не оскаржують ані обшук їхнього службового приміщення, яке є адвокатським офісом першого заявника та місцезнаходженням компанії-заявника, ані вилучення документів. Вони лише оскаржують обшук та вилучення електронних даних. Привертає увагу аргументація Суду щодо втручання саме в право на повагу до кореспонденції, а не у приватне життя. «Суд вважає, що обшук та вилучення електронних даних становили втручання у право заявників на повагу до їхньої “кореспонденції” у розумінні статті 8 … Суд повинен установити, чи відповідало втручання у право заявників на повагу до їхньої кореспонденції вимогам пункту 2 статті 8» (п. 45) і відповідно подальший аналіз втручання «згідно із законом» та пропорційність. «Що вражає у цій справі, це те, що ті самі гарантії (мова йде про документи - уточнення наше - І. Смаль) не були додержані в частині електронних даних (п. 63). Австрійський Кримінальний процесуальний кодекс містить положення щодо подвійного судового контролю (якщо власник заперечує проти вилучення документів або носіїв даних, їх слід запечатати та надати судді для прийняття

Перспективним напрямком є напрацювання наукових положень з питань використання інформації в електронному вигляді у доказовій діяльності у кримінальному провадженні, а також розроблення пропозицій щодо вдосконалення процедур обшуку носіїв інормації в електронному вигляді для забезпечення прав на повагу до приватного життя та кореспонденції. Безумовно, такі зміни мають стати можливими лише після комплексної роботи по узгодженню між собою всіх норм КПК України, пов'язаних з запропонованою категорією, та врегулювання окремих аспектів на рівні підзаконних нормативно-правових актів. Унормування питань щодо електронних доказів в кримінальних провадженнях дозволить більш ефективно проводити боротьбу з кіберзлочинністю.

В окремій думці судді Палі (concurring opinion of judge Pavli) у справі «Särgava v. Estonia» (2021) **(**основне питання у цій справі полягає в тому, чи було національне законодавство достатньо чітким і чи передбачало воно необхідні гарантії захисту адвокатської таємниці у випадку вилучення та подальшого огляду ноутбука і мобільного телефону адвоката) зазначив, що «проблеми захисту конфіденційності електронних даних продовжуватимуть займати Суд у найближчі роки. Акцент у поточному рішенні на необхідності суворої законодавчої бази в цій сфері, в тому числі щодо способів пошуку та інших специфічних цифрових механізмів, є правильним підходом. Ми повинні адаптувати фундаментальні засоби захисту до реалій цифрової епохи, не втрачаючи при цьому з поля зору сенс їхнього існування» [381].

У контексті нашого дослідження неможливо оминути увагою рішення ЄСПЛ від 23.01.2025 року у справі «Reznik v Ukraine», оскільки Суд розглядаючи питання щодо обшуку приміщення адвоката з точку зору втручання у «приватне життя», «житло» і « кореспонденцію» вкотре наголосив, що термін "кореспонденція" охоплює, серед іншого, електронну пошту та електронні файли і пристрої зберігання даних, що належать юридичним фірмам та адвокатам [379].

рішення щодо того, чи можна їх використовувати для розслідування), що фактично не було зроблено по відношенню до електронних даних. Суд констатував порушення ст. 8 Конвенції (право на повагу до кореспонденції).

Висновки зроблені в цьому рішенні ЄСПЛ мають надзвичайно важливе значення для України, оскільки вказують на необхідність внесення змін у кримінальне процесуальне законодавство.

У рішенні ЄСПЛ від 23.01.2025 року у справі «Reznik v Ukraine» Суд виснував, «вилучення носіїв інформації і передача їх на експертизу для визначення, зокрема, чи містили вони будь-яке листування через Skype або Інтернет, становили втручання у право заявника на повагу до його приватного життя, житла і кореспонденції, захищене статтею 8 Конвенції (§.62); Суд констатував, що національне законодавство, не містить жодної конкретної процедури або гарантій щодо дослідження електронних носіїв даних, які могли б запобігти розкриттю слідству електронних повідомлень, на які поширюється правова привілея (§.69); Суд також зазначає, що ордер на обшук надав правоохоронним органам дуже широкі повноваження щодо вилучення різноманітних нечітко ідентифікованих електронних носіїв інформації, не надаючи жодних конкретних інструкцій щодо того, яким чином слід захищати будь-яку конфіденційну інформацію, яка може бути знайдена на цих носіях або іншим чином у приміщенні заявника, в контексті такого вилучення (§.73); Суд зазначає, що після вилучення з житла заявника ці електронні носії були направлені на експертизу зовнішнім технічним експертам, яким було доручено ідентифікувати та вилучити, окрім документів, зазначених в ухвалі про проведення обшуку, будь-яку кореспонденцію та будь-які видалені елементи; Суд вважає, що сам факт того, що електронні пристрої адвоката, які потенційно могли містити привілійований матеріал, були вилучені та доступні посадовим особам без будь-якого зовнішнього нагляду або інших гарантій, становив, на думку Суду, непропорційне втручання у права заявника, передбачені Конвенцією (§.76); Суд визнав порушення ст. 8 , а також ст. 13 Конвенції, оскільки КПК України не передбачає можливості оскарження ухвали про проведення обшуку (§.82) [379]**.**

Про це також ЄСПЛ вказував у своєму рішенні від 05.10.2022 року у справі GOLOVAN v. UKRAINE (§ 32) [375].

Отже, у рішенні ЄСПЛ Reznik v Ukraine викладені важливі висновки, які підтверджують положення, обґрунтовані в дисертаційному дослідженні, зокрема, що електронні пошта, повідомлення в месенджерах потребують окремого правового регулювання та мають розглядатися як самостійний об'єкт захисту у межах права на «кореспонденцію» та права на «приватне життя».

Нами обґрунтовувалася думка, що положення ст. 234, 236 КПК України не містить достатньо процесуальних гарантій при проведення обшуків електронних пристроїв, які містять в собі, зокрема, об'єкти, які підпадають під захист права на «приватне життя», «кореспонденцію». Також судова практика йде по тому шляху, що проведення огляду наявного на технічних пристроях особистого листування осіб, яке відбулося в минулому, для проведення якого немає підстав проводити його в умовах таємності та негласності, не є видом НСРД і не потребує отримання дозволу слідчого судді, як і не потребує такого дозволу на тимчасовий доступ до речей і документів [202]; [286], що на нашу думку не враховує норми ст. 31 Конституції України, ст.14 КПК України та практику ЄСПЛ щодо окремого захисту права на кореспонденції в електронному вигляді.

І в світлі рішення ЄСПЛ UKRKAVA, TOV v. UKRAINE [383] можливо зробити висновок, що дотримання принципу верховенства права є гарантом передбачуваності та стабільності правової системи. Судовий активізм є корисним інструментом для усунення правових прогалин або захисту прав людини, коли законодавство є нечітким або застарілим, однак він не може замінювати законодавчу діяльність, оскільки суди не мають повноважень створювати норми права — вони їх лише застосовують та тлумачать. Якщо певне питання вимагає системного врегулювання, воно має бути вирішене через прийняття відповідних змін до законодавства.

Відповідно як результат нашого дослідження нами запропоновані зміни до законодавства, які мають на меті комплексне врегулювання питань, пов'язаних з електронними доказами, зокрема, визначення їх як самостійного процесуального джерела доказів, обов'язкового підтвердження автентичності інформації в

електронному вигляді, окремий акцент зроблено на необхідності спеціального регулювання доступу до електронної кореспонденції (електронної пошти, повідомленнях в месенджерах, СМС-листування, інших форм електронного спілкування), запровадження окремої норми щодо обшуку комп'ютерних систем та мобільних терміналів систем зв'язку (додаток Г)

Висновки до третього розділу.

1. У процесі проведеного дослідження констатовано, що показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, які визначені самостійним процесуальним джерелом доказів у кримінальному провадженні щодо кримінальних проступків, є не чим іншим, як одним із видів електронних доказів. Результат С(Р)Д, визначеної в ст.245-1 КПК України, полягає в отриманні інформації в електронному вигляді, що зафіксована технічними приладами та технічними засобами в автоматичному режимі. Запропоновані зміни до ст. 245-1 КПК України, зокрема в частині необхідності термінологічного уточнення —замість «зняття показань технічних приладів та технічних засобів» використовувати поняття «отримання електронних даних з технічних приладів та технічних засобів» та до ст.3 КПК України, доповнивши її визначенням терміна «електронні дані» — це інформація в електронному вигляді, яка придатна для сприйняття людиною після обробки автоматичними програмними засобами.

2. Враховуючи правову природу електронних доказів, а саме можливість існування на різних матеріальних носіях і бути ідентичним за змістом, необхідно на законодавчому рівні визначити необхідність підтвердження такої ідентичності. У зв'язку з цим пропонується передбачити в КПК України норму щодо обов'язкового підтвердження автентичності та цілісності інформації в електронному вигляді отриманої в результаті копіювання. Сторона обвинувачення повинна підтвердити за допомогою обчислення контрольної суми файлу або

каталогу з файлами (CRC-суми, hash-суми) або іншим технічно надійним способом відповідність копії оригіналу, що забезпечить доказову цінність такої інформації. А достовірність електронного документа повинно підтверджуватися електронним підписом. У випадку відсутності хеш кода в обов'язковому порядку призначається стороною обвинувачення експертиза, яка повинна підтвердити відповідність копії оригіналу. Допустимість доказу може заперечуватися за відсутності підтвердженого хешування або експертного дослідження.

3. Під час дослідження обґрунтовано і доведено, що національний закон не містить чітких та зрозумілих положень того, яким чином відбувається процедура вилучення та дослідження вмісту телефону, а також гарантій від свавілля. Якщо отримати кримінально значиму інформацію неможливо у відкритому доступі, а особа не надає дозволу на отримання такої інформації добровільно, слідчий повинен звернутись з відповідним клопотанням до слідчого судді. Ані ухвала суду про обшук, ані ухвала про арешт мобільного телефону не надає автоматичний дозвіл на доступ до наявної в ньому інформації, оскільки у жодному із зазначених рішень не досліджується питання щодо законності, необхідності та пропорційності таких С(Р)Д.

4. В роботі враховано можливість доступу до інформації, яка безпосередньо знаходиться не на самому носієві, а через віддалений доступ. Все це дає підстави вважати, що у слідчого (дізнавача), прокурора може з'явиться необмежена кількість інформації, яка взагалі не має відношення до кримінального провадження, але яка має відомості приватного характеру. І в цьому контексті необхідно піднімати питання забезпечення прав людини щодо захисту таємниці приватного життя та кореспонденції. У разі виявлення електронного носія інформації в ході особистого обшуку затриманого необхідно після фізичного вилучення такого пристрою отримати судове рішення щодо обшуку електронного носія інформації. Адже для того щоб втручання у право на повагу до приватного життя і кореспонденції відповідало закону та було необхідним в демократичному

суспільстві воно повинно супроводжуватися адекватними та ефективними гарантіями проти зловживань.

5. Нами вироблені наукові положення з питань використання інформації в електронному вигляді у доказовій діяльності у кримінальному провадженні, а також розроблено пропозицій щодо вдосконалення процедур обшуку носіїв електронної інформації для забезпечення прав на повагу до приватного життя та кореспонденції крізь призму європейських стандартів та сучасних вітчизняних наукових концепцій. Адже чинне законодавство України в частині збирання доказової інформації (в тому числі шляхом проведення НСРД) має відповідати підходам, закладеним ЄКПЛ.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та вирішено наукове завдання, що полягає в отриманні нових результатів у вигляді наукових висновків щодо теоретичних засад та практики застосування електронних доказів у кримінальному процесі, виявленні проблем нормативної регламентації електронних доказів та їх практичного використання, формулювання науково обґрунтованих підходів щодо можливих шляхів їх подолання. Проведене дослідження дає можливості сформулювати такі висновки та пропозиції:

1. Сучасне кримінальне процесуальне законодавство, незважаючи на його повне оновлення, все ж характеризується відставанням від стрімкого розвитку цифрових технологій та загальної цифровізації суспільних процесів. Слідча та судова практика самостійно переборює прогалини та колізії нормативного регулювання, що в країні романо-германської системи права є небажаним, адже це не сприяє правовій визначеності, захисту прав та законних інтересів осіб, що беруть участь у кримінальному провадженні, тягне за собою відсутність єдності правозастосовної практики.

2. Звернення до історичних аспектів формування концепції електронних доказів дозволило простежити періоди становлення і розвитку інституту електронних доказів у кримінальному процесуальному праві та виокремити основні періоди: І період— 1970-2000 р. Становлення доктринальних підходів щодо поняття «електронний документ»; ІІ період — 2001-2012 р. Подальший розвиток наукових уявлень щодо інформації, отриманої з електронних джерел та законодавче закріплення терміну « електронний документ»; ІІІ період— 2012-сучасний період. Прийняття КПК України, подальший доктринальний пошук оптимальних моделей використання інформації в електронному вигляді як доказу .

Запропонована періодизація становлення інституту електронних доказів дозволила проаналізувати трансформацію правового підходу до них. У процесі наукового осмислення феномену інформації в електронному вигляді в юридичній площині спочатку використовувався термін «електронний документ», який згодом

був закріплений в національному законодавстві України. Надалі це поняття зазнало еволюції— від вузького тлумачення електронного документа як носія інформації з визначеними реквізитами — до ширшого правового явища «електронних доказів». Цей процес має логічно завершитися офіційним закріпленням поняття електронних доказів у кримінальному процесуальному законодавстві, що стане важливим етапом у формуванні єдиної доктринальної та правової основи використання електронних доказів у кримінальному процесуальному доказуванні. Саме інституціоналізація електронних доказів, як окремого правового інституту, здатна забезпечити правову визначеність, посилити гарантії прав людини та сприятиме ефективності кримінального судочинства.

3. Установлені в ході дослідження характерні ознаки електронних доказів:1) нематеріальність; 2) динамічність; 3) відтворюваність; 4) залежність від технічних носіїв; 5) відсутність жорсткої прив'язки до матеріального носія; 6) наявність метаданих стали концептуальним підґрунтям для обґрунтування необхідності їх нормативного виокремлення у самостійне процесуальне джерело. Аргументацію цієї позиції доповнює комплекс об'єктивних чинників, серед яких: 1) трансформація інформаційного середовища; 2) правова визначеність та уніфікація судової практики; 3) невідповідність традиційних джерел доказів сучасним технологічним реаліям; 4) захист прав учасників кримінального провадження; 5) європейські стандарти та міжнародна практика.

4. На підставі наведених в попередньому висновку аргументів запропоновано розширити коло процесуальних джерел, виокремивши електронні докази як самостійне процесуальне джерело. З цією метою доцільно внести зміни до ст.84 КПК України, виклавши її в новій редакції «Процесуальними джерелами доказів є показання, речові докази, електронні докази, письмові докази, висновки експертів». Окрім того, пропонується доповнити главу 4 КПК України новим параграфом, у якому буде надано визначення поняття електронні докази та закріплено особливості їх процесуального статусу.

5. Класифікація електронних доказів із виокремленням релевантних критеріїв, що враховують їх походження, форму, змістовну природу та процесуальні особливості, а саме за формою існування, за способом формування, за технічним середовищем існування має важливе теоретичне та практичне значення, оскільки сприяє адаптації кримінального процесу до умов цифрової епохи, формуванню єдиних стандартів доказування з урахуванням специфіки збирання, збереження, дослідження та оцінки електронних доказів.

6. Аналіз законодавчого регулювання, наукових підходів та практики використання у судових рішеннях терміна «електронний документ» у взаємозв'язку з поняттям «електронних доказів» засвідчує, що на практиці ці поняття нерідко вживаються як синоніми. Така термінологічна невизначеність спричиняє складнощі у правозастосуванні та викликає потребу в чіткому розмежуванню понять. Проведене дослідження змісту електронного документа, його ознак, законодавчого визначення, використання як джерела доказів у судовій практиці та критерії оцінки достовірності дає нам підстави стверджувати, що його ключовою характеристикою є наявність обов'язкових реквізитів, зокрема, електронного підпису автора або підпису прирівняного до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги». Водночас ці ознаки не притаманні іншим видам електронних доказів, як то мультимедійні файли, текстові документи чи метадані, які мають іншу природу. Таке розмежування має важливе значення для формування єдиного підходу до правової оцінки інформації в електронному вигляді у кримінальному провадженні.

7. Питання використання інформації з відкритих джерел, зокрема, Інтернету, як джерела доказів у кримінальному процесі, є надзвичайно актуальним з огляду на стрімкий розвиток цифрових технологій та постійне зростання обсягу такої інформації. Проте залишається відкритим питання її правового статусу, що створює труднощі для правозастосовної практики, зокрема, в аспекті підтвердження її автентичності, цілісності, достовірності, а також встановлення

джерела її походження. Це зумовлює необхідність та перспективність подальших наукових досліджень спрямованих на формування системного підходу до правової природи та процесуального статусу інформації з відкритих джерел як джерела доказів. Огляд інформації, яка міститься у відкритих джерелах є важливим етапом у зборі електронних доказів. Проте однієї лише фіксації таких даних в порядку ст.237 КПК України недостатньо. Основна проблема полягає в тому, що цифровий контент є динамічний, його можна змінити, видалити або зробити недоступним у будь-який момент. Тому необхідно не лише зафіксувати факт наявності відповідної інформації, а й забезпечити її належне збереження та офіційне витребування.

Отже, при відсутності доступу до фізичного носія (наприклад, у випадку фіксації даних з мережі Інтернет) доцільно дотримуватися наступної процедури: 1) фіксація даних шляхом огляду інформації в порядку ст. 237 КПК України з дотриманням вимог ч. 4 ст. 99 КПК України; 2) термінове зберігання даних відповідно до процедур Будапештської конвенції (ст. 29) з подальшим скеруванням запиту в порядку ст. 548 КПК України.

8. Показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, які визначені самостійним процесуальним джерелом доказів у кримінальному провадженні щодо кримінальних проступків, є не чим іншим, як одним із видів електронних доказів. Результат С(Р)Д, визначеної в ст.245-1 КПК України, полягає в отриманні інформації в електронному вигляді, що зафіксована технічними приладами та технічними засобами в автоматичному режимі. Запропоновано зміни до ст. 245-1 КПК України, зокрема в частині необхідності термінологічного уточнення — замість «зняття показань технічних приладів та технічних засобів» використовувати поняття «отримання електронних даних з технічних приладів та технічних засобів» та до ст.3 КПК України, доповнивши її визначенням терміна «електронні дані» — це інформація в електронному вигляді, яка придатна для сприйняття людиною після обробки автоматичними програмними засобами.

9. Враховуючи правову природу електронних доказів, а саме можливість існування на різних матеріальних носіях і бути ідентичним за змістом, необхідно на законодавчому рівні визначити необхідність підтвердження такої ідентичності. У зв'язку з цим пропонується передбачити в КПК України норму щодо обов'язкового підтвердження автентичності та цілісності інформації в електронному вигляді, отриманої в результаті копіювання. Сторона обвинувачення повинна підтвердити за допомогою обчислення контрольної суми файлу або каталогу з файлами (CRC-суми, hash-суми) або іншим технічно надійним способом відповідність копії оригіналу. Це забезпечить доказову цінність такої інформації. Достовірність електронного документа має підтверджуватися накладенням електронного підпису. У разі відсутності технічного способу підтвердження цілосності та ідентичності інформації в електронному вигляді (зокрема хеш-коду), стороною обвинувачення в обов'язковому порядку має бути призначена експертиза з метою підтвердження відповідності копії оригіналу. Допустимість доказу може бути поставлена під сумнів у разі відсутності підтвердження хешування або експертного дослідження.

Запропоновано визначити в КПК України можливість надання не тільки оригінала інформації в електронному вигляді, але і її копії— за умови обов'язкового підтвердження її автентичності, цілісності та достовірності. Таке підтвердження має здійснюватися не лише шляхом хешування або іншими надійними технічними засобами, а й через забезпечення і документування ланцюга збереження відповідної інформації та обов'язкове залучення спеціалістів –фахівців у сфері інформаційних технологій.

10. Ч.6 ст.236 КПК України, яка дає дозвіл слідчому, прокурору на пошук, виявлення та фіксацію комп'ютерних даних, що містяться в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, для виявлення яких не надано дозвіл на обшук, без послідуючого судового контролю надає надмірну дискрецію слідчому, прокурору. Такий підхід не відповідає вимогам якості закону в розумінні практики ЄСПЛ, оскільки не забезпечує достатнього

рівня правової визначеності та чітких критеріїв для втручання у приватне, сімейне життя та кореспонденцію. Високий ступінь втручання у право на приватність покликаний, щоб закон встановлював низку правових гарантій пропорційності такого втручання.

Норми ст. 234, 236 КПК України не містять достатніх процесуальних гарантій при проведення обшуків електронних пристроїв, які містять в собі, зокрема, об'єкти, які підпадають під захист права на «приватне життя», «кореспонденцію». Електронна пошта, повідомлення в месенджерах потребують окремого правового регулювання та мають розглядатися як самостійний об'єкт захисту у межах права на «кореспонденцію» та права на «приватне життя».

Судова практика вирішує питання огляду інформації, яка міститься в мобільних телефонах, які вилучені органами досудового розслідування під час проведення обшуку житла, іншого володіння особи чи під час затримання особи в різні процесуальні способи: 1) надання доступу до речей та документів і відповідно до інформації, яка міститься на мобільних телефонах (ст. 163 КПК); 2) зняття інформації з електронних інформаційних систем (ст. 264 КПК); 3) відмова у задоволенні клопотань про надання тимчасового доступу до інформації на мобільному телефоні, оскільки дослідження змісту інформації, яка міститься на ньому, не потребує попереднього дозволу на це володільця телефону або слідчого судді.

11. Технології, засновані на використанні Інтернету, зазнали кардинальних змін, що в свою чергу, вимагає істотного оновлення національного кримінального процесуального регулювання із врахуванням стандартів та практики ЄСПЛ. Сьогодні існують базові правові підходи, що випливають із європейського законодавства та рішень ЄСПЛ, відповідно до яких, будь-яке втручання у приватне життя через збір даних повинно бути обмежене мінімально необхідним обсягом інформації, відповідати критеріям необхідності та пропорційності, супроводжуватися належними гарантіями захисту прав особи. Ці вимоги

поширюються не лише на комунікацію, а і на інші форми інформації в електронному вигляді, зокрема електронну кореспонденцію.

Кримінальне процесуальне законодавство України формувалося в період, коли сучасні цифрові технології ще не були розвинені, а отже не могло враховувати специфіку інформації в електронному вигляді як потенційного доказового джерела. У зв'язку з цим постає питання про доцільність зміни нормативно-правової парадигми, яка б відповідала сучасним інформаційним реаліям, зокрема в частині врегулювання порядку отримання інформації в електронному вигляді, що міститься в телефонах, комп'ютерах, інших електронних пристроях, з урахуванням вимог ст. 8 ЄКПЛ. Попри наявності законних підстав, ухвала слідчого судді про дозвіл на обшук житла чи іншого володіння особи не може автоматично охоплювати дозвіл на доступ до інформації, що міститься на мобільних телефонах, комп'ютерах та інших пристроях, оскільки таке втручання безпосередньо зачіпає право на приватне життя та кореспонденцію, гарантоване ст. 8 Конвенції. Аналогічно, ухвала слідчого судді про арешт мобільного телефону як фізичного об'єкта не може автоматично вважатися тим судовим рішенням, що надає доступ до інформації, яка в ньому міститься. Таке судове рішення ухвалюється в межах судового контролю за втручанням у право власності, гарантоване статтею 1 Протоколу 1 Конвенції, тоді як доступ до вмісту пристрою становить окреме втручання у сферу приватного життя та кореспонденції, що охоплюється гарантіями ст.8 Конвенції.

12. Технічний прогрес на стільки змінив нормативне регулювання, правозастосування, що вимагає перегляду стандартів підготовки фахівців. Програми навчання слідчих, дізнавачів, прокурорів і суддів повинні включати основи цифрової грамотності, адже без неї ефективна робота в сучасних умовах стає неможливою.

13. За результатами проведеного дослідження внесено пропозиції щодо змін до КПК України, спрямованих на комплексне врегулювання питань, пов'язаних з електронними доказами. Зокрема, пропонується визнати електронні докази

самостійним процесуальним джерелом доказів (ст.84) та доповнити Главу 4 параграфом 6, присвяченим електронним доказам. У межах запропонованих змін висунуто низку конкретних пропозицій, серед яких: перейменування статті 99 КПК України на «Письмові докази» із закріпленням визначення цього поняття; встановлення обов'язку сторони обвинувачення щодо підтвердження автентичності інформації в електронному вигляді, отриманої шляхом копіювання (ст.101-1, 104, 105, 168); запровадження обов'язкового залучення спеціаліста у разі копіювання інформації з електронних пристроїв під час проведення С(Р)Д (ст. 168, 237, 245-1); визначення необхідності спеціального правового регулювання доступу до електронної кореспонденції (електронної пошти, повідомлення в месенджерах, СМС-листування, інші форми електронного спілкування) (внесення змін до ст.236) та встановлення окремої процесуальної норми щодо обшуку комп'ютерних систем та мобільних терміналів систем зв'язку(ст.236-1).

Безумовно, реалізація запропонованих змін можлива лише за умови комплексної та зваженої роботи щодо узгодження між собою всіх норм КПК України, пов'язаних із запропонованою категорією, а також належного врегулювання окремих аспектів на рівні підзаконних нормативно-правових актів. Унормування питань щодо електронних доказів у кримінальному процесуальному законодавстві сприятиме не лише підвищенню ефективності боротьби з кіберзлочинністю, а й забезпечить належний баланс між інтересами правосуддя та захистом прав учасників кримінального провадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. Харків, 2023. Вип. 1 (30). С. 126–143. DOI: 10.32353/khrife.1.2023.07.
2. Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2017. № 1. С. 168–175.
3. Алєксєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. Київ, 2018. Вип. 2. С. 247–253.
4. Ангеленюк А.-М. Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 79, ч. 2. С. 214–218. DOI: 10.24144/2307-3322.2023.79.2.32.
5. Антонюк А. Б. Русецька В. А. Електронні докази в кримінальному провадженні. *Інтернаука. Серія: Юридичні науки*. 2020. № 10. С. 78–86.
6. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського університету. Серія: Право*. 2016. Вип. 36, т. 2. С. 123–125.
7. Ахтирська Н. М. Одержання доказів в електронній формі в світлі другого додаткового протоколу до Конвенції про кіберзлочинність. *Криміналістика і судова експертиза*. 2022. Вип. 67. С. 188–200.
8. 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, т. 2. С. 192–198. DOI: 10.24144/2307-3322.2022.72.64.

9. Барабаш А. А., Клепка Д. І. Нормативні підходи до визначення електронних доказів та порядку їх подання у процесуальному законодавстві. *Перспективні напрями розвитку кримінальної юстиції в цифрову еру : матеріали всеукр. заоч. наук.-практ. конф. (м. Харків, 24 лип. 2023 р.)*. Харків, 2023. С. 29–34.
10. Басай В. Д., Томин С. В. Дослідження віртуальних слідів – перспективний напрямок криміналістичного слідознавства. *Актуальні проблеми держави і права*. Одеса, 2008. Вип. 44. С. 220–223.
11. Басиста І. В., Гаврилюк Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти // Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право. 2024. Вип. 17. С. 227–243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243 (дата звернення: 13.04.2025).
12. Бегма А. П., Муляр Г. В., Ховпун О. С. Кримінальні проступки як новела кримінального та кримінально законодавства. *Часопис Київського університету права*. 2020. № 2. С. 365–368. DOI: 10.36695/2219-5521.2.2020.69.
13. Белоусов А. С. Использование специальных компьютерно-технических знаний при расследовании преступлений. *Вісник Запорізького національного університету. Юридичні науки*. 2006. № 3. С. 156–161.
14. Беспалько І. Л. Особливості процесуальних джерел доказів у кримінальному провадження щодо кримінальних проступків. *Громадянське суспільство як чинник модернізації сучасної держави : матеріали міжнар. наук.-практ. конф., 20 квіт. 2021 р*. Київ, 2021. С. 216–220.
15. Бєзруков Д. В. Використання оперативно-технічних засобів щодо протидії злочинам проти власності підрозділами карного розшуку : дис. … канд. юрид. наук: 12.00.09 / Донец. юрид. ін-т МВС України. Кривий Ріг, 2006. 230 с.

16. Біленчук П. Д., Гель А. П., Семаков Г. С. Криміналістична тактика і методика розслідування окремих видів злочинів : навч. посіб. Київ : МАУП, 2007. 512 с.
17. Біленчук П. Д., Кофанов А. В., Кобилянський О. Л. Комп'ютерна злочинність у кредитно-фінансовій індустрії: криміналістичний аналіз : навч. посіб. Київ : Кий, 2011. 52 с.
18. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. ... канд. юрид. наук: 12.00.09 / Класич. приват. ун-т. Київ, 2008. 18 с.
19. Білоцерковець Н. Технологічна нейтральність та заборона дискримінації як ключові принципи державного регулювання електронних довірчих послуг: поняття та ознаки. *Підприємництво, господарство і право*. 2018. № 1. С. 103–109.
20. Бірюков В. В., Коваленко В. В., Бірюкова Т. П., Ковальов К. М. Криміналістичне документознавство : практ. посіб. Київ : Паливода А. В., 2007. 332 с.
21. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів : ЛьвДУВС, 2020. 256 с.
22. Богатирьов І. Г. Актуальні проблеми запобігання кіберзлочинності в Україні. *Економіка. Фінанси. Право.* 2022. № 10/1. С. 13–17.
23. Велика українська енциклопедія : темат. реєстр з напрямку «Юрид. науки» / уклад.: В. Л. Бабка, М. М. Шумило; за ред. А. М. Киридон. Київ : Енцикл. вид-во, 2017. 152 с.
24. Велика українська юридична енциклопедія : у 20 т. Харків : Право, 2017. Т. 3. Загальна теорія права. 952 с.
25. Великий енциклопедичний юридичний словник / за ред. Ю. С. Шемшученка. 2-ге вид., переробл.і допов. Київ : Юрид. думка, 2012. 1020 с.

26. Вербіцька М., Ботвинник В. Електронні докази як новий вид доказів у адміністративному судочинстві. *Актуальні проблеми правознавства*. Тернопіль, 2020. Вип. 1. С. 48–51.
27. Вернидубов І., Белікова С. Електронні докази: поняття, особливості та проблеми щодо дослідження їх судом. *European Political and Law Discourse*. 2018. Vol. 5, Iss. 2. С. 299–305.
28. Вирок Автозаводського районного суду м. Кременчука Полтавської області від 04 травня 2007 р. у справі № 1-171/2007 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/2694538 (дата звернення: 14.04.2025).
29. Вирок Бучацького районного суду Тернопільської області від 10 березня 2023 р. у справі № 595/359/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109460422 (дата звернення: 14.04.2025).
30. Вирок Великоолександрівського районного суду Херсонської області від 29 квітня 2024 р. у справі № 650/1870/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/118734665 (дата звернення: 14.04.2025).
31. Вирок Вищого антикорупційного суду від 27 березня 2023 р. у справі № 317/2973/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109823133 (дата звернення: 14.04.2025).
32. Вирок Вищого антикорупційного суду від 09 листопада 2023 р. у справі № 991/5570/20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/114780283 (дата звернення: 14.04.2025).
33. Вирок Довгинцівського районного суду м. Кривого Рогу Дніпропетровської області від 03 жовтня 2023 р. у справі № 211/3934/22 // Єдиний державний

реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/113874884 (дата звернення: 14.04.2025).

34. Вирок Ємільчинського районного суду Житомирської області від 23 квітня 2021 р. у справі № 287/310/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/96570386 (дата звернення: 14.04.2025).
35. Вирок Жовтневого районного суду м. Запоріжжя від 04 квітня 2024 р. у справі № 331/4290/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/118116755 (дата звернення: 14.04.2025).
36. Вирок Ізмаїльського міськрайонного суду Одеської області від 06 червня 2023 р. у справі 946/5276/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/111325279 (дата звернення: 14.04.2025).
37. Вирок Краснопільського районного суду Сумської області від 07 грудня 2009 р. у справі № 1-64/09 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/8137100 (дата звернення: 14.04.2025).
38. Вирок Лебединського районного суду від 29 січня 2024 р. у справі № 950/38/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/116586853 (дата звернення: 14.04.2025).
39. Вирок Млинівського районного суду Рівненської області від 15 лютого 2022 р. у справі № 559/762/19 // Єдиний державний реєст р. у справі р судових рішень. URL: https://reyestr.court.gov.ua/Review/103303182 (дата звернення: 14.04.2025).
40. Вирок Оболонського районного суду м. Києва від 12 лютого 2024 р. у справі № 756/14896/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/116950171 (дата звернення: 14.04.2025).

41. Вирок Обухівського районного суду Київської області від 17 квітня 2023 р. у справі № 372/3820/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110291360 (дата звернення: 14.04.2025).
42. Вирок Переяслав-Хмельницького міськрайонного суду Київської області від 25 липня 2018 р. у справі № 373/1885/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/75488210 (дата звернення: 14.04.2025).
43. Вирок Сихівського районного суду м. Львова від 08 лютого 2023 р. у справі № 464/3826/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/108850834 (дата звернення: 14.04.2025).
44. Вирок Солом'янського суду м. Києва від 21 лютого 2025 р. у справі № 243/7147/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/125919734 (дата звернення: 14.04.2025).
45. Вирок Тернопільського міськрайонного суду Тернопільської області від 27 грудня 2023 р. у справі № 607/16549/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/116068192 (дата звернення: 14.04.2025).
46. Вирок Шаргородського районного суду Вінницької області від 02 червня 2023 р. у справі № 152/660/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/111273776 (дата звернення: 14.04.2025).
47. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Право*. 2020. Вип. 29. С. 281–288. DOI: 10.26565/2075-1834-2020-29-38.

48. Гетьманцев М. Електронні докази в цивільному процесі: практика застосування новел законодавства. *Підприємництво, господарство і право*. 2019. № 2. С. 19–23.
49. Гловюк І., Завтур В. Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137–IX: аналіз новел кримінального провадження // Вища школа адвокатури НААУ. 2022, 22 берез. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4514 (дата звернення: 14.04.2025).
50. Голубєв В. О. Розслідування комп'ютерних злочинів. Запоріжжя : ЗІДМУ, 2003. 296 с.
51. Гонгало С. И. Классификация электронных документов как объектов судебной технико-криминалистической экспертизы документов. *Вестник Томского государственного университета*. 2013. № 367. С. 95–97.
52. Гонгало С. Й. Електронні документи як об'єкти судової техніко-криміналістичної експертизи та їх класифікація. *Адвокат*. 2013. № 1. С. 33–36.
53. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : автореф. дис. … канд. юрид. наук: 12.00.09 / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2013. 21 с.
54. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : дис. … канд. юрид. наук: 12.00.09 / Нац. ун-т «Острозька акад.». Острог, 2013. 190 с.
55. Гонгало С. Сучасні можливості судової техніко-криміналістичної експертизи документів та перспективи її розвитку. *Право України*. 2009. № 10. С. 162–169.
56. Гончаренко В. Г. Доказування в кримінальному провадженні : наук.-практ. посіб. Київ : Акад. адвокатури України, 2014. 42 с.
57. Гончаренко С. В. Права людини інформаційної доби. *Вісник Академії адвокатури України*. 2006. № 1. С. 5–19.

58. Городецька М. С. Окремі питання забезпечення прав учасників кримінального провадження // Юридичний науковий електронний журнал. 2024. № 2. С. 402–404. URL: http://lsej.org.ua/2_2024/101.pdf (дата звернення: 14.04.2025).
59. Господарський процесуальний кодекс України : від 06 листоп. 1991 р. № 1798-XII. *Відомості Верховної Ради України*. 1992. № 6. Ст. 56. Ред. від 19.07.2024. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text (дата звернення: 14.04.2025).
60. Гринько Л. П. «Слідова картина» шахрайств, вчинених через мережу Інтернет. *Полтавський правовий часопис*. 2022. № 3. С. 16–27.
61. Грошевой Ю. М. Деякі актуальні проблеми кримінально-процесуальної теорії. *Вісник Хмельницького інституту регіонального управління та права*. 2004. № 3. С. 194–200.
62. Гусєв О. Ю. Проблеми визначення оригіналу електронного доказу в цивільному процесі України. *Проблеми законності*. Харків, 2019. Вип. 147. С. 97–109. DOI: 10.21564/2414-990x.147.175838.
63. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів : ЛьвДУВС, 2022. 204 с.
64. Гуцалюк М. В., Антонюк П. Є. Процесуальна спроможність використання електронної (цифрової) інформації як доказу в кримінальному провадженні. *Інформація і право*. 2022. № 2. С. 116–122. DOI: 10.37750/2616-6798.2022.2(41).270373.
65. Гуцалюк М. В., Антонюк П. Є. Щодо сутності електронної (цифрової) інформації як джерела доказів в кримінальному провадженні. *Криміналістичний вісник*. 2020. № 1. С. 37–49. DOI: 10.37025/1992-4437/2020-33-1-37.
66. Демура М. І., Клепка Д. І., Крицька І. О. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження. *Часопис Київського університету права*. 2020. № 1. С. 295–301.

67. Демура М. І., Клепка Д. І., Крицька І. О. Щодо обмеження прав особи під час вилучення цифрових джерел доказової інформації у кримінальному провадженні // Форум права. 2020. № 1. С. 37–46. DOI: http://doi.org/10.5281/zenodo.3577546 (дата звернення: 14.04.2025).
68. Доказування у кримінальному провадженні : навч.-практ. посіб. Київ : Нац. акад. прокуратури України. 2017. 346 с.
69. ДСТУ 2392-94. Інформація та документація. Базові поняття: Терміни та визначення. [Чинний від 1995-01-01]. Вид. офіц. Київ : Дердстандарт України, 1994. 25 с.
70. ДСТУ 2732:2004. Діловодство й архівна справа. Терміни та визначення понять. [Чинний від 2005-07-01]. Вид. офіц. Київ : Держспоживстандарт України, 2005. 36 с.
71. ДСТУ 3017-95. Видання. Основні види: Терміни та визначення. [Чинний від 1996-01-01]. Вид. офіц. Київ : Дердстандарт України, 1995. 34 с.
72. ДСТУ 4163:2020. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів. [Чинний від 2021-09-01]. Вид. офіц. URL: https://www.kdu.edu.ua/Documents/DSTU41632020v1.pdf (дата звернення: 14.04.2025).
73. 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.
74. Дубас В. М. Антикорупційне судочинство в період воєнного стану: аналіз кримінальних процесуальних змін. *Київський часопис права*. 2022. № 3. С. 127–134. DOI: 10.32782/klj/2022.3.19.
75. Електронні (цифрові) докази у кримінальних провадженнях : метод. реком. / за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во НАВС, 2020. 104 с.
76. Жеребкін В. Є. Логіка : підручник. 8-е вид., стер. Київ : Знання, 2008. 255 с.

77. Загальна декларація прав людини : прийнята резолюцією 217 А (III) Ген. Асамблеї ООН від 10 груд. 1948 р. *Офіційний вісник України*. 2008. № 93. Ст. 3103.
78. Зінковський І. П. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису як засіб збирання та перевірки доказів у досудовому розслідуванні. *Кримінальна юстиція в Україні: реалії та перспективи : матеріали круглого столу, 23 верес. 2022 р*. Львів, 2022. С. 159–163.
79. Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства // Українське право. 2018, 08 трав. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva (дата звернення: 14.04.2025).
80. Івашко С. В., Макаренко Д. В. Визнання необґрунтованими активів та їх стягнення в дохід держави: проблемні аспекти застосування законодавства. *Юридична Україна*. 2025. № 2. С. 30–38 DOI: 10.37749/2308-9639-2025-2(265)-4.
81. Інформаційна революція // Вікіпедія : вільна енцикл. 2024, 11 лют. URL: https://uk.wikipedia.org/wiki/Інформаційна_революція (дата звернення: 14.04.2025).
82. Казанчук І. В. Докази і доказування у адміністративно-деліктному процесі : автореф. дис. … канд. юрид. наук: 12.00.07. Київ, 2015. 22 с.
83. Каламайко А. Ю. Електронні засоби доказування в цивільному процесі : автореф. дис. … канд. юрид. наук: 12.00.03 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2016. 23 с.
84. Каламайко А. Ю. Електронні засоби доказування в цивільному процесі : дис. … канд. юрид. наук: 12.00.03 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2016. 242 с.

85. Каланча І. Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України: соціологічне дослідження // Успіхи і досягнення у науці. 2025. № 1. С. 78–93. DOI: https://doi.org/10.52058/3041-1254-2025-1(11)
86. Каланча І. Г. Результати OSINT як джерело доказів у кримінальному процесі України // Інновації, виклики та нові горизонти правового регулювання у світі сучасних соціально-економічних та політичних трансформацій : матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 груд. 2024 р.). Чернівці, 2024. Т. 1. С. 43–49. URL: https://hdl.handle.net/11300/28972 (дата звернення: 14.04.2025).
87. Капліна О. В. Зняття показань технічних приладів та технічних засобів: правова сутність та процесуальний порядок. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття : матеріали міжнар. наук.-практ. конф. (м. Одеса, 17 черв. 2022 р.)* : у 2 т. Одеса, 2022. Т. 2. С. 357–360.
88. Капліна О. В. Правозастосовне тлумачення норм кримінально-процесуального права : монографія. Харків : Право, 2008. 296 с.
89. Капліна О. В. Проблеми розмежування огляду комп'ютерних даних, тимчасового доступу до електронних інформаційних систем та зняття інформації з електронних інформаційних систем. *Кримінальний процес: сучасний вимір та перспективні тенденції : матеріали 6 Харків. кримін. процес. полілогу (м. Харків, 17 квіт. 2024 р.)*. Харків, 2024. С. 35–39.
90. Капліна О. В., Котова А. С. Процесуальний порядок арешту майна у кримінальному провадженні : монографія. Одеса : Гельветика, 2021. 288 с.
91. Кемп С. DIGITAL 2023 : Глобальний оглядовий звіт // DataReportal. 2023, 26 січ. URL: https://datareportal-com.translate.goog/reports/digital-2023-global-overview-report?_x_tr_sl=en&_x_tr_tl=uk&_x_tr_hl=uk&_x_tr_pto=sc (дата звернення: 14.04.2025).
92. Кіберзлочинність та електронні докази : суддя ВС розповіла про оцінку електронних доказів у кримінальному провадженні // Верховний суд. 2024, 24

квіт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1594957/ (дата звернення: 14.04.2025).

93. Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2018. Вип. 4. С. 237–245.
94. Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 202–214. DOI: 10.21564/2414-990X.161.278117.
95. Коваленко А. В. Криміналістичні вчення про збирання, дослідження та використання доказів у кримінальному провадженні» : монографія. Київ : Алерта, 2024. 558 с.
96. Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2023. Вип. 4. С. 53–58. DOI: 10.32999/ksu2307-8049/2023-4-9.
97. Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук*. 2017. № 1. С. 182–193.
98. Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : дис. … д-ра юрид. наук: 12.00.09 / Нац. ун-т «Одес. юрид. акад.». Одеса, 2018. 626 с.
99. Кодекс адміністративного судочинства України : від 06 лип. 2005 р. № 2747-IV. *Офіційний вісник України*. 2005. № 32. Ст. 1918. Ред. від 19.07.2024. URL: https://zakon.rada.gov.ua/laws/show/2747-15#top (дата звернення: 14.04.2025).
100. Кодекс України про адміністративні правопорушення (статті 213–330) : від 07 груд. 1984 № 8073-X. *Відомості Верховної Ради УРСР*. 1984. № 51. Ст. 1122. Ред. від 19.05.2024. URL: https://zakon.rada.gov.ua/laws/show/80732-10#Text (дата звернення: 14.04.2025).

101. Козинець І. Г., Кравченко В. Я. Окремі питання доказів та доказування в адміністративному судочинстві на сучасному етапі // Юридичний науковий електронний журнал. 2021. № 2. С. 173–177. DOI: https://doi.org/10.32782/2524-0374/2021-2/40 (дата звернення: 14.04.2025).
102. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні // Юридичний науковий електронний журнал. 2020. № 8. С. 418–421. DOI: https://doi.org/10.32782/2524-0374/2020-8/103 (дата звернення: 14.04.2025).
103. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. Київський часопис права. 2022. Вип. 1. С. 176–180. DOI: 10.32782/klj/2022.1.27.
104. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Страсбург, 28 січ. 1981 р. *Офіційний вісник України*. 2010. № 58. Ст. 1994; 2011. № 1. Ст. 85. Ратифікація від 06.07.2010. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 14.04.2025).
105. Конвенція про захист прав людини і основоположних свобод : (Рим, 4.XI.1950). *Офіційний вісник України*. 2006. № 32. Ст. 2371.
106. Конвенція про кіберзлочинність : Рада Європи від 23 листоп. 2001 р. *Офіційний вісник України.* 2007. № 65. Ст. 2535.
107. Конверський А. Є. Логіка (традиційна та сучасна) : підручник. Київ : Центр учб. літ., 2008. 536 с.
108. Конституція України : від 28. черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. Ред. від 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 14.04.2025).
109. Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології та захист інформації*. Запоріжжя,1998. Вип. 2. С. 70–79.

110. Кравченко О., Макарук К. Проблемні питання застосування технічних засобів фіксування та їх результатів у доказуванні у кримінальному провадженні в аспекті реформування кримінальної юстиції в Україні. *Вісник прокуратури*. 2019. № 6. С. 67–76.
111. Кримінальний кодекс України : від 05 квіт. 2001 р. № 2341-III. *Офіційний вісник України*. 2001. № 21. Ст. 920. Ред. від 19.05.2024. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 14.04.2025).
112. Кримінальний процес : підручник / за заг. ред.: А. Я. Хитра, Р. М. Шехавцов, В. В. Луцик. Львів : ЛьвДУВС, 2019. Ч. 1. 2019. 532 с.
113. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. *Офіційний вісник України*. 2012. № 37. Ст. 1370. Ред. від 19.06.2024. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 14.04.2025).
114. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301–305.
115. Крицька І. О. Речові докази у кримінальному провадженні : дис. … канд. юрид. наук: 12.00.09 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2017. 261 с.
116. Крицька І. О. Речові докази у кримінальному провадженні : монографія. Харків : Право, 2018. 276 с.
117. Кунянський С. Що не так з поглядами Верховного Суду на допустимість доказів: досліджуємо за допомогою методу чесного читання // Право без води і бруду. 2023. URL: https://kuniansky.com.ua/all/more-canons/ (дата звернення: 14.04.2025).
118. Лазукова О. В. Особливий режим досудового розслідування в умовах воєнного, надзвичайного стану або у районі проведення антитерористичної

операції : дис. ... канд. юрид. наук: 12.00.09 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2018. 263 с.

119. Левковець А. Допустимі недопустимості – блог Андрія Левковця // Pravo. 2023, 20 черв. URL: https://pravo.ua/dopustymi-nedopustymosti-bloh-andriia-levkovtsia/ (дата звернення: 14.04.2025)
120. Лейба О. А. Дефекти кримінального процесуального законодавства та засоби їх подолання : дис. … канд. юрид. наук: 12.00.09 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2018. 222 с.
121. Лисиченко В. К. Криминалистическое исследование документов (правовые и методологические проблемы) : автореф. дис. ... д-ра юрид. наук: 12.00.09 / Киев. гос. ун-т им. Т. Г. Шевченко. Киев, 1974. 66 с.
122. Лисиченко В. К. Криминалистическое исследование документов (правовые и методологические проблемы) : дис. ... д-ра юрид. наук: 12.00.09 / Киев. гос. ун-т им. Т. Г. Шевченко. Киев, 1974. 233 с.
123. Літкевич Д. О. Теоретико-правові основи використання досягнень науково-технічного прогресу у кримінальній процесуальній формі : дис. ... д-ра філософії : 081 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2020. 266 с.
124. Метелев О. П. Визначення допустимості цифрових доказів у кримінальному провадженні. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення : матеріали наук.-практ. конф. (м. Харків, 25 жовт. 2019 р.)*. Харків, 2019. С. 72–75.
125. Метелев О. П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2020. Вип. 60. С. 177–180. DOI: 10.32782/2307-3322/2020.60.39.
126. Метелев О. П. Окремі проблеми цифровізації у кримінальному процесі. *Прикарпатський юридичний вісник*. Івано-Франківськ, 2022. Вип. 3. С. 90–94. DOI: 10.32782/pyuv.v3.2022.20.

127. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238.
128. Метелев О. П. Цифрові докази як окремий вид доказів у кримінальному процесі. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення : матеріали пост. діюч. наук.-практ. семінару (м. Харків, 26 жовт. 2018 р.)*. Харків, 2018. Вип. 10 : (ювіл.). С. 100–104.
129. Міжнародний пакт про громадянські і політичні права : прийнято резолюцією 2200 А (XXI) Ген. Асамблеї ООН від 16 груд. 1966 р. // Законодавство / Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 14.04.2025).
130. Московчук Д. О. Електронні докази у країнах континентального та загального права: порівняльно-правове дослідження : дис. … д-ра філософії: 081 / Нац. ун-т «Одес. юрид. акад.». Одеса, 2023. 189 с.
131. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп’ютерних технологій : автореф. дис. … канд. юрид. наук: 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 21 с.
132. Музиченко О. В., Карандась М. В. Електронні докази як джерела доказів у межах кримінального провадження: судова практика та нормативне регулювання інших процесуальних кодексів України. *Київський часопис права*. 2022. № 2. С. 168–174. DOI: 10.32782/klj/2022.2.25.
133. Мурадов В. В. Електронні докази: криміналістичний аспект використання // Порівняльно-аналітичне право. 2013. № 3-2. С. 313–315. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf#page=316 (дата звернення: 14.04.2025).
134. Мурадов В. В. Криминалистические аспекты исследования электронных доказательств в судебном заседании. *Legea şi Viaţa*. 2014. № 4/3. С. 49–52.

135. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304–307. DOI: 10.32849/2663-5313/2019.5.56.
136. Найченко А. М. Електронні докази в господарському процесі : дис. ...д-ра філософії: 081 / Міжрегіон. акад. упр. персоналом. Київ, 2023. 252 с.
137. Никоненко М. Я. Пояснення в системі джерел доказів у кримінальних провадженнях про кримінальні проступки. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2020. № 43. С. 163–167. DOI: 10.32841/2307-1745.2020.43.36.
138. Новожилов В. С., Зозуля А. С. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису: правова природа, порядок здійснення та процесуальний результат // Форум права. 2022. № 1. С. 76–89. DOI: http://doi.org/10.5281/zenodo.6471048 (дата звернення: 14.04.2025).
139. Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники : инструктив. указания Госарбитража СССР от 29 июня 1979 г. № И-1-4 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_2783/ (дата обращения: 14.04.2025).
140. Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1. С. 12–24.
141. Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу. *Прикарпатський юридичний вісник*. Одеса, 2022. Вип. 2. С. 122–127. DOI: 10.32837/pyuv.v0i2.1028.
142. Остапчук Л. Г., Смаль І. А. Кіберзлочинність та електронні докази в кримінальному судочинстві. *Актуальні питання теорії та практики в галузі*

права, освіти, соціальних та поведінкових наук – 2021 : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 22–23 квіт. 2021 р.) : у 2 т. Чернігів, 2021. Т. 2. С. 135–138.

143. Павлишин А. А., Слюсарчук Х. Р. Стандарт доказування «достатня підстава»: тлумачення Верховного Суду США та національна практика застосування. *Правова позиція*. 2018. № 1. С. 103–110.
144. Павлова Ю. С. Електронний документ як джерело доказів у цивільному процесі : автореф. дис. … канд. юрид. наук: 12.00.03 / Нац. ун-т «Одес. юрид. акад.». Одеса, 2019. 23 с.
145. Павлова Ю. С. Електронний документ як джерело доказів у цивільному процесі : дис. ... канд. юрид. наук: 12.00.03 / Нац. ун-т «Одес. юрид. акад.». Одеса, 2019. 228 с.
146. Павлова Ю. С. Поняття та правова природа електронних доказів в теорії цивільного процесуального права. *Актуальні проблеми держави і права*. Одеса, 2017. Вип. 79. С. 102–109.
147. Палеха Ю. І., Леміш Н. О. Загальне документознавство : навч. посіб. 2-ге вид., допов. і переробл. Київ : Ліра-К, 2009. 434 с.
148. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп’ютерних технологій : автореф. дис. … канд. юрид. наук: 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2007 19 с.
149. Пашнєв Д. В. Властивості комп’ютерної інформації та особливості збирання комп’ютерних слідів. *Ученые записки Таврического национального университета им. В. И. Вернадского. Серия: Юридические науки*. 2006. Т. 19, № 2. С. 296–300.
150. Пашнєв Д. В. Особливості застосування спеціальних знань при збиранні та дослідженні слідів злочинів, що вчинені з використанням комп’ютерних технологій. *Вісник Харківського національного університету внутрішніх справ*. 2004. Вип. 27. С. 87–95.

151. Перепелиця С. І. Дотримання прав особи під час втручання у приватне спілкування в кримінальному провадженні // Форум права. 2019. № 2. С. 70–79. DOI: http://doi.org/10.5281/zenodo.2635569 (дата звернення: 14.04.2025).
152. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. *Підприємництво, господарство і право*. 2020. № 6. С. 243–247. DOI: 10.32849/2663-5313/2020.6.41.
153. Піддубна Л. П. Документ та його основні характеристики: сутність поняття, властивості, атрибути. *Науковий вісник Академії муніципального управління. Серія: Управління*. Київ, 2012. Вип. 1. С. 165–172.
154. Погорецький М. А., Кумилко А. С. Фактичні дані та їх значення для документування оперативними підрозділами злочинів у сфері рефінансування Національним банком України вітчизняних банків. *Вісник кримінального судочинства*. 2015. № 4. С. 54–62.
155. Постанова Апеляційного суду Кіровоградської області від 04 вересня 2008 р. у справі № 11-1904 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/3870303 (дата звернення: 14.04.2025).
156. Постанова Великої Палати Верховного Суду від 31 серпня 2022 р. у справі № 756/10060/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106141457 (дата звернення: 14.04.2025).
157. Постанова Великої Палати Верховного Суду від 28 лютого 2024 р. у справі № 415/2182/20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/117555176 (дата звернення: 14.04.2025).
158. Постанова Касаційного кримінального суду Верховного Суду від 25 вересня 2018 р. у справі № 210/4412/15-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/76859981 (дата звернення: 14.04.2025).

159. Постанова Касаційного кримінального суду Верховного Суду від 15 січня 2020 р. у справі № 161/5306/16-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/87053591 (дата звернення: 14.04.2025).
160. Постанова Касаційного кримінального суду Верховного Суду від 11 березня 2020 р. у справі № 149/745/14 // Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/88265263 (дата звернення: 14.04.2025).
161. Постанова Касаційного кримінального суду Верховного Суду від 09 квітня 2020 р. у справі № 727/6578/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/88749345 (дата звернення: 14.04.2025).
162. Постанова Касаційного кримінального суду Верховного Суду від 30 квітня 2020 р. у справі № 640/19897/16-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/89034985 (дата звернення: 14.04.2025).
163. Постанова Касаційного кримінального суду Верховного Суду від 20 травня 2020 р. у справі № 585/1899/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/89395920 (дата звернення: 14.04.2025).
164. Постанова Касаційного кримінального суду Верховного Суду від 10 вересня 2020 р. у справі № 751/6069/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/91722819 (дата звернення: 14.04.2025).
165. Постанова Касаційного кримінального суду Верховного Суду від 07 жовтня 2020 р. у справі № 725/1199/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/92173671 (дата звернення: 14.04.2025).
166. Постанова Касаційного кримінального суду Верховного Суду від 25 січня 2021 р. у справі № 236/4268/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/94905297 (дата звернення: 14.04.2025).
167. Постанова Касаційного кримінального суду Верховного Суду від 31 березня 2021 р. у справі № 333/1539/16-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/96071606 (дата звернення: 14.04.2025).

168. Постанова Касаційного кримінального суду Верховного Суду від 14 квітня 2021 р. у справі № 288/1418/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/96342834 (дата звернення: 14.04.2025).
169. Постанова Касаційного кримінального суду Верховного Суду від 15 вересня 2021 р. у справі № 728/1357/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/99687315 (дата звернення: 14.04.2025).
170. Постанова Касаційного кримінального суду Верховного Суду від 22 вересня 2021 р. у справі № 328/2159/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/99890264 (дата звернення: 14.04.2025).
171. Постанова Касаційного кримінального суду Верховного Суду від 30 вересня 2021 р. у справі № 498/582/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/100109348 (дата звернення: 14.04.2025).
172. Постанова Касаційного кримінального суду Верховного Суду від 26 січня 2022 р. у справі № 677/450/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/102941414 (дата звернення: 14.04.2025).
173. Постанова Касаційного кримінального суду Верховного Суду від 18 серпня 2022 р. у справі № 543/690/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105793343 (дата звернення: 14.04.2025).
174. Постанова Касаційного кримінального суду Верховного Суду від 01 вересня 2022 р. у справі № 736/2398/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106079296 (дата звернення: 14.04.2025).
175. Постанова Касаційного кримінального суду Верховного Суду від 07 вересня 2022 р. у справі № 752/165/20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106243385 (дата звернення: 14.04.2025).

176. Постанова Касаційного кримінального суду Верховного Суду від 28 вересня 2022 р. у справі № 757/38626/17-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106558696 (дата звернення: 14.04.2025).
177. Постанова Касаційного кримінального суду Верховного Суду від 03 жовтня 2022 р. у справі № 493/210/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106661432 (дата звернення: 14.04.2025).
178. Постанова Касаційного кримінального суду Верховного Суду від 10 листопада 2022 р. у справі № 686/5732/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/107354718 (дата звернення: 14.04.2025).
179. Постанова Касаційного кримінального суду Верховного Суду від 16 листопада 2022 р. у справі № 526/2314/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/107429116 (дата звернення: 14.04.2025).
180. Постанова Касаційного кримінального суду Верховного Суду від 02 грудня 2022 р. у справі № 758/1780/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/107805025 (дата звернення: 14.04.2025).
181. Постанова Касаційного кримінального суду Верховного Суду від 08 грудня 2022 р. у справі № 459/2489/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/108026328 (дата звернення: 14.04.2025).
182. Постанова Касаційного кримінального суду Верховного Суду від 14 березня 2023 р. у справі № 135/638/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109592913 (дата звернення: 14.04.2025).

183. Постанова Касаційного кримінального суду Верховного Суду від 27 квітня 2023 р. у справі № 149/2360/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110536484 (дата звернення: 14.04.2025).
184. Постанова Касаційного кримінального суду Верховного Суду від 09 травня 2023 р. у справі № 554/5867/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110807769 (дата звернення: 14.04.2025).
185. Постанова Касаційного кримінального суду Верховного Суду від 01 червня 2023 р. у справі № 464/7015/20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/111339382 (дата звернення: 14.04.2025).
186. Постанова Касаційного кримінального суду Верховного Суду від 06 червня 2023 р. у справі № 293/1947/20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/111403457 (дата звернення: 14.04.2025).
187. Постанова Касаційного кримінального суду Верховного Суду від 13 червня 2023 р. у справі № 520/2703/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/111871748 (дата звернення: 14.04.2025).
188. Постанова Касаційного кримінального суду Верховного Суду від 11 липня 2023 р. у справі № 275/368/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/112202635 (дата звернення: 14.04.2025).
189. Постанова Касаційного кримінального суду Верховного Суду від 06 вересня 2023 р. у справі № 686/2657/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/113371158 (дата звернення: 14.04.2025).

190. Постанова Касаційного кримінального суду Верховного Суду від 18 вересня 2023 р. у справі № 161/5817/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/113626920 (дата звернення: 14.04.2025).
191. Постанова Касаційного кримінального суду Верховного Суду від 17 жовтня 2023 р. у справі № 455/844/16-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/114423741 (дата звернення: 14.04.2025).
192. Постанова Касаційного кримінального суду Верховного Суду від 25 жовтня 2023 р. у справі № 755/3105/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/114581899 (дата звернення: 14.04.2025).
193. Постанова Касаційного кримінального суду Верховного Суду від 13 грудня 2023 р. у справі № 352/748/18 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/115713229 (дата звернення: 14.04.2025).
194. Постанова Касаційного кримінального суду Верховного Суду від 06 лютого 2024 р. у справі № 645/6247/16-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/116862907 (дата звернення: 14.04.2025).
195. Постанова Касаційного кримінального суду Верховного Суду від 22 лютого 2024 р. у справі № 208/3704/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/117277325 (дата звернення: 14.04.2025).
196. Постанова Касаційного кримінального суду Верховного Суду від 13 березня 2024 р. у справі № 488/470/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/117721347 (дата звернення: 14.04.2025).

197. Постанова Касаційного кримінального суду Верховного Суду від 09 квітня 2024 р. у справі № 369/4929/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/118465118 (дата звернення: 14.04.2025).
198. Постанова Касаційного кримінального суду Верховного Суду від 12 червня 2024 р. у справі № 569/1908/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/119741340 (дата звернення: 14.04.2025).
199. Постанова Касаційного кримінального суду Верховного Суду від 09 липня 2024 р. у справі № 229/1339/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/120514044 (дата звернення: 14.04.2025).
200. Постанова Касаційного кримінального суду Верховного Суду від 15 серпня 2024 р. у справі № 203/94/18,991/2/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/121051077 (дата звернення: 14.04.2025).
201. Постанова Касаційного кримінального суду Верховного Суду від 10 вересня 2024 р. у справі № 127/13972/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/122000053 (дата звернення: 14.04.2025).
202. Постанова Касаційного кримінального суду Верховного Суду від 26 листопада 2024 р. у справі № 676/6929/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/123678721 (дата звернення: 14.04.2025).
203. Постанова Касаційного кримінального суду Верховного Суду від 16 січня 2025 р. у справі № 686/18206/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/124596762 (дата звернення: 14.04.2025).

204. Постанова Касаційного кримінального суду Верховного Суду від 23 січня 2025 р. у справі № 127/28980/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/124718092 (дата звернення: 14.04.2025).
205. Постанова Касаційного кримінального суду Верховного Суду від 23 січня 2025 р. у справі № 638/6886/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/124718072 (дата звернення: 14.04.2025).
206. Постанова Об`єднаної палати Касаційного кримінального суду Верховного Суду від 29 березня 2021 р. у справі № 554/5090/16-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/96074938 (дата звернення: 14.04.2025).
207. Постанова судді Броварського міськрайонного суду Київської області від 30 серпня 2011 р. у справі № 4-347 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/45943308 (дата звернення: 15.04.2025).
208. Постанова судді військового місцевого суду Київського гарнізону від 26 березня 2009 р. у справі № 4-80 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/10811013 (дата звернення: 15.04.2025).
209. Постанова судді Вільшанського районного суду Кіровоградської області від 13 лютого 2008 р. у справі № 4-4 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/3785730 (дата звернення: 15.04.2025).
210. Постанова судді Ковпаківського районного суду м. Суми від 20 жовтня 2010 р. у справі № 4-791/10 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/11703113 (дата звернення: 15.04.2025).
211. Постанова судді Коломийського міськрайонного суду від 05 грудня 2007 р. у справі № 4-232/2007 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/5410455 (дата звернення: 15.04.2025).

212. Постанова судді Корольовського районного суду м. Житомира від 10 грудня 2007 р. у справі № 4-887 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/4441449 (дата звернення: 15.04.2025).
213. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів : Закон України від 03 жовт. 2017 р. № 2147-VIII. *Офіційний вісник України*. 2017. № 96. Ст. 2921. URL: https://zakon.rada.gov.ua/laws/show/2147-19#Text (дата звернення: 14.04.2025).
214. Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень : Закон України № 2617-VIII від 22.11.2018. *Офіційний вісник України*. 2019. № 34. Ст. 1198. Ред. від 03.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2617-19#Text (дата звернення: 14.04.2025).
215. Про внесення змін до Кримінально-процесуального кодексу України : Закон України від 25 груд. 2008 р. № 807-VI. *Офіційний вісник України*. 2009. № 2. Ст. 51. Втрата чинності: 19.11.2012.
216. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15 берез. 2022 р. № 2137-IX. *Офіційний вісник України*. 2022. № 33. Ст. 1734.
217. Про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) : проєкт Закону № 2740 від 15 січ. 2020 р. // Законопроєкти / Верхов. Рада України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67884 (дата звернення: 14.04.2025).

218. Про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) : проєкт Закону № 9484 від 17 січ. 2019 р. // Законопроєкти / Верхов. Рада України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65354 (дата звернення: 14.04.2025).
219. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : проєкт Закону України № 4004 від 01 верес. 2020 р. // Законопроєкти / Верхов. Рада України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення: 14.04.2025).
220. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за «гарячими слідами» та протидії кібератакам» : проєкт Закону № 7148, пояснювальна записка від 13.03.2022 р. // Законопроєкти / Верхов. Рада України. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1245217 (дата звернення: 14.04.2025).
221. Про внесення змін до Кримінального та Кримінально-процесуального кодексів України : Закон України від 23 груд. 2004 р. № 2289-IV. *Офіційний вісник України*. 2005. № 2. Ст. 69. Ред. від 19.11.2012. URL: https://zakon.rada.gov.ua/laws/show/2289-15/ed20121119#Text (дата звернення: 14.04.2025).
222. Про електронний цифровий підпис : Закон України від 22 трав. 2003 р. № 852-IV. *Офіційний вісник України*. 2003. № 25. Ст. 1175. Втрата чинності: 07.11.2018.
223. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV. *Офіційний вісник України*. 2003. № 25. Ст. 1174. Ред.

від 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 14.04.2025).

224. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX. *Офіційний вісник України*. 2021. № 6. Ст. 306. Ред. від 01.07.2024. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 14.04.2025).
225. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05 жовт. 2017 р. № 2155-VIII. *Офіційний вісник України*. 2017. № 91. Ст. 2764. Ред. від 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 14.04.2025).
226. Про електронну комерцію : Закон України від 3 верес. 2015 № 675-VIII. *Офіційний вісник України*. 2015. № 78. Ст. 2590. Ред. від 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 14.04.2025).
227. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : наказ МВС України від 18 груд. 2018 р. № 1026. *Офіційний вісник України*. 2018. № 11. Ст. 378.
228. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : постанова Каб. Міністрів України від 21 жовт. 2015 р. № 835. *Офіційний вісник України*. 2015. № 85. Ст. 2850. Ред. від 05.07.2024. URL: https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text (дата звернення: 14.04.2025).
229. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286. Ред. від 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 14.04.2025).

230. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. Ред. від 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 14.04.2025).
231. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII. *Офіційний вісник України*. 2015. № 63. Ст. 2075. Ред. від 18.05.2024. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 14.04.2025).
232. Про прийняття національного стандарту та скасування національного стандарту : наказ Держ. підприємства «Укр. наук.-дослід. і навч. центр проблем стандартизації, сертифікації та якості» від 25.05.2023 № 121 // Законодавство / Верхов. Рада України. URL: https://zakon.rada.gov.ua/rada/show/v0121774-23 (дата звернення: 14.04.2025).
233. Про ратифікацію Меморандуму про взаєморозуміння між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку : Закон України від 04 черв. 2015 р. № 507-VIII. *Відомості Верховної Ради України*. 2015. № 31. Ст. 296.
234. Про функціонування системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі : постанова Каб. Міністрів України від 10 листоп. 2017 р. № 833. *Офіційний вісник України*. 2017. № 92. Ст. 2800. Ред. від 19.04.2022. URL: https://zakon.rada.gov.ua/laws/show/833-2017-%D0%BF#Text (дата звернення: 14.04.2025).
235. Про чинне законодавство і проєкти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них : звіт щодо України від 3 листоп. 2016 р. № 2016/DGI/JP/3608 / Офіс Прогр. з кіберзлочинності Ради Європи ; підгот.: М. Куннапу, М. Юріч. EU ; CoE, 2016. 169 с. URL: https://rm.coe.int/16806f3743 (дата звернення: 14.04.2025).

236. Ратнова А. В. Електронний документ та його місце у системі доказів у кримінальному провадженні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2018. № 3. С. 231–241.
237. 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 (дата звернення: 14.04.2025).
238. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філософії: 081 / Львів. держ. ун-т внутр. справ. Львів, 2021. 248 с.
239. Ращенко Є. Комп'ютерні дані як носій криміналістичної інформації про злочини у сфері комп'ютерних технологій. *Правова інформатика*. 2007. № 1. С. 74–88.
240. Ревак І. О., Підхомний О. М., Яворська Т. В. Необхідність та можливості використання електронних доказів у фінансових розслідуваннях. *Наукові записки Національного університету «Острозька академія». Серія: Економіка*. 2023. № 29. С. 60–64. DOI: 10.25264/2311-5149-2023-29(57)-60-64.
241. Рішення Конституційного Суду України у справі № 1-31/2011 за конституційним поданням Служби безпеки України щодо офіційного тлумачення положення частини третьої статті 62 Конституції України : від 20 жовт. 2011 р. № 12-рп/2011. *Офіційний вісник України*. 2011. № 84. Ст. 3091.
242. Рожнова В. В. Недопустимість доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 301–306.
243. Салтевский М. В. Новый подход в технологии собирания и исследования информационных следов. *Юридический журнал*. 2008. № 1. С. 373–377.
244. Салтевський М. В. Криміналістика : підручник : у 2 ч. Харків : КонСУМ : Основа, 1999. Ч. 1. 416 с.

245. Салтевський М. В. Криміналістика у сучасному викладі : підручник. Київ : Кондор. 2005. 588 с.
246. Салтевський М. В., Гаенко В. И., Литвинов А. Н. Электронные документы в информационном обществе: проблемы формирования юридической концепции : науч.-практ. пособие. Харьков : Эспада, 2006. 96 с.
247. Сємко М. О., Крахмальов О. В. Електронна інформація як докази. *Вісник Національного технічного університету «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства*. 2021. № 1. С. 48–51. DOI: 10.20998/2227-6890.2021.1.07.
248. Сіренко О. В. Електронні докази у кримінальному провадженні. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). Ірпінь, 2019. Вип. 14. С. 208–214.
249. Січкаренко Г. Г. Документні джерела інформації : навч. посіб. Переяслав-Хмельницький : Домбровська Я. М., 2018. 212 с.
250. Скрипник А В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. ... д-ра філософії: 081 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2021. 369 с.
251. Скрипник А В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Харків: Право. 2022. 408 с.
252. Скрипник А. В. «Заборонити не можна дозволити» або проблеми огляду цифрової інформації під час обшуку затриманої особи. *Адаптація правової системи України до права Європейського Союзу: теоретичні та практичні аспекти : матеріали 5 всеукр.за міжнародною участю наук.-практ. конф. (м. Полтава, 22 жовт. 2020 р.)*. Полтава, 2020. С. 130–133.
253. Словник української мови : в 11 т. Київ : Наук. думка, 1973. Т. 4 : І – М. 840 с.
254. Словник української мови : в 11 т. Київ : Наук. думка, 1974. Т. 5 : Н – О. 840 с.
255. Словник української мови : в 11 т. Київ : Наук. думка, 1976. Т. 7 : Поїхати – Приробляти. 723 с.

256. Смаль І. А. Втручання у право на приватність під час здійснення досудового розслідування у вимірі стандартів статті 8 Конвенції про захист прав людини і основоположних свобод. *Кримінальний процес: сучасний вимір та проспективні тенденції : матеріали 6 Харків. кримін. процес. полілогу (м. Харків, 17 квіт. 2024 р.)*. Харків, 2024.

257. Смаль І. А. Історичні передумови появи електронних доказів як засобів доказування в кримінальному процесі. *Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2020 : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 23–24 квіт. 2020 р.)* : у 2 т. Чернігів, 2020. Т. 2. С. 266–268.

258. Смаль І. А. Межі втручання у приватне спілкування під час збирання електронних доказів у кримінальному процесі. *Трансформації особистості, суспільства та ринку праці: виклики майбутнього та вплив на освіту : зб. тез доп. міжнар. наук.-практ. конф., м. Харків, 20–22 верес. 2023 р.* Харків, 2023. С. 440–441.

259. Смаль І. А. Мережа Інтернету як джерело доказової інформації у кримінальному провадженні // Журнал східноєвропейського права. 2024. № 128. С. 237–243. DOI: https://doi.org/10.5281/zenodo.14212941 (дата звернення: 15.04.2025).

260. Смаль І. А. Окремі аспекти збирання та процесуального закріплення інформації з електронних носіїв. *Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квіт. 2023 р.)* : у 2 т. Чернігів, 2023. Т. 1. С. 327–330.

261. Смаль І. А. Практичні аспекти зняття показань технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі // Юридичний науковий електронний журнал. 2023. № 6. С. 552–558.

DOI: https://doi.org/10.32782/2524-0374/2023-6/127 (дата звернення: 14.04.2025).

262. Смаль І. А. Проблематика огляду носіїв цифрових даних через призму забезпечення прав та законних інтересів особи. *Інтеграція теорії у практику: проблеми, пошуки, перспективи – 2021: матеріали міжнар. наук.- практ. конф. (м. Чернігів, 5 листоп. 2021 р.)*. Чернігів, 2021. С. 186–189.
263. Смаль І. А. Проблемні аспекти застосування електронних доказів у кримінальному судочинстві. *Право і суспільство*. 2021. № 4. С. 226–232. DOI: 10.32842/2078-3736/2021.4.30.
264. Собур С. В. До питання поняття носія електронного документа. *Правова інформатика*. 2009. № 2. С. 44–48.
265. Сокиран М. Ф. Проблеми використання цифрових технологій для фіксації процесуальної інформації. *Вісник Академії адвокатури України*. 2006. № 5. С.136–144.
266. Соцький А. М. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису чи засобів фото-, кінозйомки, відеозапису // Юридичний науковий електронний журнал. 2022. № 4. С. 384–386. DOI: https://doi.org/10.32782/2524-0374/2022-4/92 (дата звернення: 14.04.2025).
267. Стахівський С. М. Теорія і практика кримінального-процесуального доказування. Київ : НАВСУ, 2005. 272 с.
268. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. Харків, 2019. Вип. 146. С. 179–191. DOI: 10.21564/2414-990x.146.171218.
269. Струк І. О., Харабуга Ю. С. Актуальні проблеми науково-методичного забезпечення при дослідженні автентичності цифрових звукозаписів. *Актуальні питання судової експертизи та криміналістики : зб. матеріалів міжнар. наук.-практ. конф., присвяч. 90-річчю створення Харків. НДІ суд.*

експертиз ім. заслуж. проф. М. С. Бокаріуса, 7–8 листоп. 2013 р. Харків, 2013. С. 165–166.

270. Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел // Верховний суд. 2022, 07 черв. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/ (дата звернення: 15.04.2025).
271. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду // Верховний суд. 2021, 28 жовт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/ (дата звернення: 15.04.2025).
272. Суддя ВС розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні в рамках курсу HELP «Кіберзлочинність та електронні докази» // Верховний суд. 2025, 05 лют. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1750192/ (дата звернення: 15.04.2025).
273. Тагієв С. Р. Проблемні питання правового регулювання використання електронних доказів у кримінальному процесі // Академічні візії. 2025. № 41. С. 1–8. URL: https://academy-vision.org/index.php/av/article/view/1742 (дата звернення: 15.04.2025).
274. Тагієв С. Р., Пузирьов М. С., Івашко С. В. Негласні слідчі (розшукові) дії в умовах війни: окремі теоретичні та практичні аспекти (частина 2) // Аналітично-порівняльне правознавство. 2023. № 2. С. 454–459. DOI: https://doi.org/10.24144/2788-6018.2023.02.79 (дата звернення: 15.04.2025).
275. Таран О. В., Тарасенко О. С. Процесуальні джерела доказів у кримінальному провадженні про кримінальні проступки. *Актуальні питання теорії та практики досудового розслідування кримінальних проступків : матеріали міжвідом. наук.-практ. круглого столу (Київ, 14 листоп. 2019 р.)*. Київ, 2019. С. 132–137.

276. Тертишник В. М. Колізії доказового права. *Наукові читання пам'яті Ганса Гросса : зб. тез міжнар. наук.-практ. конф. (м. Чернівці, 09 груд. 2021 р.)*. Чернівці, 2021. С. 220–224.
277. Тетерятник Г. К., Виходець Ю. О. Теоретичні та праксеологічні аспекти фіксування та використання у кримінальному процесуальному доказуванні інформації з інтернет-джерел // Юридичний науковий електронний журнал. 2022. № 10. С. 772–776. DOI: https://doi.org/10.32782/2524-0374/2022-10/194 (дата звернення: 14.04.2025).
278. Тітко І. А. Оцінні поняття у кримінально-процесуальному праві України : монографія. Харків : Право, 2010. 216 с.
279. Тлумачний словник з інформатики / Г. Г. Півняк та ін. Вид. 2-е, випр. і допов. Донецьк : Нац. гірн. ун-т, 2010. 600 с.
280. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с.
281. Тютюнник В. В. Інститут допустимості доказів як гарантія ухвалення законного та обґрунтованого вирок : дис. … канд. юрид. наук: 12.00.09 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2015. 220 с.
282. Уваров В. Г. Проблеми негласних слідчих (розшукових) дій. *Право і суспільство*. 2013. № 3. С. 134–140.
283. Ухвала Апеляційної палати Вищого антикорупційного суду від 19 лютого 2021 р. у справі № 487/5684/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/95013623 (дата звернення: 14.04.2025).
284. Ухвала Апеляційної палати Вищого антикорупційного суду від 16 січня 2023 р. у справі № 991/6636/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/108573094 (дата звернення: 14.04.2025).
285. Ухвала Апеляційної палати Вищого антикорупційного суду від 10 квітня 2023 р. у справі № 991/2346/23 // Єдиний державний реєстр судових рішень.

URL: https://reyestr.court.gov.ua/Review/110281196 (дата звернення: 14.04.2025).

286. Ухвала Апеляційної палати Вищого антикорупційного суду від 08 грудня 2023 р. у справі № 127/13972/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/115752525 (дата звернення: 14.04.2025).
287. Ухвала Великої Палати Верховного суду від 14 лютого 2019 р. у справі № 9901/43/19 (П/9901/43/19) // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/79883385 (дата звернення: 15.04.2025).
288. Ухвала Вищого антикорупційного суду від 01 липня 2021 р. у справі № 707/146/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/98133827 (дата звернення: 14.04.2025).
289. Ухвала Вищого антикорупційного суду від 17 лютого 2023 р. у справі № 991/667/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109173907 (дата звернення: 14.04.2025).
290. Ухвала Вищого антикорупційного суду від 26 квітня 2023 р. у справі № 991/5347/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110563113 (дата звернення: 14.04.2025).
291. Ухвала Вищого антикорупційного суду від 15 травня 2023 р. у справі № 991/3963/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110941809 (дата звернення: 14.04.2025).
292. Ухвала Житомирського апеляційного суду від 01 вересня 2022 р. у справі № 287/310/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106230420 (дата звернення: 14.04.2025).

293. Ухвала Касаційного кримінального суду Верховного Суду від 03 листопада 2022 р. у справі № 463/5461/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/107105795 (дата звернення: 14.04.2025).
294. Ухвала Касаційного кримінального суду Верховного Суду від 30 січня 2023 р. у справі № 643/6707/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/108654478 (дата звернення: 14.04.2025).
295. Ухвала Касаційного кримінального суду Верховного Суду від 21 квітня 2023 р. у справі № 635/5988/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110395927 (дата звернення: 14.04.2025).
296. Ухвала Касаційного кримінального суду Верховного Суду від 28 серпня 2023 р. у справі № 646/40/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/113121996 (дата звернення: 14.04.2025).
297. Ухвала Касаційного кримінального суду Верховного Суду від 05 вересня 2023 р. у справі № 635/520/17 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/113299868 (дата звернення: 14.04.2025).
298. Ухвала Касаційного кримінального суду Верховного Суду від 27 вересня 2023 р. у справі № 148/744/15-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/113817260 (дата звернення: 14.04.2025).
299. Ухвала Київського апеляційного суду від 09 лютого 2023 р. у справі № 759/16863/16-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109915466 (дата звернення: 14.04.2025).

300. Ухвала Олександрійського міськрайонного суду Кіровоградської області від 18 квітня 2023 р. у справі № 398/1814/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/111138573 (дата звернення: 14.04.2025).
301. Ухвала Прилуцького міськрайонного суду Чернігівської області від 04 жовтня 2023 р. у справі № 742/2247/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/114337769 (дата звернення: 14.04.2025).
302. Ухвала Пустомитівського районного суду Львівської області від 01 лютого 2024 р. у справі № 450/4548/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/116812430 (дата звернення: 14.04.2025).
303. Ухвала слідчого судді Бабушкінського районного суду м. Дніпропетровська від 17 січня 2020 р. у справі № 932/268/20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/87001237 (дата звернення: 14.04.2025).
304. Ухвала слідчого судді Бабушкінського районного суду м. Дніпропетровська від 18 квітня 2024 р. у справі № 932/3325/24 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/118575800 (дата звернення: 14.04.2025).
305. Ухвала слідчого судді Богунського районного суду м. Житомира 05 вересня 2022 р. у справі № 295/8556/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106080507 (дата звернення: 14.04.2025).
306. Ухвала слідчого судді Болградського районного суду Одеської області від 21 вересня 2022 р. у справі № 497/1823/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106368878 (дата звернення: 14.04.2025).

307. Ухвала слідчого судді Голосіївського районного суду м. Києва від 09 травня 2024 р. у справі № 752/3651/24 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/118971818 (дата звернення: 14.04.2025).
308. Ухвала слідчого судді Дарницького районного суду м. Києва 05 липня 2022 р. у справі № 753/4892/22 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/105113466 (дата звернення: 14.04.2025).
309. Ухвала слідчого судді Деснянського районного суду м. Києва від 26 жовтня 2023 р. у справі № 754/15333/23 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/114457286 (дата звернення: 14.04.2025).
310. Ухвала слідчого судді Деснянського районного суду м. Чернігова від 16 серпня 2022 р. у справі № 750/4188/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105743148 (дата звернення: 14.04.2025).
311. Ухвала слідчого судді Деснянського районного суду м. Чернігова від 23 серпня 2022 р. у справі № 750/5017/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105864006 (дата звернення: 14.04.2025).
312. Ухвала слідчого судді Деснянського районного суду м. Чернігова від 26 березня 2024 р. у справі № 750/4093/24 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/117928894 (дата звернення: 14.04.2025).
313. Ухвала слідчого судді Заводського районного суду м. Миколаєва від 09 червня 2020 р. у справі № 487/378/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/89698366 (дата звернення: 14.04.2025).
314. Ухвала слідчого судді Заводського районного суду м. Миколаєва від 19 липня 2022 р. у справі № 450/4548/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105301994 (дата звернення: 14.04.2025).

315. Ухвала слідчого судді Заводського районного суду м. Миколаєва від 25 квітня 2024 р. у справі № 487/2640/24 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/118784414 (дата звернення: 14.04.2025).
316. Ухвала слідчого судді Ізмаїльського міськрайонного суду Одеської області від 09 грудня 2022 р. у справі № 946/8451/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/107768416 (дата звернення: 14.04.2025).
317. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 04 квітня 2023 р. у справі № 202/3694/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110044416 (дата звернення: 14.04.2025).
318. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 02 травня 2023 р. у справі № 202/6872/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110555814 (дата звернення: 14.04.2025).
319. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 19 вересня 2023 р. у справі № 202/16353/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/113552856 (дата звернення: 14.04.2025).
320. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 27 грудня 2023 р. у справі № 202/7899/23 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/116064283 (дата звернення: 14.04.2025).
321. Ухвала слідчого судді Кіровського районного суду м. Дніпропетровська 03 березня 2023 р. у справі № 203/4041/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109383675 (дата звернення: 14.04.2025).

322. Ухвала слідчого судді Комунарського районного суду міста Запоріжжя від 01 червня 2022 р. у справі № 333/1938/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/104556752 (дата звернення: 14.04.2025).
323. Ухвала слідчого судді Ладижинський міський суд Вінницької області від 14 листопада 2022 р. у справі № 135/1165/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/107300055 (дата звернення: 14.04.2025).
324. Ухвала слідчого судді Луцького міськрайонного суду Волинської області від 01 вересня 2022 р. у справі № 161/11555/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106009085 (дата звернення: 14.04.2025).
325. Ухвала слідчого судді Миколаївського районного суду Львівської області від 15 вересня 2022 р. у справі № 447/1982/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106255479 (дата звернення: 14.04.2025).
326. Ухвала слідчого судді Нікопольського міськрайонного суду Дніпропетровської області від 20 січня 2022 р. у справі № 182/8177/21 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/102635016 (дата звернення: 14.04.2025).
327. Ухвала слідчого судді Нікопольського міськрайонного суду Дніпропетровської області від 21 грудня 2023 р. у справі № 182/5113/23 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/115856279 (дата звернення: 14.04.2025).
328. Ухвала слідчого судді Оболонського районного суду міста Києва від 07 травня 2024 р. у справі № 756/5595/24 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/118927970 (дата звернення: 14.04.2025).

329. Ухвала слідчого судді Овідіопольського районного суду Одеської області від 17 серпня 2023 р. у справі № 509/4789/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/112911308 (дата звернення: 14.04.2025).
330. Ухвала слідчого судді Олександрійського міськрайонного суду Кіровоградської області від 19 липня 2022 р. у справі № 398/2041/22 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/105298767 (дата звернення: 14.04.2025).
331. Ухвала слідчого судді Печерського районного суду м. Києва від 17 березня 2023 р. у справі № 757/10462/23-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109706332 (дата звернення: 14.04.2025).
332. Ухвала слідчого судді Ратнівського районного суду Волинської області від 19 січня 2023 р. у справі № 166/1059/22 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/108494851 (дата звернення: 14.04.2025).
333. Ухвала слідчого судді Саксаганського районного суду м. Кривого Рогу від 19 лютого 2020 р. у справі № 214/2400/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/87716378 (дата звернення: 14.04.2025).
334. Ухвала слідчого судді Святошинського районного суду м. Києва від 31 липня 2019 р. у справі № 759/13808/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/83480188 (дата звернення: 14.04.2025).
335. Ухвала слідчого судді Святошинського районного суду м. Києва від 25 квітня 2022 р. у справі 759/4196/22 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/104081168 (дата звернення: 14.04.2025).
336. Ухвала слідчого судді Снятинського районного суду Івано-Франківської області від 04 серпня 2022 р. у справі № 351/552/22 // Єдиний державний

реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105597364 (дата звернення: 14.04.2025).

337. Ухвала слідчого судді Солом'янського районного суду м. Києва від 28 червня 2022 р. у справі № 760/7511/22 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/104978877 (дата звернення: 14.04.2025).
338. Ухвала слідчого судді Соснівського районного суду м. Черкаси від 03 лютого 2022 р. у справі № 712/1225/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/102943930 (дата звернення: 14.04.2025).
339. Ухвала слідчого судді Суворовського районного суду м. Одеси 27 січня 2023 р. у справі № 523/1428/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/108737421 (дата звернення: 14.04.2025).
340. Ухвала слідчого судді Тернопільського міськрайонного суду Тернопільської області від 08 серпня 2022 р. у справі № 607/9884/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105704921 (дата звернення: 14.04.2025).
341. Ухвала слідчого судді Ужгородського міськрайонного суду Закарпатської області від 20 травня 2024 р. у справі № 308/8566/24 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/119161404 (дата звернення: 14.04.2025).
342. Ухвала слідчого судді Хмельницького міськрайонного суду Хмельницької області від 13 січня 2020 р. у справі № 686/540/20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/86978632 (дата звернення: 14.04.2025).
343. Ухвала слідчого судді Хмельницького міськрайонного суду Хмельницької області від 16 лютого 2023 р. у справі № 686/3258/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/109185558 (дата звернення: 14.04.2025).

344. Ухвала слідчого судді Центрального районного суду м. Миколаєва від 06 квітня 2023 р. у справі № 490/2250/23 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/110264278 (дата звернення: 14.04.2025).
345. Ухвала слідчого судді Шевченківського районного суду м. Запоріжжя від 26 серпня 2022 р. у справі № 336/3193/22 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105927604 (дата звернення: 14.04.2025).
346. Ухвала Харківського апеляційного суду від 26 вересня 2023 р. у справі № 818/5052т/23 // Єдиний державний реєстр судових рішень. URL: https://reestr.court.gov.ua/Review/115873870 (дата звернення: 14.04.2025).
347. Ухвала Шацького районного суду Волинської області від 15 вересня 2022 р. у справі № 569/1266/19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/106334653 (дата звернення: 14.04.2025).
348. Філософський енциклопедичний словник / голова редкол.: В. І. Шинкарук. Київ : Абрис, 2002. 742 с.
349. Хахановський В. Г., Гуцалюк М. В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник*. 2019. № 1. С. 13–19. DOI: 10.37025/1992-4437/2019-31-1-13.
350. Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право*. 2017. № 4. С. 80–85.
351. Хом'яченко С. І., Часова Т. О. Використання електронних доказів у кримінальному процесі. *Право. Людина. Довкілля*. 2020. Т. 11, № 2. С. 175–181. DOI: 10.31548/law2020.02.021.
352. Цехан Д. М. Правові аспекти використання цифрової інформації як доказу у кримінальному судочинстві. *Процесуальні, тактичні та психологічні проблеми, тенденції та перспективи вдосконалення досудового слідства :*

матеріали міжнар. наук.-практ. конф. (Одеса, 30 трав. 2008 р.). Одеса, 2008. С. 206–209.

353. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 5. С. 256–260.
354. Цивільний кодекс України : Закон України від . *Офіційний вісник України*. 2003. № 11. Ст. 461. Ред. від 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 14.04.2025).
355. Цивільний процесуальний кодекс України : від 18 берез. 2004 р. № 1618-IV. *Офіційний вісник України*. 2004. № 16. Ст. 1088. Ред. від 19.07.2024. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 14.04.2025).
356. Чванкін С. А. Інформаційні технології у доказуванні в цивільному процесі: теоретичні та практичні аспекти : дис. … д-ра юрид. наук: 12.00.03 / Нац. ун-т «Одес. юрид. акад.». Одеса, 2021. 488 с.
357. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 112–124.
358. 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 / Нац. ун-т внутр. справ України. Київ, 2004. 21 с.
359. Чорний С. О., Антонюк О. І. Електронні докази в цивільному процесі: проблеми застосування на практиці. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2018. Т. 1, № 10. С. 83–88.
360. Шведова О. В. Комплексне криміналістичне дослідження документів, виконаних за допомогою комп’ютерних технологій : дис. … канд. юрид. наук: 12.00.09 / Київ. нац. ун-т внутр. справ. Київ, 2006. 225 с.
361. Шевчук І. Б. Тлумачний словник основних понять і термінів програмування. Львів : ВТЗНВ, 2013. 45 с.

362. Шило А. В. Використання в кримінальному провадженні відомостей, отриманих у результаті проведення негласних слідчих (розшукових) дій : дис. … канд. юрид. наук: 12.00.09 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2019. 241 с.
363. Шило А. В. Отримання інформації з вилученої електронної техніки як спосіб збирання доказів: спірні питання практичного правозастосування. *Правові новели*. 2018. № 5. С. 172–178.
364. Школьніков В. І. Правова основа отримання інформації з мережі інтернет у кримінальному провадженні. *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право*. 2018. № 4. С. 172–176. DOI: 10.20535/2308-5053.2018.4(40).194405.
365. Штефан А. С. Веб-сайт і веб-сторінка як докази у цивільному судочинстві. *Судова апеляція*. 2017. № 4. С. 77–85.
366. Штефан А. Електронні докази: ознаки та особливості використання.*Теорія і практика інтелектуальної власності*. 2019. № 6. С. 65–80. DOI: 10.33731/62019.188333.
367. Шумило М. Є. Поняття «докази» у Кримінальному процесуальному кодексі України: спроба критичного переосмислення ідеології нормативної моделі. *Вісник Верховного Суду України*. 2013. № 2. С. 40–48.
368. Щербаковська К. О. Засоби мобільного зв’язку при розслідуванні торгівлі дітьми // Форум права. 2012. № 1. С. 1109–1113. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/5193 (дата звернення: 14.04.2025).
369. A Brief History of the Internet / B. M. Leiner et al. *ACM SIGCOMM Computer Communication Review*. 2009. Vol. 39, iss. 5. P. 22–31.
370. Approvazione del codice di procedura penale : Decreto del Presidente della Republica 22 settembre 1988, n. 447. *Gazzetta Ufficiale dela Reepubblica Italiana*. 1988. n. 250, Suppl. Ordinario n. 92. Last red.: 16.04.2025. URL: https://www.normattiva.it/uri-

res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447 (Last accessed: 06.04.2025).

371. Brown C. Computer Evidence: Collection and Preservation. New-York : Charles River Media, 2009. 518 p.
372. Case Georgia v. Russia (II) (Application no. 38263/08) : Judgment of the ECtHR of 21 Jan. 2021 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-207757 (Last accessed: 14.04.2025).
373. Case of Contrada v. Italy (no. 4) (Application no. 2507/19) : Judgment of the ECtHR of 23 May 2024 // HUDOC. URL: https://hudoc.echr.coe.int/ukr?i=001-233733 (Last accessed: 14.04.2025).
374. Case of Golder v. the United Kingdom (Application no. 4451/70) : Judgment of the ECtHR of 21 Febr. 1975 // HUDOC. URL: https://hudoc.echr.coe.int/ukr?i=001-57496 (Last accessed: 14.04.2025).
375. Case of Golovan v. Ukraine (Application no. 41716/06) : Judgment of the ECtHR of 05 Oct. 2022 // HUDOC. URL: https://hudoc.echr.coe.int/ukr?i=001-112021 (Last accessed: 14.04.2025).
376. Case of Klass and others v. Germany (Application no. 5029/71) : Judgment of the ECtHR of 6 Sept. 1978 // HUDOC. URL: http://hudoc.echr.coe.int/eng?i=001-57510 (Last accessed: 14.04.2025).
377. Case of Malone v. the United Kingdom (Application no. 8691/79) : Judgment of the ECtHR of 26 Apr. 1985 // HUDOC. URL: http://hudoc.echr.coe.int/eng?i=001-57532 (Last accessed: 14.04.2025).
378. Case of Plechlo v. Slovakia (Application no. 18593/19) : Judgment of the ECtHR of 26 Oct. 2023 // HUDOC. URL: https://hudoc.echr.coe.int/ukr?i=001-228383 (Last accessed: 14.04.2025).
379. Case of Reznik v Ukraine (Application No. 31175/14) : Judgment of ECtHR, 23 Jan. 2025 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-240192 (last accessed: 12.04.2025).

380. Case of Saber v. Norway (Application no. 459/18) : Judgment 17 Dec. 2020 : Judgment of the ECtHR of 17 Dec. 2020 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-206519 (Last accessed: 14.04.2025).
381. Case of Särgava v. Estonia (Application no. 698/19) : Judgment of the ECtHR of 16 Nov. 2021 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-213208 (Last accessed: 14.04.2025).
382. Case of Sérvulo & Associados - Sociedade de Advogados, RL and others v. Portugal (Application no. 27013/10) : Judgment of the ECtHR of 3 Sept. 2015 // HUDOC. URL: https://hudoc.echr.coe.int/ukr?i=001-156519 (Last accessed: 14.04.2025).
383. Case of Ukrkava, TOV v. Ukraine (Application No. 10233/20) : Judgment of ECtHR, 06 Febr. 2025. // HUDOC. URL: https://hudoc.echr.coe.int/ukr?i=001-241576 (last accessed: 12.04.2025).
384. Case of Volokhy v. Ukraine (Application no. 23543/02) : Judgment of the ECtHR of 2 Nov. 2006 // HUDOC. URL: http://hudoc.echr.coe.int/eng?i=001-77837 (Last accessed: 14.04.2025).
385. Case of Wieser and Bicos Beteiligungen GmbH v. Austria (Application no. 74336/01) : Judgment of the ECtHR of 16 Oct. 2007 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-82711 (Last accessed: 14.04.2025).
386. Case of Yuditskaya and others v. Russia (Application no. 5678/06) : Judgment of the ECtHR of 12 Febr. 2015 // HUDOC. URL: https://hudoc.echr.coe.int/ukr?i=001-151037 (Last accessed: 14.04.2025).
387. Casey E. Digital Evidence and Computer Crime. London : Academic Press, 2000. 780 p.
388. Casey E. The value of forensic preparedness and digital-identification expertise in smart society. *Digital Investigation*. 2017. Vol. 22. P. 1–2. DOI: 10.1016/j.diin.2017.09.001.
389. Chisum J. W. Crime Reconstruction and Evidence Dynamics. *The Forensic Laboratory Handbook Procedures and Practice* / eds.: A. Mozayani, C. Noziglia.

Totowa, NJ : Humana Press, 2010. P. 105–122. DOI: 10.1007/978-1-60761-872-0_4.

390. Code de procédure pénale : version consolidée au 2 novembre 2018 // Legifrance. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154 (Last accessed: 05.04.2025).
391. Code of Criminal Procedure of The Republic of Estonia = Kriminaalmenetluse seadustik : Passed 12 Febr. 2003 // Riigi Teataja. URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/509012019001/consolide (Last accessed: 06.04.2025).
392. Código de Processo Penal – CPP : Decreto-Lei n.º78/87. *Diário da República, Série I*. 1987. n.º40. Versão à data de 2025-04-15. URL: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075 (Last accessed: 05.04.2025).
393. Criminal Procedure Code of the Republic of Lithuania : Passed 14 March 2002 // ICC Legal Tools Database. URL: https://www.legal-tools.org/doc/70b7df/ (Last accessed: 15.04.2025).
394. Criminal Procedure Law of The Republic of Latvia = Krimināl procesa likums : Passed 21.04.2005. *Latvijas Vēstnesis*. 2005. No. 74. Last red.: 26.02.2005. URL: https://likumi.lv/ta/id/107820-kriminalprocesa-likums (Last accessed: 06.07.2025).
395. Developments in the Field of Information and Telecommunications in the Context of International Security : Resolution A/RES/53/70 adopted by the UNGA on 4 Dec. 1998 // United Nations Digital Library. URL: https://digitallibrary.un.org/record/285350?ln=en (Last accessed: 14.04.2025).
396. Developments in the field of Information and Telecommunications in the Context of International Security : Resolution A/RES/54/49 adopted by the UNGA on 1 Dec. 1999 // United Nations Digital Library.

URL: https://digitallibrary.un.org/record/404489?ln=en (Last accessed: 14.04.2025).

397. German Code of Criminal Procedure = Strafprozeßordnung (StPO) : of 12.09.1950. *Bundesgesetzblatt*. 1987. Pt I. P. 1074, 1319. Last red.: 21.02.2024. URL: https://www.gesetze-im-internet.de/englisch_stpo/ (Last accessed: 05.04.2025).
398. Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence / Council of Europe, European Court of Human Rights. ECtHR, 2024. 180 p. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng (Last accessed: 14.04.2025).
399. ICC Digital Platform: Timbuktu, Mali // SITU Research. URL: https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali (Last accessed: 14.04.2025).
400. Information Society and Development Conference, Midrand, 13–15 May 1996 : Chair's Conclusion. *The Information Society and Development: the Role of the European Union Communication from the Commission to the Council to the European Parliament to the Economic and Social Committee and to the Committee of the Regions*. Brussels : Commission of the European Communities, 1997. P. 24–29. URL: https://aei.pitt.edu/5649/1/5649.pdf (Last accessed: 14.04.2025).
401. International Electronic Evidence / ed. S. Mason. London : British Institute of International and Comparative Law, 2008. 1002 p.
402. ISO 12651-1:2012. Electronic document management – Vocabulary. Part 1: Electronic document imaging. [1st edn 2012-01-15]. Geneva : ISO copyright office, 2012. 18 c.
403. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. [1st edn 2012-10-15]. Geneva : ISO copyright office, 2012. 38 p.

404. List of ISO Standards for Digital Forensics // Digital Forensics Myanmar. 2020, 5 Jan. URL: https://www.forensicsmyanmar.com/2020/01/list-of-iso-standards-for-digital.html (Last accessed: 14.04.2025).
405. Manes G., Downing E., Watson L., Thrutchley C. New Federal Rules and Digital Evidence. *Annual ADFSL Conference on Digital Forensic, Security and Law*. Arlington, Virginia, 18–20 Apr. 2007. P. 31–40. URL: https://commons.erau.edu/adfsl/2007/session-6/3 (Last accessed: 14.04.2025).
406. Mason S. Electronic Signatures in Law. 4th edn. London : Institute of Advanced Legal Studies, 2016. 418 p. DOI: 10.14296/117.9781911507017.
407. Mason S. Report on the Use of Electronic Evidence in Civil and Administrative Law Proceedings and its Effect on the Rules of Evidence and Modes of Proof : A Comparative Study and Analysis, 27 July 2016. Strasbourg : CDCJ, 2016. 56 p. URL: https://rm.coe.int/1680700298 (Last accessed: 14.04.2025).
408. Mason S., Seng D. Electronic Evidence. 4th edn. London : Institute of Advanced Legal Studies, 2017. 379 p.
409. Moore J. L. Time for an Upgrade : Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation. *Jurimetrics*. 2010. Vol. 50, iss. 2. P. 147–193.
410. Resolution No 1 on the Links between Corruption and Organised Crime // 21st Conference of European Ministers of Justice «Links Between Corruption and Organised Crime» 10–11 June, Prague, Czech Republic. URL: https://www.coe.int/en/web/human-rights-rule-of-law/mju21-1997-prague(Last accessed: 14.04.2025).
411. Role of Science and Technology in the Context of International Security and Disarmament : Resolution A/RES/54/50 adopted by the UNGA on 1 Dec. 1999 // United Nations Digital Library. URL: https://digitallibrary.un.org/record/404030?ln=en (Last accessed: 14.04.2025).

412. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence : Special edition dedicated to the drafters of the Protocol, 17 Nov. 2021. Strasbourg : Council of Europe, 2021. 125 p. URL: https://rm.coe.int/168008160f (Last accessed: 14.04.2025).
413. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence : Strasbourg, 12.V.2022. *Council of Europe Treaty Series*. No. 224. URL: https://rm.coe.int/1680a49dab (Last accessed: 05.04.2025).
414. SITU – Codec, a Collaborative Tool for Managing Video Evidence // SITU Research. URL: https://situ.nyc/research/projects/codec-collaborative-tool (Last accessed: 14.04.2025).
415. Standard Operating Procedures for the Collection, Analysis and Presentation of Electronic Evidence / Cybercrime Programme Office of the Council of Europe (C-PROC). EU : CoE, 2019. 39 p. URL: https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb (Last accessed: 14.04.2025).
416. The Admissibility of Electronic Evidence in Court: Fighting Against High-Tech Crime / B. Schafter et al. Barcelona : Cyber Experience S.L., 2006. 64 p.
417. The Promotion, Protection and Enjoyment of Human Rights on the Internet : Resolution A/HRC/RES/32/13 adopted by the UNHRC on 1 July 2016 // United Nations Digital Library. URL: https://digitallibrary.un.org/record/845727?ln=en (Last accessed: 14.04.2025).
418. The role of transnational electronic evidence in the investigation of crimes / Akhtyrska N., Kostiuchenko O., Sereda Y., Vynohradova A., Miroshnykov I. // Amazonia Investiga. 2023. Vol. 12, no. 71. P. 293–303. URL: https://amazoniainvestiga.info/index.php/amazonia/article/view/2604 (дата звернення: 15.04.2025).
419. U. S. Constitution // Legal Information Institute (LII). URL: https://www.law.cornell.edu/constitution (Last accessed: 14.04.2025).

420. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998. New York : UN Publication, 1999. 74 p. URL: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf (Last accessed: 14.04.2025).
421. United Nations. 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 ; Geneva : Human Rights Center ; OHCHR, 2022. 87 p.

ДОДАТКИ

Додаток А

АНКЕТА

Шановний респонденте!

На кафедрі кримінального, кримінально-виконавчого права та кримінології Академії Державної пенітенціарної служби України проводиться дослідження практики застосування електронних доказів у кримінальному процесі. Таке дослідження потребує активної допомоги практичних працівників. З метою виявлення проблем, які виникають під час збирання доказової інформації в електронній формі, оцінки доказів у кримінальному провадженні щодо кримінальних проступків та злочинів, формування пропозицій щодо їх подолання, просимо Вас взяти участь у анкетуванні та надати відверті відповіді на поставлені в анкеті питання. Думка практикуючих працівників має для нас визначальне значення. Ваші відповіді будуть покладені в основу наукового дослідження за темою « Теоретичні засади формування та практика застосування електронних доказів у кримінальному процесі».

Даючи відповідь на запитання, позначте варіант (або декілька варіантів), що відповідає (відповідають) Вашій позиції. Якщо жоден із запропонованих варіантів відповідей не відповідає Вашому переконанню, можете зазначити свою точку зору.

Анкетування є анонімним: прізвище, ім’ я та по батькові вказувати не потрібно. Дякуємо за участь в опитуванні!

Відповіді можна надсилати на електронну адресу: sia1901@ukr.net

1. **Вкажіть ,будь ласка, Ваше місце роботи та посаду** :

_____

2. Ваш стаж роботи на посаді :

□ до 1 року
□ від 1 року
□ до 3 років
□ від 3
□ до 5 років
□ від 5 до 10 років
□більш 10 років

3. Який термін, на Вашу думку, найбільш коректно вживати для позначення інформації з комп'ютерів, смартфонів, планшетів, інших технічних пристроїв?

□ електронна інформація
□ цифрова інформація
□ інформація з електронних носіїв
□ інформація з цифрових носіїв
□ комп'ютерна інформація
□ електронні докази
□ цифрові докази
□ електронний документ
□ інше:

_____

4.Чи вважаєте Ви за необхідне виділити електронні (цифрові) докази як окреме джерело доказів у кримінальному процесі?

□ так
□ ні
□ інше:

_____

***5*.Чи вважаєте Ви достатнім та повним нормативне регулювання процесуального порядку збирання електронних (цифрових) доказів?**

□ так
□ ні
□ складно відповісти
□ інше:

_____

6. Чи не вважаєте Ви за необхідне регламентувати в окремій главі КПК України процесуальний порядок вилучення, фіксації, критерії оцінки електронних доказів?

□ так
□ ні
□ складно відповісти
□ інше:

_____

7. На які дефекти чинного кримінального процесуального законодавства стосовно унормування процесуального порядку збирання електронних (цифрових) доказів Ви можете вказати?

_____

8.Чи були труднощі з оцінкою відомостей (фактичних даних), отриманих з електронних носіїв ?

□ так
□ ні
□ складно відповісти
□ інше:

_____

9. З якими видами електронних доказів Ви стикалися у своїй практиці ?

□ відеозаписи
□ аудіозаписи
□ цифрові фотографії та зображення
□ електронні повідомлення(смс-та ммс-повідомлення, електронна пошта)
□ вебсайти (вебсторінки)
□ дані геолокації
□ комп'ютерні дані
□ електронні документи
□ інше

_____

10. Чи існують відмінності у тактиці збирання «традиційних» доказів та електронних (цифрових) доказів?

□ так
□ ні
□ складно відповісти
□ інше:

_____

11.Чи необхідно залучати спеціаліста під час збирання електронних (цифрових) доказів?

□ так
□ ні

□ в окремих випадках
□ складно відповісти
□ інше:

_____

12.Чи необхідно залучати спеціаліста під час дослідження електронних (цифрових) доказів?

□ так
□ ні
□ в окремих випадках
□ складно відповісти
□ інше:

_____

13. Що, на Вашу думку, потрібно для того, щоб використовувати як доказ фактичні дані отримані з електронного носія інформації?

□ подання оригіналу технічного носія інформації в електронному вигляді
□ подання копії інформації в електронному вигляді
□ подання копії інформації в електронному вигляді, виготовленої спеціалістом
□інше

_____

14.Чи є логічним на Вашу думку вживання поняття «дублікат» для позначення електронних доказів, в тому числі і електронних документів ?

□ так
□ ні
□ складно відповісти
□ інше:

_____

15. Чи має на Вашу думку значення для допустимості доказів джерело доказів (тобто чи буде доказом фактичні дані отримані з не передбаченого КПК джерела доказів) ?

□ так
□ ні
□ інше:

_____

16. Чи має на Вашу думку значення для допустимості доказів порядок отримання доказів (тобто якщо фактичні дані отримані в не передбаченому КПК порядку)?

□ так
□ ні
□ інше:

_____

17. Чи відчували Ви труднощі під час збирання та дослідження електронних доказів?)

□ так
□ ні
□ інше

_____

18. Якщо так, то які саме? (декілька варіантів відповідей)

□ Відсутність законодавчого закріплення поняття електронних доказів та критеріїв їх оцінки
□ Складність встановлення оригіналу, копії, дублікату інформації в електронній формі
□ Відсутність базових знань у сфері інформаційних технологій
□ Вербалізація(словесне вираження) у процесуальних документах та інших матеріалах кримінального провадження процесів, пов'язаних із збиранням та використанням інформації в електронному вигляді
□ Відсутність сформованої методики збирання
□ Відсутність технічних засобів для копіювання, вилучення, транспортування, зберігання таких доказів
□ Відсутність достатньої кількості спеціалістів для залучення до проведення слідчих (розшукових) дій
□ інше

_____

19. Чи виникали у Вас труднощі із збиранням доказів в порядку ст.245-1 КПК України ?

□ так
□ ні
□ інше

_____

20. Чи виникали у Вас труднощі з оцінкою доказів, отриманих в порядку ст.245-1 КПК України ?

□ так
□ ні
□ інше

_____

21. Як Ви вважаєте чи є коректним термін «показання», який використовується для позначення фактичних даних отриманих в порядку ст.245-1 КПК України ?

□ так
□ ні
□ інше

_____

22. Як Ви вважаєте, чи може слідчий проводити слідчу (розшукову)дію в порядку ст.245-1 КПК України у кримінальних провадженнях щодо злочинів?

□ так
□ ні
□ інше

_____

23. Як Ви вважаєте, чи можна використовувати як докази фактичні дані отримані слідчим в порядку ст.245-1 КПК України у кримінальних провадженнях щодо злочинів?

□ так
□ ні
□ інше

_____

24. Чи отримували Ви відмову (відмовляли) у задоволенні клопотання про надання тимчасового доступу до речей і документів у випадку необхідності отримання копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб у кримінальному провадженні щодо проступків?

□ так
□ ні
□ підставою відмови було необхідність отримання відповідної інформації в порядку ст.245-1 КПК України
□ інше

_____

25. Чи отримували Ви відмову (відмовляли) у задоволенні клопотання про надання тимчасового доступу до речей і документів у випадку необхідності отримання копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб у кримінальному провадженні щодо злочинів ?

□ так
□ ні
□ підставою відмови було необхідність отримання відповідної інформації в порядку ст.245-1 КПК України
□ інше

_____

26. Як Ви вважаєте, чи є необхідним викладення ст.245-1 КПК України в іншій редакції ? Якщо так, то які потрібно внести зміни ?
□ так
□ ні
□ інше

_____

27. Як Ви вважаєте, чи є доцільним виділення процесуальних джерел доказів у кримінальних проступках (ст.298-1 КПК України)?

□ так
□ ні
□ інше

_____

28. Які питання повинен дослідити слідчий суддя при прийняття рішення за клопотанням прокурора про надання дозволу на використання процесуальних джерел доказів у кримінальних провадженнях щодо злочинів у порядку ст.298-1 КПК України?

□ задовольнити клопотання автоматично, якщо такі докази, передбачені ч.1 ст.298-1 КПК України
□ відмовити у задоволені клопотання, якщо порушені права,свободи та інтереси

осіб у кримінальному провадженні
□ інше

_____

29. Чи були у Вашій практиці випадки, коли знімали показання технічних приладів і технічних засобів у провадженнях щодо вчинення кримінальних проступків, що мають функції фото-і кінозйомки, відеозапису до внесення відомостей про кримінальний проступок до Єдиного реєстру досудових розслідувань.

□ так
□ ні
□ інше

_____

30. Чи вважаєте Ви за необхідне поширення поняття кореспонденція на листування в застосунках для обміну повідомленнями, електронній пошті ?
□ так
□ ні
□ інше

_____

31. Чи буде на Вашу думку втручання у приватне спілкування коли при затриманні особи слідчий, дізнавач отримує доступ до листування в застосунках для обміну повідомленнями, електронній пошті, зокрема, в мобільних телефонах без відповідного дозволу слідчого судді ?
□ так
□ ні
□ інше

_____

Додаток Б

Узагальнення результатів анкетування 1289 практикуючих юристів (суддів-154 прокурорів-461, слідчих (дізнавачів)-669, адвокатів-5)

Питання 2	**Ваш стаж роботи на посаді?**									
	судді		**Прокурори**		**слідчі (дізнавачі)**		**адвокати**		**ВСЬОГО**	
	кількість	**%**	**Кількість**	**%**	**кількість**	**%**	**кількість**	**%**	**кількість**	**%**
до одного року	2	1	9	1	99	14	0	0	110	8
від 1 до 3 років	13	8	61	13	162	25	1	20	237	18
від 3 до 5 років	20	13	38	8	88	13	1	20	147	11
від 5 до 10 років	18	12	105	23	122	18	0	0	245	19
більше 10 років	101	66	248	55	198	30	3	60	550	43
Питання 3	**Який термін, на Вашу думку, найбільш коректно вживати для позначення інформації з комп'ютерів, смартфонів, планшетів, інших технічних пристроїв?**									
електронна інформація	18	12	45	11	151	22	1	20	215	17
цифрова інформація	7	5	49	11	61	9	1	20	118	9
інформація з електроннних носіїв	40	26	141	32	249	36	1	20	431	33
інформація з цифрових носіїв	21	14	57	13	89	13	0	0	167	13
Комп'ютерна інформація	1	1	5	1	18	3	0	0	24	2
електронні докази	47	31	87	20	61	9	2	40	197	15
цифрові докази	11	7	22	5	26	4	0	0	59	5
електронний документ	9	6	25	6	34	5	0	0	68	5
інше	0	0	3	1	7	1	0	0	10	1
Питання 4	**Чи вважаєте Ви за необхідне виділити електронні (цифрові) докази як окреме джерело доказів у кримінальному процесі?**									
так	114	74	292	67	412	59	5	100	823	64
ні	28	18	111	26	170	25	0	0	309	24

інше	12	8	31	7	114	16	0	0	157	12
Питання 5	**Чи вважаєте Ви достатнім та повним нормативне регулювання процесуального порядку збирання електронних (цифрових) доказів?**									
так	21	14	70	16	249	36	2	40	342	27
ні	106	69	298	69	316	45	3	60	723	56
складно відповісти	27	18	66	15	131	19	0	0	224	17
інше	0	0	0	0	0	0	0	0	0	0
Питання 6	**Чи не вважаєте Ви за необхідне регламентувати в окремій главі КПК України процесуальний порядок вилучення, фіксації, критерії оцінки електронних доказів?**									
так	100	65	295	68	395	57	3	60	793	62
ні	43	28	114	26	203	29	2	40	362	28
складно відповісти	10	6	25	6	92	13	0	0	127	10
інше	1	1	0	0	6	1	0	0	7	1
Питання 7	**На які дефекти чинного кримінального процесуального законодавства стосовно унормування процесуального порядку збирання електронних (цифрових) доказів Ви можете вказати?**									
Результати за посиланням	*7-1*		*7-2*		*7-3*		*7-4*			
Питання 8	**Чи були труднощі з оцінкою відомостей (фактичних даних), отриманих з електронних носіїв ?**									
так	88	57	193	45	329	47	3	60	613	48
ні	62	40	238	55	349	50	2	40	651	51
складно відповісти	4	3	1	0	2	0	0	0	7	1
інше	0	0	2	0	16	2	0	0	18	1
Питання 9	**З якими видами електронних доказів Ви стикалися у своїй практиці ?**									
аудіозаписи	131	8	276	64	641	92	4	80	1052	82

		5								
відеозаписи	148	96	378	87	580	83	5	100	1111	86
цифрові фотографії та зображення	112	73	259	60	483	69	4	80	858	67
електронні повідомлення (смс-та ммс-повідомлення, електронна пошта)	100	65	250	58	403	58	4	80	757	59
вебсайти (вебсторінки)	79	51	210	48	378	54	2	40	669	52
дані геолокації	56	36	143	33	211	30	1	20	411	32
комп'ютерні дані	44	29	145	33	282	41	1	20	472	37
електронні документи	70	45	101	37	307	44	4	80	482	37
інше	0	0		0		0		0	0	0
Питання 10	**Чи існують відмінності у тактиці збирання «традиційних» доказів та електронних (цифрових) доказів?**									
так	121	79	343	79	498	72	5	100	967	75
ні	27	18	90	21	190	27	0	0	307	24
складно відповісти	5	3	1	0	2	0	0	0	8	1
інше	1	1	0	0	6	1	0	0	7	1
Питання 11	**Чи необхідно залучати спеціаліста під час збирання електронних (цифрових) доказів?**									
так	56	36	219	51	283	41	2	40	560	43
ні	6	4	19	4	69	10	0	0	94	7
в окремих випадках	83	54	182	42	301	42	3	60	569	44
складно відповісти	8	5	12	3	39	6	0	0	59	5
інше	1	1	0	0	6	1	0	0	7	1
Питання 12	**Чи необхідно залучати спеціаліста під час дослідження електронних (цифрових) доказів?**									
так	45	29	201	46	310	45	0	0	556	43
ні	7	5	21	5	55	8	0	0	83	6
в окремих випадках	97	63	203	47	283	42	5	100	588	46

складно відповісти	5	3	9	2	43	6	0	0	57	4
інше	0	0	0	0	5	1	0	0	5	0
Питання 13	**Що, на Вашу думку, потрібно для того, щоб використовувати як доказ фактичні дані отримані з електронного носія інформації?**									
подання оригіналу технічного носія інформації в електронному вигляді	64	42	123	28	273	39	1	20	461	36
подання копії інформації в електронному вигляді	38	25	154	35	290	42	2	40	484	38
подання копії інформації в електронному вигляді, виготовленої спеціалістом	64	42	213	49	218	31	2	40	497	39
інше	4	3	6	1	3	0	0	0	13	1
Питання 14	**Чи є логічним на Вашу думку вживання поняття «дублікат» для позначення електронних доказів, в тому числі і електронних документів ?**									
так	46	30	206	47	388	56	3	60	643	50
ні	73	47	151	35	157	23	1	20	382	30
складно відповісти	32	21	74	17	149	21	1	20	256	20
інше	3	2	3	1	2	0	0	0	8	1
Питання 15	**Чи має на Вашу думку значення для допустимості доказів джерело доказів (тобто чи буде доказом фактичні дані отримані з не передбаченого КПК джерела доказів) ?**									
так	123	80	334	48	478	69	5	100	940	73
ні	26	17	98	35	197	28	0	0	321	25
інше	5	3	1	17	22	3	0	0	28	2
Питання 16	**Чи має на Вашу думку значення для допустимості доказів порядок отримання доказів (тобто якщо фактичні дані отримані в не передбаченому КПК порядку)?**									
так	147	95	391	90	537	77	5	100	1080	84
ні	7	5	43	10	143	21	0	0	193	15
інше	0	0	0	0	16	2	0	0	16	1
Питання 17	**Чи відчували Ви труднощі під час збирання та дослідження електронних доказів?**									
так	111	72	322	74	460	66	5	100	898	70
ні	42	27	112	26	214	31	0	0	368	29

інше	1	1	0	0	22	3	0	0	23	2
Питання 18	**Якщо так, то які саме? (декілька варіантів відповідей)**									
Відсутність законодавчого закріплення поняття електронних доказів та критеріїв їх оцінки	69	45	185	43	334	48	4	80	592	46
Складність встановлення оригіналу, копії, дублікату інформації в електронній формі	89	58	182	42	254	36	4	80	529	41
Відсутність базових знань у сфері інформаційних технологій	41	27	144	33	187	27	2	40	374	29
Вербалізація(словесне вираження) у процесуальних документах та інших матеріалах кримінального провадження процесів, пов'язаних із збиранням та використанням інформації в електронному вигляді	27	18	73	17	112	16	2	40	214	17
Відсутність сформованої методики збирання	60	39	192	44	222	32	4	80	478	37
Відсутність технічних засобів для копіювання, вилучення, транспортування, зберігання таких доказів	42	27	154	35	242	35	2	40	440	34
Відсутність достатньої кількості спеціалістів для залучення до проведення слідчих (розшукових) дій	44	29	186	43	217	31	1	20	448	35
інше	0	0	0	0	0	0	0	0	0	0
Питання 19	**Чи виникали у Вас труднощі із збиранням доказів в порядку ст.245-1 КПК України ?**									
так	25	16	115	26	232	33	2	40	374	29
ні	129	84	291	67	427	62	3	60	849	66
інше	0	0	29	7	37	5	0	0	66	5
Питання 20	**Чи виникали у Вас труднощі з оцінкою доказів, отриманих в порядку ст.245-1 КПК України ?**									
так	41	27	106	24	220	32	2	40	369	29
ні	113	73	303	70	447	64	3	60	866	67

інше	0	0	25	6	29	4	0	0	54	4
Питання 21	**Як Ви вважаєте чи є коректним термін «показання», який використовується для позначення фактичних даних отриманих в порядку ст.245-1 КПК України ?**									
так	54	35	182	42	357	51	0	0	593	46
ні	100	65	243	56	323	47	5	100	671	52
інше	0	0	9	2	16	2	0	0	25	2
Питання 22	**Як Ви вважаєте, чи може слідчий проводити слідчу (розшукову)дію в порядку ст.245-1 КПК України у кримінальних провадженнях щодо злочинів?**									
так	132	86	391	90	578	83	3	60	1104	86
ні	19	12	33	8	97	14	2	40	151	12
інше	3	2	10	2	21	3	0	0	34	3
Питання 23	**Як Ви вважаєте, чи можна використовувати як докази фактичні дані отримані слідчим в порядку ст.245-1 КПК України у кримінальних провадженнях щодо злочинів?**									
так	141	92	401	93	614	88	3	60	1159	90
ні	12	8	23	5	72	11	2	40	109	8
інше	1	1	10	2	10	1	0	0	21	2
Питання 24	**Чи отримували Ви відмову (відмовляли) у задоволенні клопотання про надання тимчасового доступу до речей і документів у випадку необхідності отримання копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб у кримінальному провадженні щодо проступків?**									
так	13	8	53	12	153	22	3	60	222	17
ні	136	88	356	82	471	68	2	40	966	75
підставою відмови було необхідність отримання відповідної інформації в порядку ст.245-1 КПК України	5	3	11	3	36	5	0	0	52	4
інше	0	0	13	3	36	5	0	0	49	4

Питання 25	**Чи отримували Ви відмову (відмовляли) у задоволенні клопотання про надання тимчасового доступу до речей і документів у випадку необхідності отримання копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб у кримінальному провадженні щодо злочинів ?**									
так	11	7	55	13	144	21	2	40	212	16
ні	140	91	356	82	480	69	2	40	978	76
підставою відмови було необхідність отримання відповідної інформації в порядку ст.245-1 КПК України	3	2	6	1	33	5	1	20	43	3
інше	0	0	17	4	39	5	0	0	56	4
Питання 26	**Як Ви вважаєте, чи є необхідним викладення ст.245-1 КПК України в іншій редакції ? Якщо так, то які потрібно внести зміни ?**									
так	41	27	122	28	167	24	3	60	333	26
ні	101	66	285	66	502	72	1	20	889	69
інше	12	8	27	6	27	4	1	20	67	5
Питання 27	**Як Ви вважаєте, чи є доцільним виділення процесуальних джерел доказів у кримінальних проступках (ст.298-1 КПК України)?**									
так	69	45	246	57	363	52	3	60	681	53
ні	85	55	183	42	318	46	1	20	587	46
інше	0	0	5	1	15	2	1	20	21	2
Питання 28	**Які питання повинен дослідити слідчий суддя при прийнятті рішення за клопотанням прокурора про надання дозволу на використання процесуальних джерел доказів у кримінальних провадженнях щодо злочинів у порядку ст.298-1 КПК України?**									
задовольнити клопотання автоматично, якщо такі докази, передбачені ч.1 ст.298-1 КПК України	40	26	290	67	563	81	0	0	893	69
відмовити у задоволені клопотання, якщо порушені права,свободи та інтереси осіб у кримінальному провадженні	89	58	129	30	113	16	5	100	336	26

інше	25	16	15	3	20	3	0	0	60	5
Питання 29	**Чи були у Вашій практиці випадки, коли знімали показання технічних приладів і технічних засобів у провадженнях щодо вчинення кримінальних проступків, що мають функції фото-і кінозйомки, відеозапису до внесення відомостей про кримінальний проступок до Єдиного реєстру досудових розслідувань?**									
так	11	7	59	14	164	24	4	80	238	18
ні	143	93	375	86	515	74	1	20	1034	80
інше	0	0	0	0	17	2	0	0	17	1
Питання 30	**Чи вважаєте Ви за необхідне поширення поняття кореспонденція на листування в застосунках для обміну повідомленнями, електронній пошті ?**									
так	116	75	322	74	360	63	5	100	877	68
ні	36	23	111	26	309	35	0	0	392	30
інше	2	1	1	0	27	2	0	0	20	2
Питання 31	**Чи буде на Вашу думку втручання у приватне спілкування коли при затриманні особи слідчий, дізнавач отримує доступ до листування в застосунках для обміну повідомленнями, електронній пошті, зокрема, в мобільних телефонах без відповідного дозволу слідчого судді ?**									
так	131	85	335	77	330	52	5	100	831	64
ні	13	8	81	19	288	44	0	0	403	31
інше	10	6	18	4	24	4	0	0	55	4

Питання 7. На які дефекти чинного кримінального процесуального законодавства стосовно унормування процесуального порядку збирання електронних (цифрових) доказів Ви можете вказати?

7-1 (судді)

1. Домінування формального підходу в оцінці доказів - для цифрових доказів більш важливим їх можливість бути верифікованими, аніж дотримання формальних вимог при їх вилученні.

2. Відсутність виписаного в законі порядку огляду/обшуку мобільних телефонів та інших аналогічних пристроїв та судового контроль за цим. Внаслідок чого, вилучивши телефон, слідство може отримати фактично безконтрольний доступ до життя людини: електронної пошти, повідомлень, фото за багато років, програм управління розумним будинком, тощо.

3. Процесуальним законодавством не враховано динамічний розвиток цифрових технологій, не унормовано порядок отримання інформації з мобільних телефонів, зокрема щодо листування з месенджерів.

4. Можливі деякі дефекти в унормуванні процесу збирання електронних доказів, такі як нестача чітких норм щодо проведення кіберекспертизи, недостатнє регулювання правил вилучення та збереження електронних доказів, а також можливість невідповідності технічних засобів для збирання даних стандартам доказування.

5. Головною проблемою КПК України у цьому питанні є відсутність будь-якого регулювання такої групи доказів. Поняття електронних (цифрових) доказів чинному КПК невідоме.

6. Проблематика з первинними джерелами походження, наявності оригіналів, при не можливості їх встановлення.

7. Не визначено, який саме примірник електронного документом є його оригіналом, що таке копія, як зберігаються електронні докази.

8. Нечітко виписані процедури збирання різних видів електронних доказів.

9. Відсутність чітких критеріїв допустимості електронних доказів, порядку їх збирання враховуючи, наприклад те, що порядок виготовлення копій зображень з соціальних мереж, електронної пошти (скріншот) не регламентовано законом.

10. Надмірна деталізація щодо порядку збирання електронних доказів створить нові шпарини для уникнення відповідальності правопорушникам. Діючі норми вже достатньо врегульовують дані питання.

11. Відсутній вичерпний перелік видів електронних (цифрових) доказів. Не врегульовано порядок їх отримання для визначення допустимості чи недопустимості доказу.

12. Положення ст. 245-1 КПК України «Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису» також не надає відповіді, яким чином фіксувати інформацію, що знаходиться на носіях. В цьому аспекті необхідно прийняти відповідні зміни до ст. 84, 98 КПК України, а так само доповнити кодекс після статті 245-1 КПК України новою статтею, яка б регламентувала порядок фіксації інформації, що "вилучається в якості доказу з електронних інформаційних систем, комп’ютерних систем або їх частин, мобільних терміналів систем зв’язку.

13. Відсутність регламентованого порядку огляду електронного носія інформації при добровільній його видачі з метою збереження інформації.

14. Відсутність чіткого визначення поняття оригіналу таких доказів, через їх специфіку. Тобто у цифровому вигляді їхня оригінальність не залежить від носія, на якому вони знаходяться, важливим є лише саме оригінальність файлу із вихідними даними (метадані тощо). Натомість дуже частим є питання щодо "оригінальності" запису чи іншої інформації, яка записана для відтворення на іншій носій.

7-2 (прокурори)

1. В діючому КПК України чітко не регламентовано порядок виявлення, фіксації, вилучення та зберігання електронних (цифрових) доказів

2. Відсутність критеріїв допустимості електронних доказів, відсутність належної нормативної бази, відсутність норм КПК, яка регулює електронні докази .

3. Необхідно враховувати постійну зміну і оновлення електронної інформації Для вилучення (копіювання, тощо) такої інформації обов’язкова участь спеціаліста. При цьому, не завжди є можливість залучення такого спеціаліста, як і не завжди потрібні спеціальні знання для копіювання такої інформації, виготовлення прінт-скрін, тощо.

4. Не має чіткого порядку та визначеності щодо електронних (цифрових) доказів. Не можливо їх отримати через ст.93 КПК України. Не унормовано порядок копіювання при вилученні або огляді (чітко не визначені переліки носіїв чи ресурсів, на які копіюється

інформація, технічні вимоги, спосіб позначення); відсутність чіткого визначення, що така інформація (вилучена/скопійована у передбачений КПК) спосіб має однакову юридичну силу поряд с іншими доказами.

5. Не має деталізованого алгоритму процесуальних дій щодо збирання, дослідження та надання оцінки електронним доказам. Не має чіткого розуміння щодо процесуального закріплення отриманого електронного доказу (наприклад, є незрозумілим чи слід повністю відображати в протоколі всі дії слідчого і прокурора пов'язанні із здобуттям вказаного електронного доказу чи то вистачить зазначити короткий опис про долучення електронного носія з файлом).

6. Чітке визначення поняття електронного доказу, їх види та порядок отримання, чітке розмежування оригіналу та копій електронного документу, надання можливості долучати до протоколів слідчих дій копій з носіїв на які фіксувалась слідча дія чіткий порядок збирання таких доказів.

7-3 (слідчі, дізнавачі)

1. Віднесення електронних джерел до певних видів джерел доказів, наприклад, сама інформація в електронному вигляді, файл відеозапису, відноситься до такого джерела доказів як документ, а носій інформації, на якому така інформація (файли) містяться - мають ознаки речового доказу. Віднесення носія інформації до речового доказу є невірним, оскільки це лише форма фіксації, однак на практиці суд в більшості випадків вимагає визнання носіїв речовим доказом та винесення відповідної постанови.

2. Недостатньо врегульована правова процесуальна процедура збирання електронних доказів. Як приклад, правова колізія у отриманні певної інформації з комп'ютерної техніки та мобільних пристроїв, що містить спілкування особи (переписки). За загальним правилом, приватне спілкування особи являється інформацією, яка відноситься до охоронюваної законом таємниці. Доступ до такої інформації відповідно до чинного КПК України, має відбуватися виключно за рішенням суду. Положення чинного КПК України, передбачають лише дві правові процедури отримання таких відомостей - тимчасовий доступ до речей і документів в порядку ст.ст. 159-166 КПК України та НСРД. Зняття інформації з електронних інформаційних систем в порядку ст. 264 КПК України. Однак, постає питання доцільності проведення таких процесуальних дій, у випадку вже вилученої такої техніки, яка перебуває у розпорядженні слідчого та матеріалах кримінального провадження.

3. Допустимість електронних доказів, наданою стороною кримінального провадження, або свідками шляхом направлення на електронну адресу слідчому. Якщо такі докази будуть визнані допустимими, то можливо було б оперативно приймати процесуальній рішення у кримінальному провадженні, призначити експертизи, використовувати як докази при обрані запобіжних заходів, тощо без виклику свідка або особи у володінні якої знаходиться вказана інформація, та підпису зазначеної особи у протоколі слідчої дії. Не завжди, володілець відео реєстратора, на якому зафіксовано факт вчинення злочину, хоче прибути до слідчого для допиту та надання інформації з його приладу. Хоча як правило він не є прямим свідком кримінального правопорушення.

4. Не врегульоване питання щодо доступу до інформації, яка була вилучена на носії, а саме не зазначено процесуально порядок доступу до неї, її огляду та в подальшому зберігання у вигляді дубліката, якщо під час проведення експертизи у подальшому може відбутися її пошкодження, було б добре якщо були б захищені сервери до яких можна було фізично або через Інтернет розміщувати на зберігання вказану інформацію.

5. Неможливо використовувати належним чином отриману інформацію з Інтернет ресурсів. Необхідність проведення НСРД при подоланні системи логічного захисту; необхідність участі спеціаліста при огляді; необхідність проведення комп'ютерно-технічної експертизи при копіюванні файлів.

6. Судами не приймається до уваги як належний доказ копія цифрової інформації, виготовлена з оригіналу, що зберігається на технічному носії (відеокамера, телефон, жорсткий диск комп'ютера)

7. У ст. 84 КПК України докази з електронних носіїв не передбачене як джерело доказу.

7-4 (адвокати)

1. Відсутність чіткої процедури, ускладненість роботи з цифровим слідом та цифровою інформацію. Підтвердження достовірності та автентичності доказу, пошук першоджерела, складність самостійного збору таких доказів стороною захисту.

2. Не достатній рівень перевірки дійсності доказу.

26-1 (судді)

1. Термін «показання» не є доречним для відображення суті процесуальні дії , а так само змісту та сутності зафіксованої інформації.

2. Можливо більш детально прописати порядок збирання таких доказів і їх фіксацію за участю спеціаліста.

29-1 (судді)

1. Це буде надмірним контролем з боку слідчого судді. Оцінка доказів має бути надана судом при розгляді по суті.

2. Перевірити чи на момент розгляду клопотання слідчий може отримати за допомогою інших засобів доказування такі докази у кримінальному провадженні щодо злочину, перевірити чи не було зловживання правом з боку органу досудового розслідування, який умисно не реєстрував кримінальне провадження щодо злочину, а зареєстрував суміжний склад кримінального правопорушення, що є кримінальним проступком, чи дотримано процедуру збирання доказів встановлену КПК, тощо.

31-1 (судді)

1. Це втручання в спілкування в розумінні Конвенції, але не в розумінні КПК як негласна слідча дія, бо ця дія не негласна. Втім, вона має бути обов»язково врегульована в законі, із виписуванням належної процедури судового контролю за цим втручанням, адже в нинішній час телефони і застосунки - неодмінна частина людського життя

Додаток В

АКТИ про впровадження результатів дисертаційного дослідження

ТРЕНІНГОВИЙ ЦЕНТР ПРОКУРОРІВ УКРАЇНИ
вул. Юрія Іллєнка, 81-б,
м. Київ, 04050, Код ЄДРПОУ: 43556710
тел./факс: +38 (044)206-00-53, 206-18-44
ptcu@gp.gov.ua, http://ptcu.gp.gov.ua

PROSECUTOR'S TRAINING CENTER OF UKRAINE
81-b, Yuriia Illienka Str.,
Kyiv, 04050, EDPNOU code: 43556710
tel./fax: +38 (044) 206-00-53, 206-18-44
ptcu@gp.gov.ua, http://ptcu.gp.gov.ua

26.06.2024 № 2/1-03/828 На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Смаль Інни Анатоліївни

«Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі»

на здобуття наукового ступеня доктора філософії

за спеціальністю 081 «Право»

Результати дисертаційного дослідження «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі» Смаль Інни Анатоліївни опубліковані у перелічених нижче фахових статтях:

1. Смаль І. А. Правові аспекти застосування електронних доказів у кримінальному судочинстві. Право і суспільство №4/2021 с.226-233.

2. Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу електронний документ. Прикарпатський юридичний вісник Випуск 2(43), 2022. с.122-127

3. Смаль І.А. Практичні аспекти зняття показань технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі. Юридичний науковий електронний журнал – електронне наукове фахове видання юридичного факультету Запорізького національного університету Випуск 6/2023. с.552-558

Результати дисертаційного дослідження вивчено та використано в діяльності Тренінгового центру прокурорів України, зокрема під час первинної підготовки кандидатів на посади прокурорів та підвищення кваліфікації прокурорів з метою розвитку професійної компетенції за напрямом виконання завдань використання електронних доказів у кримінальному провадженні.

Директор **Олеся ОТРАДНОВА**

ЗАТВЕРДЖУЮ
Ректор Національного юридичного університету
Імені Ярослава Мудрого
Анатолій ГЕТЬМАН
«16» 08 2024 р.

АКТ
впровадження наукових результатів дисертації
Смаль Інни Анатоліївни на тему: «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі» в навчальну діяльність кафедри кримінального процесу Національного юридичного університету імені Ярослава Мудрого

Комісія у складі: ***голови комісії*** — докторки юридичних наук, професорки, завідувачки кафедри кримінального процесу Національного юридичного університету імені Ярослава Мудрого Капліної Оксани Володимирівни; ***членів комісії:*** професорки кафедри кримінального процесу Національного юридичного університету імені Ярослава Мудрого Ануш Робертівни Туманянц; доцентки кафедри кримінального процесу Національного юридичного університету імені Ярослава Мудрого Ольги Ігорівни Тищенко склала цей акт про те, що опубліковані у низці наукових статей та тезах наукових доповідей на міжнародних та всеукраїнських науково-практичних конференціях, медико-правових форумах, круглих столах, полілогах, результати дисертаційного дослідження Смаль Інни Анатоліївни «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі» на здобуття наукового ступеня доктор філософії за спеціальністю 081 «Право» використовуються у навчальному процесі при викладанні дисциплін кафедри кримінального процесу — «Кримінальний процес», «Досудове розслідування кримінальних правопорушень», «Проблеми досудового розслідування кримінальних правопорушень», «Нагляд прокурора за слідчими (розшуковими) та негласними слідчими (розшуковими) діями» та при підготовці підручників, навчальних посібників, методичних рекомендацій.

Зокрема, йдеться про такі публікації:

1. Смаль І. А. Правові аспекти застосування електронних доказів у

кримінальному судочинстві. Право і суспільство №4/2021 с.226-233.

2. Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу електронний документ. Прикарпатський юридичний вісник Випуск 2(43), 2022. с.122-127.

3. Смаль І.А. Практичні аспекти зняття показань технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі. Юридичний науковий електронний журнал – електронне наукове фахове видання юридичного факультету Запорізького національного університету Випуск 6/2023 с.552-558.

4. Смаль І. А. «Історичні передумови появи електронних доказів як засобів доказування в кримінальному процесі» // Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2020: матеріали міжнар. наук.- практ. конф. (м. Чернігів, 23-24 квіт. 2020 р.): у двох томах. Т. 2 / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2020. С. 266-268.

5. Смаль І. А. «Перспективи використання електронних доказів як засобів доказування у кримінальному процесі» / Смаль І. А. //»Теорія та практика сучасної юриспруденції»-2020 (м.Харків,20.12.2020:/ 2 т. матеріали XXVI Всеукраїнської науково-практичної конференції (м.Харків,20.12.2020:/гол.ред. О.О. Нанарова Національний юридичний університет ім. Ярослава Мудрого. Харків. т.2. с.324-326.;

6. Остапчук Л. Г., Смаль І. А. Кіберзлочинність та електронні докази в кримінальному судочинстві. / Остапчук Л. Г, Смаль І. А. // Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2021: матеріали міжнар. наук.- практ. конф. (м. Чернігів, 22-23 квіт. 2021 р.): у двох томах. Т. 2 / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2021.

7. Смаль І.А. Проблематика огляду носіїв цифрових даних через призму забезпечення прав та законних інтересів особи / Смаль І.А. //« Інтеграція теорії у практику : проблеми, пошуки, перспективи – 2021: матеріали міжнародної науково- практичної конференції (м. Чернігів, 05 листопада 2021 р.) / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2021.Чернігів: Академія ДПтС с. 186-189.

8. Смаль І. А. Окремі аспекти збирання та процесуального закріплення інформації з електронних носіїв. Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квітня 2023 р.) : у двох томах. Том 1 / голов. ред. В. Ф. Пузирний ; Академія Державної пенітенціарної служби. Чернігів : Академія ДПтС, 2023. 448 с. с.327-330.

9. Смаль І. А. Межі втручання у приватне спілкування під час збирання електронних доказів у кримінальному процесі. Трансформації особистості, суспільства та ринку праці: виклики майбутнього та вплив на освіту. Збірник тез доповідей Міжнародної науково-практичної конференції 20-22 вересня 2023 року, м. Харків. Харків : ХНУ імені В. Н. Каразіна, 2023. – 560 с. (с. 440-441).

10. Смаль І. Втручання у право на приватність під час здійснення досудового розслідування у вимірі стандартів статті 8 Конвенції про захист прав людини і основоположних свобод. Матеріали VI Харківського кримінально процесуального полілогу «Кримінальний процес: сучасний вимір та проспективні тенденції» (м. Харків, 17 квітня 2024 р.) / ред-кол.: О. В. Капліна, А.Р. Туманянц. – Харків : Право, 2024.

Голова комісії:

Завідувачка кафедри кримінального процесу,
докторка юридичних наук, професорка,
член-кореспондент Національної академії
правових наук України,
заслужений діяч науки і техніки України О.В. Капліна

Члени комісії:

Кандидатка юридичних наук,
професорка кафедри кримінального процесу
Національного юридичного університету
імені Ярослава Мудрого А.Р. Туманянц

Кандидатка юридичних наук,
доцентка кафедри кримінального процесу
Національного юридичного університету
імені Ярослава Мудрого О. І. Тищенко

ВИЩА КВАЛІФІКАЦІЙНА КОМІСІЯ СУДДІВ УКРАЇНИ
НАЦІОНАЛЬНА ШКОЛА СУДДІВ УКРАЇНИ
Адреса: вул. Жилянська, 120 А, м. Київ, 01032
Тел/факс: +38 044 597 09 30; e-mail: info@nsj.gov.ua
Код ЄДРПОУ 37451388

ЗАТВЕРДЖУЮ
Ректор Національної школи суддів України
_____ **Микола ОНІЩУК**
"17" 07 2024 р.

АКТ

впровадження у навчальний і науковий процес Національної школи суддів України результатів дисертаційного дослідження Смаль Інни Анатоліївни на тему: «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі», за спеціальністю 081 - Право

Комісія у складі:

кандидата юридичних наук, заступника начальника відділу підготовки викладачів (тренерів) Національної школи суддів України – Закревської Т. О.;

кандидата юридичних наук, начальника відділу науково-методичного забезпечення діяльності судів та органів суддівського врядування Національної школи суддів України – Шамрай О. В.;

кандидата юридичних наук, головного наукового співробітника відділу "Тестологічний центр" Національної школи суддів України – Ігнатченко Н. В.

склала цей акт про те, що положення, висновки, пропозиції та рекомендації, сформульовані у дисертаційному дослідженні аспірантки кафедри кримінального, кримінально-виконавчого права та кримінології Пенітенціарної академії України на тему: «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі», за спеціальністю 081 - Право, є вагомим внеском у розвиток юридичної науки і впроваджені в

науково-дослідну та навчально-методичну діяльність Національної школи суддів України.

Сформульовані автором положення і висновки є науково обґрунтованими та впроваджуються Національною школою суддів України при викладанні відповідних навчальних курсів стандартизованих програм підготовки та періодичного навчання суддів з метою підвищення їх кваліфікації, а також у науково-дослідній сфері – як підґрунтя для подальших наукових розробок.

Зокрема, результати дисертації Смаль І. А. в частині практичних аспектів використання інформації в електронному вигляді в якості доказів у кримінальному процесі; забезпечення права на повагу до приватного життя та кореспонденції під час провадження слідчих (розшукових), негласних слідчих (розшукових) дій були використані під час організаційного та змістово-методичного забезпечення спеціальної підготовки кандидатів на посаду судді, підготовки суддів, їх періодичного навчання з метою підвищення рівня їх кваліфікації а також науково-методичного забезпечення підготовки викладачів (тренерів), зокрема розробки відповідних навчальних курсів, в тому числі тренінгу «Практичні аспекти використання інформації в електронному вигляді в якості доказів».

З науковим доробком, що міститься в дисертаційному дослідженні, ознайомлені викладачі Національної школи суддів України, а також співробітники відділів науково-методичного забезпечення діяльності судів та органів суддівського врядування, підготовки викладачів (тренерів), наукових досліджень проблем судочинства та науково-методичного забезпечення суддівської освіти та підготовки суддів.

У навчальному процесі Національної школи суддів України застосовуються результати досліджень Смаль І. А., які відображають основні положення дисертаційного дослідження та відображені у наступних роботах:

1. Смаль І. А. Правові аспекти застосування електронних доказів у кримінальному судочинстві. Право і суспільство №4/2021 с.226-233.
2. Остапчук Л. Г., Смаль І. А. До питання правової природи

електронного документу та його місця у системі доказів кримінального процесу. Прикарпатський юридичний вісник Випуск 2(43), 2022. с.122-127.

3. Смаль І. А. Практичні аспекти зняття показань технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі. Юридичний науковий електронний журнал – електронне наукове фахове видання юридичного факультету Запорізького національного університету Випуск 6/2023. с.552-558.

4. Смаль І. А. «Історичні передумови появи електронних доказів як засобів доказування в кримінальному процесі» // Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2020: матеріали міжнар. наук.- практ. конф. (м. Чернігів, 23-24 квіт. 2020 р.): у двох томах. Т. 2 / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2020. С. 266-268.

5. Смаль І. А. Перспективи використання електронних доказів як засобів доказування у кримінальному процесі / Смаль І. А. //»Теорія та практика сучасної юриспруденції»-2020 (м.Харків,20.12.2020:/ 2 т. матеріали XXVI Всеукраїнської науково-практичної конференції (м.Харків,20.12.2020:/гол.ред. О.О. Нанарова Національний юридичний університет ім..Я.Мудрого. Харків. т. 2 с.324-326.

6. Остапчук Л. Г., Смаль І. А. Кіберзлочинність та електронні докази в кримінальному судочинстві. / Остапчук Л. Г, Смаль І. А. // Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2021: матеріали міжнар. наук.- практ. конф. (м. Чернігів, 22-23 квіт. 2021 р.): у двох томах. Т. 2 / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2021.

7. Смаль І. А. Проблематика огляду носіїв цифрових даних через призму забезпечення прав та законних інтересів особи / Смаль І. А. //« Інтеграція теорії у практику: проблеми, пошуки, перспективи – 2021: матеріали міжнародної науково- практичної конференції (м. Чернігів, 05 листопада 2021 р.) / гол. ред.: Тогочинський О. М. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, Чернігів 2021: Академія ДПтС с.186-189.

8. Смаль І. А. Окремі аспекти збирання та процесуального закріплення інформації з електронних носіїв. Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану: матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квітня 2023 р.): у двох томах. Том 1 / голов. ред. Пузирний В. Ф.; Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2023. 448 с. с.327-330.

9. Смаль І. А. Межі втручання у приватне спілкування під час збирання електронних доказів у кримінальному процесі. Трансформації особистості, суспільства та ринку праці: виклики майбутнього та вплив на освіту. Збірник тез доповідей Міжнародної науково-практичної конференції 20-22 вересня 2023 року, м. Харків. Харків : ХНУ імені В. Н. Каразіна, 2023. – 560 с.с.440-441.

10. Смаль І. А. Втручання у право на приватність під час здійснення досудового розслідування у вимірі стандартів статті 8 Конвенції про захист прав людини і основоположних свобод. Матеріали VI Харківського кримінаально процесуального полілогу « Кримінальний процес: сучасний вимір та перспективні тенденції (м. Харків, 17 квітня 2024 р.) ред-кол.: Капліна О. В., Тумянец А.Р.— Харків: Право, 2024.

Заступник начальника відділу
підготовки викладачів (тренерів)
Національної школи
суддів України,
кандидат юридичних наук **Тамара ЗАКРЕВСЬКА**

Начальник відділу
науково-методичного
забезпечення діяльності судів та
органів суддівського врядування,
кандидат юридичних наук **Оксана ШАМРАЙ**

Головний науковий співробітник
відділу "Тестологічний центр"
Національної школи суддів України,
кандидат юридичних наук **Ніна ІГНАТЧЕНКО**

ВЕРХОВНИЙ СУД
КАСАЦІЙНИЙ КРИМІНАЛЬНИЙ СУД
вул. П. Орлика, 4-А, м. Київ, 01043, тел. (044) 253 03 14, тел./факс (044) 253 86 20
e-mail: kks@supreme.court.gov.ua
Код ЄДРПОУ 41721784

ЗАТВЕРДЖУЮ

Заступник керівника Апарату Верховного Суду –
керівник секретаріату
Касаційного кримінального суду,
кандидат юридичних наук

Юрій ХІМ'ЯК

«25» вересня 2024 року

АКТ
впровадження наукових результатів дисертації
Смаль Інни Анатоліївни на тему: «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі»

Комісія у складі: начальника управління аналітичної та правової роботи Касаційного кримінального суду департаменту аналітичної та правової роботи, кандидата юридичних наук Бринзанської Ольги Василівни; начальника відділу систематизації судової практики касаційного суду управління аналітичної та правової роботи Касаційного кримінального суду департаменту аналітичної та правової роботи, кандидата юридичних наук Ліхолєтової Юлії Андріївни; керівника служби розгляду звернень та надання інформації секретаріату Касаційного кримінального суду, кандидата юридичних наук, заслуженого юриста України Слуцької Тетяни Іванівни склала цей акт про те, що опубліковані у низці наукових статей та тезах наукових доповідей на міжнародних та всеукраїнських науково-практичних конференціях, медико-правових форумах, круглих столах, полілогах (зокрема Смаль І. А. Правові аспекти застосування електронних доказів у кримінальному судочинстві. Право і суспільство №4/2021. - С. 226-233; Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу електронний документ. Прикарпатський юридичний вісник

Випуск 2(43), 2022. - С.122-127; Смаль І.А. Практичні аспекти зняття показань технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі. Юридичний науковий електронний журнал – електронне наукове фахове видання юридичного факультету Запорізького національного університету Випуск 6/2023. - С.552-558; Смаль І. А. «Історичні передумови появи електронних доказів як засобів доказування в кримінальному процесі» // Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2020: матеріали міжнар. наук.- практ. конф. (м. Чернігів, 23-24 квіт. 2020 р.): у двох томах. Т. 2 / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2020. С. 266-268; Смаль І. А. «Перспективи використання електронних доказів як засобів доказування у кримінальному процесі» / Смаль І. А. //»Теорія та практика сучасної юриспруденції» - 2020 (м. Харків, 20.12.2020:/ 2 т. матеріали XXVI Всеукраїнської науково-практичної конференції (м. Харків, 20.12.2020:/гол.ред. О.О. Нанарова Національний юридичний університет ім. Я. Мудрого. Харків. Т.2. - С. 324-326; Остапчук Л. Г., Смаль І. А. Кіберзлочинність та електронні докази в кримінальному судочинстві. / Остапчук Л. Г, Смаль І. А. // Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2021: матеріали міжнар. наук.- практ. конф. (м. Чернігів, 22-23 квіт. 2021 р.): у двох томах. Т. 2 / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2021; Смаль І.А. Проблематика огляду носіїв цифрових даних через призму забезпечення прав та законних інтересів особи / Смаль І.А. //« Інтеграція теорії у практику : проблеми, пошуки, перспективи – 2021: матеріали міжнародної науково- практичної конференції (м. Чернігів, 05 листопада 2021 р.) / гол. ред.: О. М. Тогочинський. Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2021.Чернігів: Академія ДПтС - С.186-189; Смаль І. А. Окремі аспекти збирання та процесуального закріплення інформації з електронних носіїв. Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квітня 2023 р.): у двох томах. Том 1 / голов. ред. В. Ф. Пузирний; Академія Державної пенітенціарної служби. Чернігів: Академія ДПтС, 2023. 448 с. - С.327-330; Смаль І. А. Межі втручання у приватне спілкування під час збирання електронних доказів у кримінальному процесі. Трансформації особистості, суспільства та ринку праці: виклики майбутнього та вплив на освіту. Збірник тез доповідей Міжнародної науково-практичної конференції 20-22 вересня 2023 року, м. Харків. Харків: ХНУ імені В. Н. Каразіна, 2023. – 560 с. - С. 440-441) результати дисертаційного дослідження Смаль Інни Анатоліївни «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі» на здобуття наукового ступеня доктор філософії за спеціальністю 12.00.09 - кримінальний процес та

криміналістика можуть бути використані під час аналітичного забезпечення діяльності Касаційного кримінального суду у складі Верховного Суду.

начальник управління аналітичної та правової роботи Касаційного кримінального суду департаменту аналітичної та правової роботи, кандидат юридичних наук — Ольга БРИНЗАНСЬКА

начальник відділу систематизації судової практики касаційного суду управління аналітичної та правової роботи Касаційного кримінального суду департаменту аналітичної та правової роботи, кандидат юридичних наук — Юлія ЛІХОЛЄТОВА

керівник служби розгляду звернень та надання інформації секретаріату Касаційного кримінального суду, кандидат юридичних наук, заслужений юрист України — Тетяна СЛУЦЬКА

Паперова копія
електронного документа

РАДА

КОМІТЕТ ВЕРХОВНОЇ РАДИ УКРАЇНИ
з питань правоохоронної діяльності

вул. М. Грушевського, 5, м. Київ, 01008, www.rada.gov.ua

Смаль І.А.
вул. Чернігівська, буд. 54,
смт Сосниця,
Корюківський район,
Чернігівська обл., 16100

Шановна Інно Анатоліївно!

У Комітеті Верховної Ради України з питань правоохоронної діяльності розглянуто зміни до Кримінального процесуального кодексу України, підготовлені Вами у межах здійснення дисертаційного дослідження на тему: «Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі».

За результатами розгляду інформуємо, що законодавчі пропозиції, зроблені в межах дисертаційного дослідження, надані народним депутатам України – членам Комітету для ознайомлення.

З повагою

Голова Комітету **С. Іонушас**

Додаток Г

Проєкт Закону про внесення змін до Кримінального процесуального кодексу України, пов'язаних з запровадженням процесуального джерела –електронні докази та забезпечення права на приватність під час проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, пов'язаних з вторгненням в «електронний простір» людини.

З А К О Н У К Р А Ї Н И

«Про внесення змін до Кримінального процесуального кодексу України,

пов'язаних з запровадженням процесуального джерела –електронні докази та забезпечення права на приватність під час проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, пов'язаних з вторгненням в «електронний простір» людини»

Верховна Рада України п о с т а н о в л я є:

І. Внести до Кримінального процесуального кодексу України (Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88) такі зміни:

1. **Частину 1 статті 3 доповнити пунктами 6-1, 9-1 та 26-1 наступного змісту:**

«6-1 електронні дані – це інформація в електронному вигляді, яка придатна для сприйняття людиною після обробки автоматичними програмними засобами;

9-1контрольна сума (CRC-сума, хеш-сума) – це деяке значення, що розраховане за набором даних шляхом застосування певного алгоритму і використовується для перевірки цілісності даних під час їх передачі або зберігання;

26-1 хешування - спосіб підтвердження цілісності та незмінності інформації в електронному вигляді під час її зберігання, перезапису, перенесення та передавання каналами зв'язку»

2. В частині 2 статті 84 після слів «речові докази» доповнити словами «електронні докази, письмові докази»;

3. В частині 2 статті 92 після слова «допустимості» доповнити словами «та достовірності».

4. В частині 2 статті 93 після слова «…організацій,» слова «…службових та фізичних…» виключити; після слова «…осіб…» слова «…речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок,…» виключити; після слів «…документів…» доповнити словами «…інформації, отримання від фізичних осіб речей, документів,…»;

в частині 3 після слів «…фізичних осіб…» виключити слова «…речей, копій…»; після слів «…висновків експертів…» виключити слова «…висновків

ревізій, актів перевірок;…»; після слова «…допустимих…» доповнити словами «… та достовірних…»;

5. Статтю 99 викласти в наступній редакції:

«Стаття 99. Письмові докази»

Частину 1 викласти в наступній редакції:

«Письмовими доказами є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить текстову, графічну або змішану інформацію, зафіксовану за допомогою письмових знаків, зображення тощо відомості, які можуть бути використані як доказ обставин, що підлягають доказуванню у кримінальному провадженні .»

В частині 2 слово «…документів…» змінити на «…письмових доказів…»

Пункт 1 частини 2 виключити;

В пункті 3 частини 2 слова «…а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії» виключити.

Пункт 4 частини 2 виключити;

В абзаці 2 частини 2 слово «…документами…» змінити на «…письмовими доказами…»;

в частині 3 після слово «документа» змінити на «…письмового доказу або копію письмового доказу».;

Друге речення частини 3 виключити;

частину 4 виключити;

в частині 5 слова «документа» змінити словами «письмових доказів»;

в частині 6 після слово «документи» змінити на « такі письмові докази»;

в частині 7 слово «документів» змінити словами «письмових доказів»;

6. Доповнити параграфом 6:

«§ 6 Електронні докази.

Стаття 101-1. Електронні докази

1.Електронний доказ – це інформація в електронному вигляді, що містить відомості про обставини, що мають значення для кримінального проводження та підлягають доказуванню, створена, збережена, або передана за допомогою електронних пристроїв, систем, або мереж та яка існує в формі, що забезпечує її автентичність, цілісність та придатність для дослідження.

2.Електронний документом є документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, у тому числі електронний підпис автора або підпис, прирівняний до власноручного підпису відповідно до Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

3.Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал електронного доказу або копію інформації в електронному вигляді (електронні

дані), що міститься комп'ютерних системах, їх невід'ємних частинах з обов'язковим підтвердженням автентичності такої інформації шляхом хешування чи іншим способом, що забезпечить можливість перевірки автентичності та цілісності інформації.

4. Для підтвердження змісту електронних доказів можуть бути визнані допустимими й інші відомості, якщо:

1) оригінал електронного доказу втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає;

2) оригінал електронного доказу не може бути отриманий за допомогою доступних правових процедур;

3) оригінал електронного доказу знаходиться у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони.

5. Сторона зобов'язана надати іншій стороні можливість оглянути або скопіювати оригінали електронних доказів, зміст яких доводився у передбаченому цією статтею порядку. У випадку неможливості надання оригіналу електронного доказу підтвердити його автентичність у визначеному цим Кодексом порядку.

7. В пункті 3 частини 3 статті 104 після слова «ідентифікації;» доповнити словами «а також копії інформації в електронному вигляді (електронні дані) та спосіб її ідентифікації та автентифікації.»

8. В пункті 4 частини 2 статті 105 після слова «носії» доповнити словами «інформації в електронному вигляді»

доповнити пунктом 5 частину 2 статті 105:

«5) довідка слідчого, дізнавача, прокурора, спеціаліста про застосований алгоритм хешування та контрольна сума (CRC-сума, хеш-сума) чи інший спосіб, що забезпечить можливість перевірки автентичності та цілісності інформації»

9. В статті 168:

абзац 2 частини 2 викласти в такій редакції:

«У разі отримання письмової інформованої згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку на пошук, виявлення та фіксацію інформації в електронному вигляді, що міститься в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку , дізнавач, слідчий чи прокурор може виготовити за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах з обов'язковим підтвердженням автентичності такої інформації шляхом хешування чи іншим способом, що забезпечить можливість перевірки автентичності та цілісності інформації. Копіювання такої інформації здійснюється із залученням спеціаліста »

в абзаці 3 частини 2:

після слова «вимогу» доповнити словами «власника або»;

10. В статті 234:

в пункті 8 частини 3 після слова «документів» доповнити словом «інформації»;

в пункті 5 частини 5 слова «заходом, пропорційним втручанню в особисте і сімейне життя особи» виключити;

в пункт 5 частини 5 доповнити словами «пропорційним заходом втручання у право на повагу до приватного і сімейного життя, житла особи»;

11. В статті 236:

абзац 2 і 3 частини 6 викласти в такій редакції:

«Якщо під час обшуку слідчий, дізнавач прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, а власник чи володілець комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку заперечує проти проведення такого огляду, прокурор слідчий, дізнавач має право здійснити пошук, виявлення та фіксацію інформації електронному вигляді (електронних даних), що на них міститься, тільки після отримання ухвали слідчого судді місцевого загального суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування, на проведення їх обшуку .

Прокурор, слідчий, дізнавач має право здійснити пошук, виявлення та фіксацію інформації в електронному вигляді, що міститься в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, на місці проведення обшуку тільки у разі отримання письмової інформованої згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку»

12. Доповнити статтею 236-1 наступного змісту:

«Стаття 236-1 Обшук комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку

1. Обшук комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку проводиться з метою виявлення та фіксації інформації в електронному вигляді про обставини вчинення кримінального правопорушення, а також встановлення місцезнаходження розшукуваних осіб.

2. Обшук проводиться на підставі ухвали слідчого судді місцевого загального суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування, а у кримінальних провадженнях щодо злочинів, віднесених до підсудності Вищого антикорупційного суду, - на підставі ухвали слідчого судді Вищого антикорупційного суду.

3. У разі необхідності провести обшук слідчий, дізнавач за погодженням з прокурором або прокурор звертається до слідчого судді з відповідним клопотанням, яке повинно містити відомості про:

1) найменування кримінального провадження та його реєстраційний номер;

2) короткий виклад обставин кримінального правопорушення, у зв'язку з розслідуванням якого подається клопотання;

3) правову кваліфікацію кримінального правопорушення з зазначенням статті (частини статті) закону України про кримінальну відповідальність;

4) підстави для обшуку;

5) ідентифікуючі дані комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку. що містять інформацію в електронному вигляді;

6) особу, якій належить на праві власності чи володінні комп'ютерні системи або їх частини, мобільні термінали систем зв'язку;

7) інформацію, яку планується відшукати, за який період, а також її зв'язок із вчиненим кримінальним правопорушенням;

8) обґрунтування того, що доступ до інформації в електронному вигляді , яка може міститися в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, неможливо отримати органом досудового розслідування у добровільному порядку шляхом надання інформативної згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку.

До клопотання також мають бути додані оригінали або копії документів та інших матеріалів, якими прокурор, слідчий, дізнавач обґрунтовує доводи клопотання, а також витяг з Єдиного реєстру досудових розслідувань щодо кримінального провадження, в рамках якого подається клопотання.

4. Клопотання про обшук розглядається у суді в день його надходження за участю слідчого (дізнавача)або прокурора.

5. Слідчий суддя відмовляє у задоволенні клопотання про обшук, якщо прокурор, слідчий, дізнавач не доведе наявність достатніх підстав вважати, що:

1) було вчинено кримінальне правопорушення;

2) відшукувана інформація в електронному вигляді ,електронні документи мають значення для досудового розслідування;

3) відомості, які містяться у відшукуваній інформації, електронних документах, можуть бути доказами під час судового розгляду;

4) відшукувана інформація в електронному вигляді, електронні документи знаходяться у зазначених клопотанні комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку;

5) за встановлених обставин обшук є найбільш доцільним та ефективним способом відшукання інформації в електронному вигляді,електронних документів,які мають значення для досудового розслідування, а також

встановлення місцезнаходження розшукуваних осіб, а також є пропорційним заходом втручанню в право на повагу до приватного і сімейного життя, до кореспонденції .

6. У разі відмови у задоволенні клопотання про дозвіл на обшук комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку дізнавач, слідчий, прокурор не має права повторно звертатися до слідчого судді з клопотанням про дозвіл на обшук тих самих комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, якщо у клопотанні не зазначені нові обставини, які не розглядалися слідчим суддею.

13. В статті 237:

в частині 1:

після слова «правопорушення» доповнити словом «дізнавач»;

після слів «документів та» доповнити словами «електронних даних»;

частину 2 викласти в наступній редакції:

«2. Огляд електронних даних, що містяться в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку проводиться дізнавачем, слідчим, прокурором у разі отримання письмової інформованої згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку чи інших носіїв інформації за винятком випадків, коли відповідна інформація знаходиться у відкритому доступі..

Огляд електронних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду відомостей щодо обставин вчинення кримінального правопорушення, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо)»

в частині 3 слова «може бути запрошений» замінити на «запрошуються»; «може запросити» замінити на «запрошує».

14. В ст.245-1:

Назву статті викласти в такій редакції:

«Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі»

Статтю 245-1 викласти в такій редакції:

«1. Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі полягає в одержанні слідчим, дізнавачем, прокурором від особи, яка є власником або володільцем відповідних приладів або засобів, необхідних для з'ясування обставин, що мають значення для кримінального провадження, копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях в автоматичному режимі.

2. Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється на підставі постанови дізнавача, слідчого, прокурора за участю спеціаліста.

3. Для отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі особі, яка є власником або володільцем відповідних приладів або засобів, пред'являється постанова дізнавача, слідчого, прокурора.

4. Постанова дізнавача, слідчого, прокурора про отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі повинна містити:

1) найменування кримінального провадження та його реєстраційний номер;

2) відомості про власника або володільця відповідних технічних приладів або засобів;

3) період часу, за який має бути отримано електронні дані технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі.

5. Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється дізнавачем, слідчим, прокурором шляхом самостійного копіювання або за участю спеціаліста відповідних записів на носії, які надаються дізнавачем, слідчого, прокурором з обов'язковим підтвердженням автентичності такої інформації шляхом хешування чи іншим способом, що забезпечить можливість перевірки автентичності та цілісності інформації.

6. Про проведення даної слідчої (розшукової) дії складається протокол згідно з вимогами цього Кодексу.

15. В статтю 298-1:

В абзаці 1 частини 1 слово «показання» змінити на «електронні дані»;

16. В статті 300:

в частині 1:

після слів «висновку експерта» слова «знімати показання технічних приладів і технічних засобів у провадженнях щодо вчинення кримінальних проступків» замінити словами «отримувати електронні дані технічних приладів і технічних засобів»;

після слова «відеозапису» доповнити словами «в автоматичному режимі»;

II. Прикінцеві та перехідні положення

Цей Закон набирає чинності з дня, наступного за днем його опублікування.

Додаток Д

ПОРІВНЯЛЬНА ТАБЛИЦЯ

Кримінальний процесуальний кодекс України (Відомості Верховної Ради України (ВВР), 2013, №9-10, №11-12,№13-, ст.88)		
№	**Чинна редакція закону**	**Запропонована редакція закону**
1	**Стаття 3. Визначення основних термінів Кодексу** 1. Терміни, що їх вжито в цьому Кодексі, якщо немає окремих вказівок, мають таке значення: **…….** **Пункт відсутній** **……..** **Пункт відсутній**	**Стаття 3. Визначення основних термінів Кодексу** 1. Терміни, що їх вжито в цьому Кодексі, якщо немає окремих вказівок, мають таке значення: **6-1 електронні дані – це інформація в електронному вигляді, яка придатна для сприйняття людиною після обробки автоматичними програмними засобами** **9-1контрольна сума (CRC-сума, хеш-сума) – це деяке значення, що розраховане за набором даних шляхом застосування певного алгоритму і використовується для перевірки цілісності даних під час їх передачі або зберігання** **26-1 хешування- спосіб підтвердження цілісності та незмінності інформації в електронному вигляді під час її зберігання, перезапису, перенесення та передавання каналами зв'язку**
2	**Стаття 84. Докази** 1. Доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких	**Стаття 84. Докази** 1. Доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор,

	слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. 2. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів.	слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. 2. Процесуальними джерелами доказів є показання, речові докази, **електронні докази**, **письмові докази**, висновки експертів.
3	**Стаття 92. Обов'язок доказування** 1. Обов'язок доказування обставин, передбачених статтею 91 цього Кодексу, за винятком випадків, передбачених частиною другою цієї статті, покладається на слідчого, прокурора та, в установлених цим Кодексом випадках, - на потерпілого. 2. Обов'язок доказування належності та допустимості доказів, даних щодо розміру процесуальних витрат та обставин, які характеризують обвинуваченого, покладається на сторону, що їх подає.	**Стаття 92. Обов'язок доказування** 1. Обов'язок доказування обставин, передбачених статтею 91 цього Кодексу, за винятком випадків, передбачених частиною другою цієї статті, покладається на слідчого, прокурора та, в установлених цим Кодексом випадках, - на потерпілого. 2. Обов'язок доказування належності, допустимості **та достовірності** доказів, даних щодо розміру процесуальних витрат та обставин, які характеризують обвинуваченого, покладається на сторону, що їх подає.
4	**Стаття 93. Збирання доказів** 1. Збирання доказів здійснюється сторонами кримінального провадження, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, у порядку, передбаченому цим Кодексом. 2. Сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, **службових та фізичних** осіб **речей, документів, відомостей, висновків**	**Стаття 93. Збирання доказів** 1. Збирання доказів здійснюється сторонами кримінального провадження, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, у порядку, передбаченому цим Кодексом. 2. Сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій,витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, речей, документів, **інформації, отримання від фізичних осіб речей, документів**, отримання висновків експертів, проведення інших

	експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом. 3. Сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, здійснює збирання доказів шляхом витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб **речей**, **копій** документів, відомостей, висновків експертів, **висновків ревізій, актів перевірок;** ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, а також шляхом здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів.	процесуальних дій, передбачених цим Кодексом. 3. Сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, здійснює збирання доказів шляхом витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб документів, інформації,висновків експертів, ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, а також шляхом здійснення інших дій, які здатні забезпечити подання суду належних, допустимих **та достовірних** доказів.
5	**Стаття 99. Документи** 1. Документом є спеціально створений з метою збереження інформації матеріальний об’єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. 2. До **документів**, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп’ютерні дані);	**Стаття 99. Письмові докази** 1. **Письмовими доказами є спеціально створений з метою збереження інформації матеріальний об’єкт, який містить текстову, графічну або змішану інформацію, зафіксовану за допомогою письмових знаків, зображення тощо відомості, які можуть бути використані як доказ обставин, що підлягають доказуванню у кримінальному провадженні .** 2. До **письмових доказів**, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати **виключити**

	2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України; 3) складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій та додатки до них, **а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії;** 4) висновки ревізій та акти перевірок.	2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України; 3) складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій та додатки до них. **виключити**
	Матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України "Про оперативно-розшукову діяльність", за умови відповідності вимогам цієї статті, є **документами** та можуть використовуватися в кримінальному провадженні як докази.	Матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України "Про оперативно-розшукову діяльність", за умови відповідності вимогам цієї статті, є **письмовими доказами** та можуть використовуватися в кримінальному провадженні як докази.
	3. Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал **документа**. **Оригіналом документа є сам документ, а оригіналом електронного документа - його відображення, якому надається таке ж значення, як документу.**	3. Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал **письмового доказу.**
	4. Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних	**Виключити**

	комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.	
	5. Для підтвердження змісту **документа** можуть бути визнані допустимими й інші відомості, якщо:	5. Для підтвердження змісту **письмових доказів** можуть бути визнані допустимими й інші відомості, якщо:
	1) оригінал **документа** втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає;	1) оригінал **письмового доказу** втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає;
	2) оригінал **документа** не може бути отриманий за допомогою доступних правових процедур;	2) оригінал **письмового доказу** не може бути отриманий за допомогою доступних правових процедур;
	3) оригінал **документа** знаходиться у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони.	3) оригінал **письмового доказу** знаходиться у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони.
	6. Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право надати витяги, компіляції, узагальнення документів, які незручно повністю досліджувати в суді, а на вимогу суду - зобов'язані надати **документи** у повному обсязі.	6. Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право надати витяги, компіляції, узагальнення письмового доказу, які незручно повністю досліджувати в суді, а на вимогу суду - зобов'язані надати **такі письмові докази** у повному обсязі.
	7. Сторона зобов'язана надати іншій стороні можливість оглянути або скопіювати оригінали **документів**, зміст яких доводився у передбаченому цією статтею порядку.	7. Сторона зобов'язана надати іншій стороні можливість оглянути або скопіювати оригінали **письмових доказів**, зміст яких доводився у передбаченому цією статтею порядку.

6	**Відсутня**	**§ 6 Електронні докази.** **Стаття101-1. Електронні докази** **1.Електронний доказ – це інформація в електронному вигляді, що містить відомості про обставини, що мають значення для кримінального проводження та підлягають доказуванню, створена, збережена, або передана за допомогою електронних пристроїв, систем, або мереж та яка існує в формі, що забезпечує її автентичність, цілісність та придатність для дослідження.** **2.Електронний документом є документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, у тому числі електронний підпис автора або підпис, прирівняний до власноручного підпису відповідно до Закону України "Про електронну ідентифікацію та електронні довірчі послуги".** **3.Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал електронного доказу або копію інформації в електронному вигляді (електронні дані), що міститься комп'ютерних системах, їх невід'ємних частинах з обов'язковим підтвердженням автентичності такої інформації шляхом хешування або чи іншим способом, що забезпечить можливість перевірки автентичності та цілісності інформації .** **4. Для підтвердження змісту електронних доказів можуть бути визнані допустимими й інші відомості, якщо:**

		1) оригінал електронного доказу втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає; **2) оригінал електронного доказу не може бути отриманий за допомогою доступних правових процедур;** **3) оригінал електронного доказу знаходиться у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони.** **5. Сторона зобов'язана надати іншій стороні можливість оглянути або скопіювати оригінали електронних доказів, зміст яких доводився у передбаченому цією статтею порядку. У випадку неможливості надання оригіналу електронного доказу підтвердити його автентичність у визначеному цим Кодексом порядку.**
7	**Стаття 104. Протокол** …….. 3. Протокол складається з: ……. 3) заключної частини, яка повинна містити відомості про: вилучені речі і документи та спосіб їх ідентифікації; виготовлені дублікати документів, а також копії інформації, у тому числі комп'ютерних даних, та спосіб їх ідентифікації;	**Стаття 104. Протокол** **…….** 3. Протокол складається з: **……..** 3) заключної частини, яка повинна містити відомості про: вилучені речі і письмові докази та спосіб їх ідентифікації; **а також копії інформації в електронному вигляді (електронні дані) та спосіб її ідентифікації та автентифікації .** **……**
8	**Стаття 105. Додатки до протоколів** 1. Особою, яка проводила процесуальну дію, до протоколу долучаються додатки. 2. Додатками до протоколу можуть бути: 1) спеціально виготовлені копії, зразки об'єктів, речей і документів;	**Стаття 105. Додатки до протоколів** 1. Особою, яка проводила процесуальну дію, до протоколу долучаються додатки. 2. Додатками до протоколу можуть бути: 1) спеціально виготовлені копії, зразки об'єктів, речей і документів;

	2) письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії; 3) стенограма, аудіо-, відеозапис процесуальної дії; 4) фототаблиці, схеми, зліпки, носії комп'ютерних даних та інші матеріали, які пояснюють зміст протоколу. **Пункт відсутній**	2) письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії; 3) стенограма, аудіо-, відеозапис процесуальної дії; 4) фототаблиці, схеми, зліпки, носії **інформації в електронному вигляді** (електронних даних)та інші матеріали, які пояснюють зміст протоколу; **5) довідка слідчого, дізнавача, прокурора, спеціаліста про застосований алгоритм хешування та контрольну суму (CRC-сума, хеш-сума) чи інший спосіб, що забезпечить можливість перевірки автентичності та цілісності інформації.**
9	**Стаття 168**. Порядок тимчасового вилучення майна …… 2. Тимчасове вилучення майна може здійснюватися також під час обшуку, огляду. У разі необхідності слідчий чи прокурор виготовляє за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста.	**Стаття 168**. Порядок тимчасового вилучення майна …… 2. Тимчасове вилучення майна може здійснюватися також під час обшуку, огляду. **У разі отримання письмової інформованої згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку на пошук, виявлення та фіксацію інформації в електронному вигляді, що міститься в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку , дізнавач, слідчий чи прокурор може виготовити за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих)**

		системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах з обов'язковим підтвердженням автентичності такої інформації шляхом хешування чи іншим способом, що забезпечить можливість перевірки автентичності та цілісності інформації. Копіювання такої інформації здійснюватися із залученням спеціаліста.
	На вимогу володільця особа, яка здійснює тимчасове вилучення комп'ютерних систем або їх частин, залишає йому копії інформації з таких комп'ютерних систем або їх частин (за наявності технічної можливості здійснення копіювання) з використанням матеріальних носіїв володільця комп'ютерних систем або їх частин. Копії інформації з комп'ютерних систем або їх частин, які вилучаються, виготовляються з використанням технічних засобів, програмно-технічних засобів, апаратно-програмних комплексів володільця із залученням спеціаліста.	На вимогу **власника або** володільця особа, яка здійснює тимчасове вилучення комп'ютерних систем або їх частин, залишає йому копії інформації з таких комп'ютерних систем або їх частин (за наявності технічної можливості здійснення копіювання) з використанням матеріальних носіїв володільця комп'ютерних систем або їх частин. Копії інформації з комп'ютерних систем або їх частин, які вилучаються, виготовляються з використанням технічних засобів, програмно-технічних засобів, апаратно-програмних комплексів володільця із залученням спеціаліста.
10	**Стаття 234. Обшук** **……** 3. У разі необхідності провести обшук слідчий за погодженням з прокурором або прокурор звертається до слідчого судді з відповідним клопотанням, яке повинно містити відомості про: …… 8) обґрунтування того, що доступ до речей, документів або відомостей, які можуть у них міститися, неможливо отримати органом досудового розслідування у добровільному	**Стаття 234. Обшук житла чи іншого володіння особи** **……..** 3. У разі необхідності провести обшук слідчий за погодженням з прокурором або прокурор звертається до слідчого судді з відповідним клопотанням, яке повинно містити відомості про: **…….** 8) обґрунтування того, що доступ до речей, документів або відомостей, які можуть у них міститися, неможливо отримати органом досудового розслідування у добровільному порядку

	порядку шляхом витребування речей, документів, відомостей відповідно до частини другої статті 93 цього Кодексу, або за допомогою інших слідчих дій, передбачених цим Кодексом, а доступ до осіб, яких планується відшукати, - за допомогою інших слідчих дій, передбачених цим Кодексом. Зазначена вимога не поширюється на випадки проведення обшуку з метою відшукання знаряддя кримінального правопорушення, предметів і документів, вилучених з обігу.	шляхом витребування речей, документів, **інформації** відповідно до частини другої статті 93 цього Кодексу, або за допомогою інших слідчих дій, передбачених цим Кодексом, а доступ до осіб, яких планується відшукати, - за допомогою інших слідчих дій, передбачених цим Кодексом. Зазначена вимога не поширюється на випадки проведення обшуку з метою відшукання знаряддя кримінального правопорушення, предметів і документів, вилучених з обігу.
	4. Клопотання про обшук розглядається у суді в день його надходження за участю слідчого або прокурора.	4. Клопотання про обшук розглядається у суді в день його надходження за участю слідчого або прокурора.
	5. Слідчий суддя відмовляє у задоволенні клопотання про обшук, якщо прокурор, слідчий не доведе наявність достатніх підстав вважати, що:	5. Слідчий суддя відмовляє у задоволенні клопотання про обшук, якщо прокурор, слідчий не доведе наявність достатніх підстав вважати, що:
	1) було вчинено кримінальне правопорушення;	1) було вчинено кримінальне правопорушення;
	2) відшукувані речі і документи мають значення для досудового розслідування;	2) відшукувані речі і документи мають значення для досудового розслідування;
	3) відомості, які містяться у відшукуваних речах і документах, можуть бути доказами під час судового розгляду;	3) відомості, які містяться у відшукуваних речах і документах, можуть бути доказами під час судового розгляду;
	4) відшукувані речі, документи або особи знаходяться у зазначеному в клопотанні житлі чи іншому володінні особи;	4) відшукувані речі, документи або особи знаходяться у зазначеному в клопотанні житлі чи іншому володінні особи;
	5) за встановлених обставин обшук є найбільш доцільним та ефективним способом відшукання та вилучення речей і документів, які мають значення для досудового розслідування, а також встановлення місцезнаходження розшукуваних осіб, а також **заходом, пропорційним**	5) за встановлених обставин обшук є найбільш доцільним та ефективним способом відшукання та вилучення речей і документів, які мають значення для досудового розслідування, а також встановлення місцезнаходження розшукуваних осіб, а також **пропорційним заходом втручання у**

	втручанню в особисте і сімейне життя особи.	**право на повагу до приватного і сімейного життя особи, житла та кореспонденції.**
11	**Стаття 236**. Виконання ухвали про дозвіл на обшук житла чи іншого володіння особи …….. 6. Слідчий, прокурор під час проведення обшуку має право відкривати закриті приміщення, сховища, речі, долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється їх відкрити чи зняти (деактивувати) систему логічного захисту або обшук здійснюється за відсутності осіб, зазначених у частині третій цієї статті. Якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку.	**Стаття 236**. Виконання ухвали про дозвіл на обшук житла чи іншого володіння особи **……..** 6. Слідчий,дізнавач прокурор під час проведення обшуку має право відкривати закриті приміщення, сховища, речі, долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється їх відкрити чи зняти (деактивувати) систему логічного захисту або обшук здійснюється за відсутності осіб, зазначених у частині третій цієї статті. **Якщо під час обшуку слідчий, дізнавач, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, а власник чи володілець комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку заперечує проти проведення такого огляду, прокурор слідчий, дізнавач має право здійснити пошук, виявлення та фіксацію інформації електронному вигляді (електронних даних), що на них міститься, тільки після отримання ухвали слідчого судді місцевого загального суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування, на проведення їх обшуку .**

	Особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, відомості про що вносяться до протоколу обшуку.	**Прокурор, слідчий, дізнавач має право здійснити пошук, виявлення та фіксацію інформації в електронному вигляді, що міститься в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, на місці проведення обшуку тільки у разі отримання письмової інформованої згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку.** **……**
12	**Відсутня**	**Стаття 236-1 Обшук комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку** 1**. Обшук комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку проводиться з метою виявлення та фіксації інформації в електронному вигляді про обставини вчинення кримінального правопорушення, а також встановлення місцезнаходження розшукуваних осіб.** **2. Обшук проводиться на підставі ухвали слідчого судді місцевого загального суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування, а у кримінальних провадженнях щодо злочинів, віднесених до підсудності Вищого антикорупційного суду, - на підставі ухвали слідчого судді Вищого антикорупційного суду.** **3. У разі необхідності провести обшук слідчий, дізнавач за погодженням з прокурором або прокурор звертається до слідчого судді з відповідним клопотанням, яке повинно містити відомості про:**

		1) найменування кримінального провадження та його реєстраційний номер; **2) короткий виклад обставин кримінального правопорушення, у зв'язку з розслідуванням якого подається клопотання;** **3) правову кваліфікацію кримінального правопорушення з зазначенням статті (частини статті) закону України про кримінальну відповідальність;** **4) підстави для обшуку;** **5) ідентифікуючі дані комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку. що містять інформацію в електронному вигляді;** **6) особу, якій належить на праві власності чи володінні комп'ютерні системи або їх частини, мобільні термінали систем зв'язку;** **7) інформацію, яку планується відшукати, за який період , а також її зв'язок із вчиненим кримінальним правопорушенням;** **8) обґрунтування того, що доступ до інформації в електронному вигляді , яка може міститися в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, неможливо отримати органом досудового розслідування у добровільному порядку шляхом надання інформативної згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку.** **До клопотання також мають бути додані оригінали або копії документів та інших матеріалів, якими прокурор, слідчий, дізнавач обґрунтовує доводи клопотання, а також витяг з Єдиного реєстру**

		досудових розслідувань щодо кримінального провадження, в рамках якого подається клопотання. **4. Клопотання про обшук розглядається у суді в день його надходження за участю слідчого (дізнавача)або прокурора.** **5. Слідчий суддя відмовляє у задоволенні клопотання про обшук, якщо прокурор, слідчий, дізнавач не доведе наявність достатніх підстав вважати, що:** **1) було вчинено кримінальне правопорушення;** **2) відшукувана інформація в електронному вигляді, електронні документи мають значення для досудового розслідування;** **3) відомості, які містяться у відшукуваній інформації, електронних документах, можуть бути доказами під час судового розгляду;** **4) відшукувана інформація в електронному вигляді, електронні документи знаходяться у зазначених клопотанні комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку;** **5) за встановлених обставин обшук є найбільш доцільним та ефективним способом відшукання інформації в електронному вигляді, електронних документів ,які мають значення для досудового розслідування, а також встановлення місцезнаходження розшукуваних осіб, а також є пропорційним заходом втручанню в право на повагу до приватного і сімейного життя, до кореспонденції .** **6. У разі відмови у задоволенні клопотання про дозвіл на обшук комп'ютерних систем або їх частин,**

		мобільних терміналів систем зв'язку дізнавач, слідчий, прокурор не має права повторно звертатися до слідчого судді з клопотанням про дозвіл на обшук тих самих комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, якщо у клопотанні не зазначені нові обставини, які не розглядалися слідчим суддею.
13	**Стаття 237.** Огляд 1. З метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та **комп'ютерних д**аних. 2. Огляд житла чи іншого володіння особи здійснюється згідно з правилами цього Кодексу, передбаченими для обшуку житла чи іншого володіння особи. Огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у 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 у паперовій формі).	**Стаття 237.** Огляд 1. З метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення **дізнавач,** слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та **електронних даних.** **2. Огляд електронних даних, що містяться в комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку проводиться дізнавачем, слідчим, прокурором у разі отримання письмової інформованої згоди власника або володільця комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку чи інших носіїв інформації за винятком випадків, коли відповідна інформація знаходиться у відкритому доступі.** **Огляд електронних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду відомостей щодо обставин вчинення кримінального правопорушення, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо).** 3. Для участі в огляді **запрошуються** потерпілий, підозрюваний, захисник,

	3. Для участі в огляді **може бути запрошений** потерпілий, підозрюваний, захисник, законний представник та інші учасники кримінального провадження. З метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в огляді може запросити спеціалістів. **……**	законний представник та інші учасники кримінального провадження. З метою одержання допомоги з питань, що потребують спеціальних знань, дізнавач,слідчий, прокурор для участі в огляді запрошує спеціаліста. **……..**
15	**Стаття 245-1 Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису** 1. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису полягає в одержанні слідчим, прокурором від особи, яка є власником або володільцем відповідних приладів або засобів, необхідних для з'ясування обставин, що мають значення для кримінального провадження, копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб. 2. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється на підставі постанови слідчого, прокурора та, за необхідності, за участю спеціаліста. 3. Для здійснення зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису особі, яка є власником або володільцем	**Ст.245-1 Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі** **1. Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі полягає в одержанні дізнавачем, слідчим, прокурором від особи, яка є власником або володільцем відповідних приладів або засобів, необхідних для з'ясування обставин, що мають значення для кримінального провадження, копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях в автоматичному режимі.** **2. Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється на підставі постанови дізнавача, слідчого, прокурора та за участю спеціаліста.** **3. Для отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі особі, яка є**

	відповідних приладів або засобів, пред'являється постанова слідчого, прокурора.	**власником або володільцем відповідних приладів або засобів, пред'являється постанова дізнавача,слідчого, прокурора.**
	4. Постанова слідчого, прокурора про зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису повинна містити:	**4. Постанова дізнавача, слідчого, прокурора про отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі повинна містити:**
	1) найменування кримінального провадження та його реєстраційний номер; 2) відомості про власника або володільця відповідних приладів або засобів;	**1) найменування кримінального провадження та його реєстраційний номер;** **2) відомості про власника або володільця відповідних технічних приладів або засобів;**
	3) період часу, за який має бути здійснено зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису.	**3) період часу, за який має бути отримано електронні дані технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису в автоматичному режимі.**
	5. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється у присутності слідчого, прокурора шляхом самостійного копіювання особою, яка є власником або володільцем відповідних приладів та засобів, або копіювання такою особою за участю спеціаліста відповідних записів на носії, які надаються слідчим, прокурором. Надання таких копій на носіях, особи, яка є власником або володільцем відповідних приладів та засобів, здійснюється за бажанням такої особи.	**5. Отримання електронних даних технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється дізнавачем, слідчим, прокурором шляхом самостійного копіювання або за участю спеціаліста відповідних записів на носії, які надаються дізнавачем, прокурором з обов'язковим підтвердженням автентичності такої інформації шляхом хешування чи іншим способом, що забезпечить можливість перевірки автентичності та цілісності інформації..**
	6. Про здійснення зняття показань технічних приладів та технічних	**6. Про проведення даної слідчої (розшукової) дії складається**

	засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису складається протокол згідно з вимогами цього Кодексу.	**протокол згідно з вимогами цього Кодексу.**
15	**Стаття 298-1 Процесуальні джерела доказів у кримінальних провадженнях про кримінальні проступки** 1. Процесуальними джерелами доказів у кримінальному провадженні про кримінальні проступки, крім визначених статтею 84 цього Кодексу, також є пояснення осіб, результати медичного освідування, висновок спеціаліста, **показання** технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису. Такі процесуальні джерела доказів не можуть бути використані у кримінальному провадженні щодо злочину, окрім як на підставі ухвали слідчого судді, яка постановляється за клопотанням прокурора.	**Стаття 298-1 Процесуальні джерела доказів у кримінальних провадженнях про кримінальні проступки** 1. Процесуальними джерелами доказів у кримінальному провадженні про кримінальні проступки, крім визначених статтею 84 цього Кодексу, також є пояснення осіб, результати медичного освідування, висновок спеціаліста, **електронні дані** технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису. Такі процесуальні джерела доказів не можуть бути використані у кримінальному провадженні щодо злочину, окрім як на підставі ухвали слідчого судді, яка постановляється за клопотанням прокурора.
17	**Стаття 300. Слідчі (розшукові) дії під час досудового розслідування кримінальнихпроступків** 1. Для досудового розслідування кримінальних проступків дозволяється виконувати всі слідчі (розшукові) дії, передбачені цим Кодексом, та негласні слідчі (розшукові) дії, передбачені частиною другою статті 264 та статтею 268 цього Кодексу, а також відбирати пояснення для з'ясування обставин вчинення кримінального проступку, проводити медичне освідування, отримувати висновок спеціаліста, що має відповідати вимогам до висновку експерта, **знімати показання технічних приладів і технічних засобів у провадженнях щодо вчинення кримінальних**	**Стаття 300. Слідчі (розшукові) дії під час досудового розслідування кримінальних проступків** 1. Для досудового розслідування кримінальних проступків дозволяється виконувати всі слідчі (розшукові) дії, передбачені цим Кодексом, та негласні слідчі (розшукові) дії, передбачені частиною другою статті 264 та статтею 268 цього Кодексу, а також відбирати пояснення для з'ясування обставин вчинення кримінального проступку, проводити медичне освідування, отримувати висновок спеціаліста, що має відповідати вимогам до висновку експерта, **отримувати електронні дані технічних приладів і технічних засобів** що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису **в**

	проступків, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, вилучати знаряддя і засоби вчинення кримінального проступку, речі і документи, що є безпосереднім предметом кримінального проступку, або які виявлені під час затримання особи, особистого огляду або огляду речей, до внесення відомостей про кримінальний проступок до Єдиного реєстру досудових розслідувань	**автоматичному режимі**, вилучати знаряддя і засоби вчинення кримінального проступку, речі і документи, що є безпосереднім предметом кримінального проступку, або які виявлені під час затримання особи, особистого огляду або огляду речей, до внесення відомостей про кримінальний проступок до Єдиного реєстру досудових розслідувань

Народні депутати

Додаток Е

ПРОТОКОЛ ОГЛЯДУ

комп’ютерних даних

Місто (сел.)_____ «____»_____20 року

Огляд почато о «____» год. «_____»хв.

Огляд закінчено о «____» год. «____»хв.

_____

Номер кримінального провадження та дата внесення в ЄРДР_____

посада та інші дані, які ідентифікують особу, яка проводить слідчу дію

_____

Рішення суду, яке дає дозвіл на проведення такої слідчої дії

_____

Відповідно до ст. 104, 105, 106, 234, 237, 223 КПК України в присутності понятих:

1) _____

(прізвище, ім’я, по батькові, дата народження, місце проживання, особистий підпис)

2) _____,

(прізвище, ім’я, по батькові, дата народження, місце проживання, особистий підпис)

яким відповідно до ст. 11, 14, 15, 223 КПК України роз’яснено їхні права й обов’язки;

за участю потерпілого: _____,

(прізвище, ім’я, по батькові, дата народження, місце проживання, особистий підпис)

якому відповідно до ч. 1, 2 ст. 56, ст. 57 КПК України роз’яснено його права й обов’язки;

за участю підозрюваного: _____,

(прізвище, ім’я, по батькові, дата народження, місце проживання, особистий підпис)

якому відповідно до ч. 3, 5, 6, 7 ст. 42 КПК України роз’яснено його права й обов’язки;

за участю захисника: _____,

(прізвище, ім’я, по батькові, підтвердження повноважень (свідоцтво про зайняття адвокатською діяльністю,ордер, договір із захисником або доручення органу (установи) уповноваженого законом на надання безоплатної правової допомоги) особистий підпис))
якому відповідно ст. 46, 47 КПК України роз’яснено його права і обов’язки;
за участю законного представника: _____
(прізвище, ім’я, по батькові, дата народження, місце проживання, особистий підпис)
якому відповідно до ч. 5 ст. 44, ч. 4 ст. 58, ч. 2 ст. 59 КПК України роз’яснено
його права і обов’язки;
за участю спеціаліста: _____
(прізвище, ім’я, по батькові,підтвердження компетенції (володіння спеціальними знаннями та навичками) особистий підпис)),
якому відповідно до ч. 4, 5 ст. 71 КПК України роз’яснено його права й обов’язки;
за участю інших учасників: _____;
(прізвище, ім’я, по батькові, посада, особистий підпис)

за участю власника (володільця) комп’ютерних систем чи інших пристроїв, в яких знаходяться комп’ютерні дані _____
(прізвище, ім’я, по батькові, дата народження, місце проживання, особистий підпис)
Перед початком огляду зазначеним вище особам роз'яснено їхнє право бути присутніми при всіх діях, які проводяться в процесі огляду, робити зауваження, що підлягають занесенню до протоколу. Особам, які беруть участь у проведенні огляду, також роз’яснено вимоги ст. 222 КПК України про їх обов’язок не розголошувати відомості щодо проведеної процесуальної дії, а також про застосування технічних засобів фіксації, умови та
порядок їх використання:
_____
(характеристики технічних засобів фіксації та носіїв інформації, які застосовуються
при проведенні цієї процесуальної дії, підписи осіб)

Перед початком огляду зазначеним вище особам роз’яснено їхнє право бути присутніми при всіх діях, які проводяться в процесі огляду, робити зауваження, що підлягають занесенню до протоколу.

Одночасно всім учасникам роз’яснено положення ст. 63 Конституції України, відповідно до якої: «особа не несе відповідальності за відмову давати показання або пояснення щодо себе, членів сім’ї чи близьких родичів, коло яких визначається законом та положення ст. 18 КПК України про те, що жодна особа не може бути примушена визнати свою винуватість у вчиненні

кримінального правопорушення або примушена давати пояснення, показання, які можуть стати підставою для підозри,обвинувачення у вчиненні нею кримінального правопорушення. Кожна особа має право не говорити нічого з приводу підозри чи обвинувачення проти неї, у будь-який момент відмовитися відповідати на запитання, а також бути негайно повідомленою про ці права. Жодна особа не може бути примушена давати пояснення, показання, які можуть стати підставою для підозри, обвинувачення у вчиненні її близькими родичами чи членами її сім'ї кримінального правопорушення.

(підпис осіб, які беруть участь у проведенні огляду).

Проведеним оглядом встановлено:

_____

Опис того як комп'ютерні системи чи інші цифрові пристрої були упаковані

_____

Ідентифікаційні ознаки комп'ютерних систем чи інших пристроїв, в яких знаходяться комп'ютерні дані які підлягають огляду, в тому числі і автономні пристрої зберігання даних: внутрішні та зовнішні жорсткі диски (HDD, SSHD, SSD, CD, DVD, SD, microSD, флеш пам'ять тощо)

_____

Елементи ідентифікації (марка, модель, серійний номер або код IMEI та операційну систему встановлену на пристрої, дату встановлення операційної системи, облікові записи користувачів, мережеві налаштування, код, пароль блокування на мобільному пристрої, ємність зберігання, різні написи, можливі видимі недоліки чи пошкодження

_____

Апаратні пристрої та програми, які будуть використані для такого огляду

_____

Час початку огляду комп'ютерних даних (обов'язково перевірити часовий пояс, який використовується в системі)_____

Під час огляду виявлено

_____

-назва файла, який оглядається, розширення файла, тип файла, дата та час створення , дата та час останнього використання, дата та час останньої зміни, розташування, значення хешів

-всі зроблені кроки в хронологічному порядку (детальний опис проведених заходів і операцій)

- посилання на технічний звіт сформований програмними засобами, які використовують для криміналістичного аналіз;

-опис носія інформації, на який здійснюється копіювання або створюється образ;

-програмні засоби, що забезпечують цілісність скопійованих даних (хешування);

-опис комп'ютерних систем та цифрових пристроїв, які підлягають упакуванню після огляду

_____

Час закінчення огляду комп'ютерних даних_____

Під час огляду застосовані технічні засоби:_____

(вказуються застосовування фото -, відеозйомки, інших технічних та спеціальних засобів, їх технічні параметри)

_____

Протокол прочитаний, записано_____

(зауваження учасників огляду)

Учасники:

1. _____ /_____/

(прізвище, ім'я, по батькові) (підпис)

Поняті:

1. _____ /_____/

(прізвище, ім'я, по батькові) (підпис)

2. _____ /_____/

(прізвище, ім'я, по батькові) (підпис)

Огляд провів:

_____

(слідчий, прокурор, посада, найменування органу, підпис, прізвище, ініціали)

Додаток Є

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких відображено основні результати дослідження:

1. Смаль І. А. Проблемні аспекти застосування електронних доказів у кримінальному судочинстві. *Право і суспільство*. 2021. № 4. С. 226–232. DOI: 10.32842/2078-3736/2021.4.30.

2. Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу. *Прикарпатський юридичний вісник*. Одеса, 2022. Вип. 2. С. 122–127. DOI: 10.32837/pyuv.v0i2.1028.

3. Смаль І. А. Практичні аспекти зняття показань технічних приладів та технічних засобів, що мають функцію фото- кінозйомки, відеозапису чи засобів фото- кінозйомки, відеозапису у кримінальному процесі. *Юридичний науковий електронний журнал.* 2023. № 6. С. 552–558. DOI: https://doi.org/10.32782/2524-0374/2023-6/127 (дата звернення: 20.03.2025).

4. Смаль І. А. Мережа Інтернету як джерело доказової інформації у кримінальному провадженні. *The Journal of Eastern European Law / Журнал східноєвропейського права*. 2024. № 128. С. 237–243.

Наукові праці, в яких засвідчено апробацію матеріалів дослідження:

1. Смаль І. А. Історичні передумови появи електронних доказів як засобів доказування в кримінальному процесі. *Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2020 : матеріали міжнар. наук.- практ. конф. (м. Чернігів, 23–24 квіт. 2020 р.)* : у 2 т. Чернігів : Акад. ДПтС, 2020. Т. 2. С. 266–268.

2. Смаль І. А. Перспективи використання електронних доказів як засобів доказування у кримінальному процесі. *Теорія та практика сучасної юриспруденції : матеріали XXVI всеукр. наук.-практ. конф. (м. Харків, 20 груд. 2020 р.)* : у 2 т. Харків

: Нац. юрид. ун-т ім. Ярослава Мудрого, 2020. Т. 2. С. 324–326.

3. Остапчук Л. Г., Смаль І. А. Кіберзлочинність та електронні докази в кримінальному судочинстві. *Актуальні питання теорії та практики в галузі права, освіти, соціальних та поведінкових наук – 2021 : матеріали міжнар. наук.- практ. конф. (м. Чернігів, 22–23 квіт. 2021 р.)* : у 2 т. Чернігів : Акад. ДПтС, 2021. Т. 2. С. 135–138.

4. Смаль І. А. Проблематика огляду носіїв цифрових даних через призму забезпечення прав та законних інтересів особи. *Інтеграція теорії у практику : проблеми, пошуки, перспективи : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 5 листоп. 2021 р.)*. Чернігів : Акад. ДПтС, 2021. С. 186–189.

5. Смаль І. А. Окремі аспекти збирання та процесуального закріплення інформації з електронних носіїв. *Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квіт. 2023 р.)* : у 2 т. Чернігів : Акад. ДПтС, 2023. Т. 1. С. 327–330.

6. Смаль І. А. Межі втручання у приватне спілкування під час збирання електронних доказів у кримінальному процесі. *Трансформації особистості, суспільства та ринку праці: виклики майбутнього та вплив на освіту : зб. тез доп. міжнар. наук.-практ. конф., м. Харків, 20–22 верес. 2023 р*. Харків : ХНУ ім. В. Н. Каразіна, 2023. С. 440–441.

7. Смаль І. А. Втручання у право на приватність під час здійснення досудового розслідування у вимірі стандартів статті 8 Конвенції про захист прав людини і основоположних свобод. *Кримінальний процес: сучасний вимір та перспективні тенденції : матеріали VI Харків. кримін. процес. полілогу (м. Харків, 17 квіт. 2024 р.)*. Харків : Право, 2024. С. 138-143.