Юридичні науки

УДК 343.9

Цюприк Ігор Володимирович

доктор юридичних наук,

професор кафедри кримінального процесу та криміналістики

Національна академія СБУ

Tsiupryk Igor

Doctor of Law, Professor of the

Department of Criminal Procedure and Forensics

National Academy of the Security Service of Ukraine

ORCID: 0009-0007-4460-9968

ЕЛЕКТРОННІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОБЛЕМИ ПРОЦЕСУАЛЬНОГО РЕГУЛЮВАННЯ В УКРАЇНІ
ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: ISSUES OF PROCEDURAL REGULATION IN UKRAINE

Анотація. *Вступ. У сучасному кримінальному судочинстві спостерігається стрімке зростання ролі інформаційних технологій, що безпосередньо впливає на трансформацію усталених підходів до процесу доказування. Одним із найбільш динамічних явищ у цій сфері є використання електронних доказів, які дедалі частіше стають основним джерелом інформації у кримінальних провадженнях, що особливо помітно в умовах відкритої збройної агресії російської федерації та стрімкого зростання кількості злочинів, які посягають на основи національної безпеки, спрямовані проти миру й безпеки людства, а також мають терористичний характер. Переважна більшість таких протиправних діянь вчиняється у кіберпросторі або за активного використання цифрових технологій, що зумовлює необхідність використання інформаційних*

технологій у процесі доказування як одного з ключових інструментів кримінального переслідування. Саме тому електронні докази набувають вирішального значення під час встановлення фактичних обставин у кримінальних провадженнях.

Комплексний аналіз положень Кримінального процесуального кодексу України (далі - КПК України) дозволяє дійти висновку, що національне законодавство не містить чітко структурованого, системного врегулювання порядку збирання, подання, дослідження та оцінки електронних доказів, що створює суттєві перешкоди для ефективного застосування таких доказів у кримінальному процесі. У результаті, значна частина інформації, що становить інтерес для органів досудового розслідування та суду залишається у зоні невизначеності, що, у свою чергу, створює простір для зловживань і маніпуляцій з боку учасників кримінального провадження, що прямо впливає на ефективність досудового розслідування, справедливість судового розгляду та дотримання балансу між публічним інтересом і правами сторони захисту.

Зазначена проблема особливо загострюється у контексті оцінки належності, допустимості, достовірності та достатності електронних доказів. Відсутність єдиних стандартів чи процесуальних інструментів роботи з електронними доказами не лише ставить під сумнів принцип правової визначеності, а й нерідко суперечить засадам змагальності, рівності сторін та справедливого суду, гарантованим Конституцією України та міжнародними актами.

Метою цієї наукової статті є детальне дослідження теоретико-правових аспектів використання електронних доказів, виявлення прогалин у національному кримінальному процесуальному законодавстві України щодо процесуальної фіксації електронних доказів у кримінальному судочинстві, а також визначення шляхів їх усунення з урахуванням

міжнародних стандартів і практичних потреб правоохоронної та судової діяльності.

Матеріали і методи. У процесі дослідження використано як загальнонаукові, так і спеціально-юридичні методи пізнання. До загальнонаукових методів належать аналіз, синтез, індукція, дедукція, абстрагування, що дозволили сформувати цілісне бачення проблеми. Спеціально-юридичний інструментарій включав формально-юридичний, логіко-нормативний та порівняльно-правовий методи, які застосовувались для вивчення правових норм, їхнього взаємозв'язку, а також порівняння національного підходу до регулювання електронних доказів із міжнародними стандартами. Матеріальну основу дослідження склали: положення КПК України, Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про електронні документи та електронний документообіг», міжнародні стандарти, зокрема Конвенція про кібербезпеку, The Berkeley Protocol on Digital Open Source Investigations, сучасна наукова доктрина, а також національна судова практика, сформована Касаційним кримінальним судом у складі Верховного Суду.

Результати. У межах наукової статті здійснено концептуальне розмежування понять «електронний документ», «електронний доказ», «комп'ютерні дані» та «цифровий доказ» з урахуванням нормативного змісту, контексту правозастосування та функціонального призначення кожного з цих елементів у межах кримінального процесу. Обґрунтовано, що чинне законодавство України потребує істотного удосконалення, у тому числі доповнення окремими процесуальними нормами, які б закріплювали поняття електронних доказів, визначали їхні ознаки, порядок фіксації, обробки, зберігання та використання, а також встановлювали єдині правила поводження з такими доказами у кримінальному провадженні.

Окрему увагу приділено аналізу сформованої судової практики щодо використання електронних доказів, яка демонструє фрагментарний підхід та відсутність єдиного тлумачення окремих процесуальних положень, що підтверджує нагальну потребу у систематизації нормативного врегулювання відповідних питань.

Перспективи подальших досліджень. У подальших наукових дослідженнях варто зосередити увагу на: законодавчому закріпленні визначення поняття «електронний доказ» у кримінальному процесуальному законодавстві України та його узгодженні з міжнародними нормами у сфері дотримання прав та свобод людини під час поводження з електронними доказам; розробці чітких алгоритмів процесуальної фіксації, зберігання та подання електронних доказів.

Ключові слова: *кібербезпека, електронний доказ, цифровий доказ, електронний документ, комп'ютерні дані, доказування, допустимість доказу, Протокол Берклі.*

Summary. *Introduction. In modern criminal proceedings, the role of information technologies is rapidly increasing, directly influencing the transformation of established approaches to the evidentiary process. One of the most dynamic phenomena in this sphere is the use of electronic evidence, which is increasingly becoming the primary source of information in criminal cases.*

A comprehensive analysis of the provisions of the Criminal Procedure Code of Ukraine (hereinafter – the CPC of Ukraine) leads to the conclusion that national legislation does not contain a clearly structured and systematic regulation of the procedure for collecting, submitting, examining, and evaluating electronic evidence. This creates significant obstacles to the effective use of such evidence in criminal proceedings. As a result, a substantial amount of information of interest to pre-trial investigation bodies and the court remains in a zone of legal uncertainty, which in turn opens the way for abuses and

manipulations by participants in criminal proceedings. This directly affects the efficiency of pre-trial investigation, the fairness of trial, and the maintenance of a proper balance between the public interest and the rights of the defence.

This problem becomes particularly acute in the context of assessing the relevance, admissibility, reliability, and sufficiency of electronic evidence. The absence of unified standards or procedural instruments for working with electronic evidence not only calls into question the principle of legal certainty but also often contradicts the principles of adversarial proceedings, equality of arms, and the right to a fair trial, as guaranteed by the Constitution of Ukraine and international instruments.

The purpose of this scientific article is to conduct a detailed study of the theoretical and legal aspects of the use of electronic evidence, to identify gaps in the national criminal procedural legislation of Ukraine concerning the procedural recording of electronic evidence in criminal proceedings, and to define ways to eliminate these gaps, taking into account international standards and the practical needs of law enforcement and judicial activities.

Materials and Methods. The study employs both general scientific and special legal methods of research. General scientific methods include analysis, synthesis, induction, deduction, and abstraction, which made it possible to form a comprehensive understanding of the problem. Special legal tools included formal-legal, logical-normative, and comparative legal methods used to study legal norms, their interrelation, and to compare the national approach to the regulation of electronic evidence with international standards. The material basis of the research consists of: the provisions of the Criminal Procedure Code of Ukraine, the Law of Ukraine «On Electronic Documents and Electronic Document Management», international standards, including The Berkeley Protocol on Digital Open Source Investigations, contemporary legal doctrine, as well as national case law developed by the Criminal Cassation Court within the Supreme Court.

Results. The article provides a conceptual distinction between the notions of «electronic document», «electronic evidence», «computer data» and «digital evidence» taking into account their normative content, legal application context, and functional role within criminal proceedings. It is argued that the current legislation of Ukraine requires amendments introducing specific procedural norms that would define the concept of electronic evidence, determine its characteristics, and establish the procedures for its recording, processing, storage, and use, as well as unified rules for handling such evidence in criminal proceedings.

Special attention is devoted to the analysis of existing case law on the use of electronic evidence, which demonstrates a fragmented approach and the absence of a uniform interpretation of certain procedural provisions, thereby confirming the urgent need for systematisation of the regulatory framework in this area.

Prospects for Further Research. Further studies should focus on: legislative consolidation of the definition of «electronic evidence» in the criminal procedural legislation of Ukraine and its harmonisation with international standards on the protection of defence rights in the handling of electronic evidence; and the development of clear procedural algorithms for the recording, preservation, and submission of electronic evidence.

Key words: *electronic evidence, digital evidence, electronic document, computer data, proof, admissibility of evidence, Berkeley Protocol.*

Постановка проблеми. Стрімкий розвиток цифрових технологій та інформатизація суспільства зумовили появу нових видів джерел доказової інформації у кримінальному судочинстві, серед яких важливе місце посідають електронні докази. Водночас чинне кримінальне процесуальне законодавство України не забезпечує достатньо чіткого, внутрішньо узгодженого та системного механізму роботи з ними, шо свідчить про

недостатню готовність правової системи та законодавства до динамічного розвитку цифрового середовища.

Найбільш проблемними залишаються питання забезпечення цілісності електронних доказів, дотримання принципів їх автентичності, достовірності та допустимості, а також належної процесуальної фіксації. Відсутність чітко визначених процесуальних інструментів створює нагальну потребу у проведенні наукового аналізу, виявленні прогалин у законодавстві, розробленні точних юридичних дефініцій і процесуальних стандартів, а також у впровадженні кращих практик міжнародного досвіду в українську правову систему.

Аналіз останніх досліджень і публікацій. Питання нормативного врегулювання електронних доказів у кримінальному процесі є предметом наукового інтересу багатьох українських дослідників. У сучасній правовій доктрині спостерігається активна дискусія щодо формулювання належного визначення електронних доказів, а також розробки ефективних процесуальних механізмів їх збирання, фіксації, дослідження та зберігання. Так, Фоміна Т. Г., Рачинський О. О. та Мілімко Л. В. запропонували авторське визначення поняття «електронний (цифровий) доказ» у кримінальному провадженні [13,16]. Окрему увагу технічному змісту електронних доказів приділяють Поліщук А. та Киливник К., які зосередилися на вивченні правової природи таких об'єктів, як системні журнали, кеш-файли, видалені файли [14]. Гарасимів О.І., Марко С.І. та Ряшко О.В. зробили внесок у визначення специфічних ознак електронних доказів, підкресливши, що саме дотримання визначених вимог щодо форми електронного документа забезпечує його належну доказову силу [15]. Смаль І. А. звернув увагу на необхідність виокремлення обшуку електронного носія інформації як самостійної слідчої дії, оскільки звичні форми процесуального втручання не забезпечують належного рівня процесуальних гарантій [17]. Тагієв С. Р., наприклад, переконаний що для

того, щоб електронний доказ отримав правове закріплення необхідно продовжувати наукове вивчення всіх ознак і особливостей електронних носіїв інформації, виявити ті ознаки, які мають правове значення, сформувати нові процесуальні правила виявлення та вилучення електронних носіїв інформації та їх дослідження з урахуванням юридично значущих ознак [18].

Сукупність значної кількості дослідження та публікацій засвідчують високий науковий інтерес до висвітленої теми, проте також демонструють й відсутність єдності в поглядах щодо поняття та використання електронних доказів у кримінальному провадженні, що підтверджує доцільність подальшого теоретико-прикладного аналізу, зокрема з урахуванням міжнародних стандартів і новітніх технологічних реалій.

Виклад основного матеріалу. У сучасних умовах цифровізації суспільних відносин дедалі актуальнішим постає питання належного нормативного врегулювання обігу електронної інформації в кримінальному процесі, що, зокрема, вимагає не лише унормування порядку фіксації та оцінки відповідної інформації, а й чіткого розмежування базових понять, що активно використовуються у правозастосовній практиці: «електронний доказ», «комп'ютерні дані», «цифровий доказ», «електронний документ». Відсутність нормативного визначення або ж ототожнення цих понять породжує правову невизначеність у процесуальній кваліфікації дій, унеможливлює формування сталої судової практики та ставить під сумнів допустимість певної категорій доказів.

Так, термін «цифровий доказ» на сьогодні використовується переважно у міжнародній практиці та наукових дослідженнях, де його зміст часто ототожнюється з «електронним доказом». Проте слід звернути увагу, що у рамках концептуальних підходів, цифровий доказ - це будь-яка інформація цифрового походження, яка може мати значення для розслідування та бути використаною як доказ у кримінальному процесі,

тобто це поняття охоплює як структуровані, так і неструктуровані дані, добуті з відкритих або закритих цифрових джерел, із дотриманням методів, що забезпечують їхню автентичність та допустимість. У п 3.5. ДСТУ 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» зазначено, що цифровий доказ – це інформація або данні, збережені або передані в бінарному вигляді (за допомогою двійкового коду), на які можна покладатися як на докази [6]. Цифровий доказ фактично є міжнародною категорією, що охоплює електронні документи, електронні повідомлення, мультимедійні файли, а також сліди цифрової активності особи в мережі.

Головною ознакою поняття «електронний доказ» є не форма, а зміст і джерело походження інформації, що має доказове значення. До електронних доказів належать будь-які відомості, що містяться в електронній формі й мають значення для кримінального провадження незалежно від того, чи оформлені вони у вигляді документа, наприклад електронні листи, записи з месенджерів або систем відеоспостереження, метадані, геолокаційні дані, історія дій користувача в обліковому записі. Важливою ознакою електронного доказу є його походження з цифрового середовища, а також можливість ідентифікації джерела, часу створення і способу зберігання.

Комп'ютерні дані, у свою чергу, є ще більш ширшим і технічним за природою терміном, який охоплює будь-яку інформацію, що зберігається, обробляється або передається за допомогою електронно-обчислювальної техніки. В цьому контексті, важливим є законодавче визначення терміну «дані» у Законі України «Про електронні комунікації», відповідно до якого дані – це інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки, технічними та програмними засобами [3]. В той же час, відповідно до п. b статті 1 Конвенції про кіберзлочинність: «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 [4]. У кримінальному процесі комп'ютерні дані можуть стати об'єктом слідчих (розшукових) дій, зокрема огляду в порядку ст. 237 КПК України [1]. Водночас самі по собі комп'ютерні дані не завжди мають доказове значення, поки не пройдуть оцінки на предмет достовірності, належності та допустимості.

Поняття «цифровий доказ», «електронний доказ» та «комп'ютерні дані» у сучасній кримінально-процесуальній практиці здебільшого залишаються абстрактними та не мають достатньої нормативної визначеності. Водночас категорія «електронний документ» хоча й не є повністю врегульованою на законодавчому рівні, проте вже використовується та певною мірою закріплена у національній правозастосовній практиці.

В контексті наведеного актуальним є проведення порівняльного аналізу визначень поняття «документ» і «електронний документ», закріплених у КПК України, Законі України «Про електронні документи та електронний документообіг» та Державних Стандартах України 7157:2010 «Інформація та документація. Видання електронні. Основні види та вихідні відомості».

Згідно з ч. 1 ст. 99 КПК України, документом визнається матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ [1]. Вказана дефініція акцентує увагу на триєдиній природі документа як: матеріального об'єкта, носія інформації, доказу. Тож, варто стверджувати, що документ у розумінні КПК України - це не лише форма подання інформації, а й процесуальний інструмент, що повинен відповідати певним вимогам достовірності, допустимості та належності.

Відповідно до ст. 5 Закону України «Про електронні документи та електронний документообіг», електронний документ - це документ, інформація в якому зафіксована у вигляді електронних даних з обов'язковими реквізитами[2]. Вказане визначення розширює класичне розуміння документа за рахунок дематеріалізації носія (відсутності його фізичної форми) та його правової співмірності з паперовим документом за наявності необхідної сукупності постійних елементів – реквізитів.

У свою чергу, п. 3.8 ДСТУ 7157:2010 «Інформація та документація. Видання електронні. Основні види та вихідні відомості» деталізує технічний аспект та вказує, що для використання електронного документу потрібні засоби обчислювальної техніки [5]. Зазначена термінологія дозволяє виокремити спільну ознаку документів, а саме їх функціональне призначення - збереження та передача інформації. Водночас, не кожен електронний документ автоматично є доказом у кримінальному провадженні, оскільки для цього необхідна його процесуальна легалізація у порядку, передбаченому КПК України.

Також, варто звернути увагу, що використання електронних документів - доказів у кримінальному провадженні, значно відрізняється від норм цивільно-процесуального та господарського-процесуального права України. Як зазначено у постанові від 23.01.2025 по справі № 638/6886/22 Касаційного кримінального суду: «…Натомість у кримінальному провадженні щодо ОСОБА_6 та ОСОБА_9 суд оцінював докази за правилами, визначеними кримінальним процесуальним законом, а саме в контексті реалізації приписів статей 84-86, 93, 94, 99 КПК, де відображені відповідні критерії оцінки доказів на предмет їх допустимості, в тому числі й електронних документів, 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 України «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.

Захисник ОСОБА_7 , спираючись на положення ч. 1 ст. 7 Закону № 851-IV,в обґрунтування вимог касаційної скарги посилається на недопустимість як доказів даних електронної документації діяльності Ізюмського РЕМ АТ «ХАРКІВОБЛЕНЕРГО» під час окупації, яка міститься на оптичному носії інформації CD. Стверджує, що з урахуванням правозастосовної позиції Верховного Суду в постанові від 29 березня 2021 року у справі № 554/5090/16-к, у значенні ст. 99 КПК електронний документ вважається процесуальним джерелом доказів лише після накладення електронного підпису та/або використання іншого способу ідентифікації автора такого документа. Проте такі доводи захисника Верховний Суд вважає необґрунтованими, а посилання на відповідну правозастосовну позицію цього Суду - нерелевантним…» [11].

Вказана судова практика засвідчує наявність нормативної колізії між КПК України, як спеціального процесуального акту в кримінальному судочинстві та інших чинних нормативно - правових актів України, яка потребує негайного вирішення та вироблення єдиної доктрини щодо використання електронного документу в кримінальному процесі, яка відповідатиме як вимогам процесуального права, так і вимогам інформаційної безпеки та цифрової ідентифікації.

Не менш важливим залишається й правовий статус електронного документа в кримінальному провадженні у частині визначення його «оригіналу», оскільки від правильного розуміння цього терміну залежить допустимість та подальша оцінка електронного доказу в суді.

Частина 3 статті 99 КПК України встановлює, що оригіналом документа є сам документ, а оригіналом електронного документа - його

відображення, якому надається таке ж значення, як документу [1]. Ключовим у даному визначенні є термін «відображення», який, однак, не має законодавчого визначення, що ускладнює його розуміння та тлумачення.

Фактично, КПК України дозволяє використовувати копію електронного документа, яка відображає його зміст, як еквівалент оригіналу за умови, що їй «надається таке ж значення», що свідчить про орієнтованість на зовнішнє сприйняття інформації та відсутність обов'язковості електронного підпису чи технічної автентифікації. Попри такий гнучкий процесуальний підхід вказане створює ризики правової невизначеності, оскільки суд без опори на об'єктивні технічні критерії, самостійно вирішує, коли таке «відображення» відповідає оригіналу. Аналогічно, оригіналом документа відповідно до ч.4 ст. 99 КПК України визнається й дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, виготовлені слідчим, прокурором із залученням спеціаліста [1].

В той же час, на відміну від КПК України, ст. 7 Закону «Про електронні документи та електронний документообіг» встановлює чітке поняття, яке передбачає 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;

- кожний з електронних примірників, у разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації;

- ідентичний за документарною інформацією та реквізитами електронний документ та візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством [2].

Норми, які регламентують використання документів як в КПК України, так і в Законі не суперечать одна одній безпосередньо, проте їхні концепції суттєво відрізняються, що й призводить до неоднорідності судової практики. Саме тому, в ході дослідження було здійснено аналіз релевантних судових рішень Касаційного кримінального суду Верховного Суду з метою виявлення усталеної судової практики та формування висновків щодо правового розуміння спірних аспектів використання електронних доказів у кримінальних провадженнях. У результаті проведеного аналізу встановлено наступні правові позиції.

1. Відповідно до Постанови від 04.10.2023 по справі № 159/1506/20 Касаційного кримінального суду: «…Матеріальний носій - лише спосіб збереження інформації, який має значення, тільки коли електронний документ виступає речовим доказом. Головною особливістю електронного документа є відсутність жорсткої прив`язки до конкретного матеріального носія. Один і той же електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення.

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.

Отже, дослідження диска, на який перенесено дані з іншого накопичувача, за умови того, що сторона захисту не посилається на монтаж та невідповідність відтвореного запису ходу проведення обшуку, не

свідчить про порушення порядку дослідження доказів, зокрема тих, що зафіксовані на електронному носії інформації…» [9].

У даному рішенні Касаційний кримінальний суд формулює надзвичайно важливу правову позицію щодо електронного документа як джерела доказів у кримінальному процесі, акцентуючи на його нематеріальній природі та техніко-правовій відмінності від традиційних документів на паперовому носії.

Суд обґрунтовано виходить із того, що матеріальний носій не є визначальним для ідентифікації електронного документа, що відповідає сучасній інформаційній парадигмі, згідно з якою електронний документ – це не об'єкт у фізичному сенсі, а сукупність електронних даних, які можуть бути збережені, передані та відтворені на різних носіях, не втрачаючи при цьому своєї юридичної природи.

Окремо заслуговує на увагу теза суду про неприпустимість ототожнення електронного доказу як засобу доказування з матеріальним носієм, на якому він збережений, що є цілком коректним підходом відповідно до положень ст. 99 КПК України.

Суд обґрунтовано наголошує, що перенесення даних з одного електронного носія на інший (наприклад, із жорсткого диска на диск для огляду в суді) не нівелює їх доказової сили, якщо сторона захисту не заявляє про факти підробки, маніпуляцій або монтажу, що також слугує гарантією процесуальної економії, оскільки у цифрову епоху вимагати дослідження «оригіналу» виключно на первинному носії було б архаїчним і технічно невиправданим.

2. Відповідно до Постанови від 19.09.2023 по справі № 756/8251/19 Касаційного кримінального суду: «…Один і той же електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як

оригінали та відрізнятися один від одного тільки часом і датою створення. 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…» [8].

У вказаному судовому рішенні Касаційний кримінальний суд чітко окреслює техніко-правовий механізм ідентифікації електронного документа як оригіналу, що має важливе значення для процесуальної допустимості таких доказів у кримінальному провадженні. Суд визнає, що ідентифікація електронного документа як оригіналу можлива:

– шляхом перевірки контрольної суми уповноваженою особою, яка його створила. Hash-сума (або CRC) - це унікальний цифровий відбиток файлу, що дає змогу підтвердити його цілісність та автентичність. Зміна хоча б одного байта вмісту призводить до зміни контрольної суми, тобто, якщо обчислена hash-сума співпадає з початковою, можна стверджувати, що файл не був змінений;

– за допомогою спеціального дослідження, зокрема судової комп'ютерно-технічної експертизи, що особливо важливо у випадках спірності походження електронного документа та наявності заперечень із боку захисту щодо достовірності даних.

Таким чином, наведена правова позиція дає чітке розуміння сторонам кримінального провадження, що відсутність електронного підпису не є автоматичною підставою для визнання доказу недопустимим, якщо існують інші способи перевірки його автентичності. У перспективі ця практика може лягти в основу типових рекомендацій або методичних підходів до обробки електронних доказів у кримінальному процесі.

3. Відповідно до Постанови від 12.06.2024 по справі № 569/1908/23 Касаційного кримінального суду: «…оперуповноваженим

співробітником було проведено огляд інтернет-сторінок, зроблено скриншоти і завантажено відеофайли, які є додатками до протоколів огляду, оформлених, відповідно до вимог КПК.

Місцевий суд, з висновком якого погодився суд апеляційної інстанції, оцінюючи досліджені та перевірені в судовому засіданні докази, визнав їх такими, що перебувають в об`єктивному взаємозв`язку з інкримінованими злочинами, не спростовані в ході судового розгляду, чинним законодавством передбачені як джерела доказування та зібрані з дотриманням процесуальних норм.

…Як убачається з матеріалів провадження, під час судового провадження сторона захисту хоча й ставила питання про недостовірність таких доказів, однак не заявляла будь-яких клопотань про залучення спеціалістів чи експертів, проведення експертизи, а тому колегія суддів погоджується з висновками, зробленими місцевим судом…» [10].

У наведеній постанові Касаційний кримінальний суд підтверджує важливу позицію щодо допустимості результатів огляду веб-ресурсів (зокрема, шляхом створення скріншотів та відеофайлів), здійсненого уповноваженою особою, як доказів у кримінальному провадженні, якщо вони оформлені у відповідному протоколі огляду та не були спростовані стороною захисту.

Важливою є згадка про те, що суд оцінював не лише наявність доказів, а їх зв'язок із предметом доказування, що є черговим підтвердженням важливості визнання цифрових доказів, отриманих, зокрема, через огляд відкритих інтернет-ресурсів, як повноцінних доказів у кримінальному процесі, за умови належного їх процесуального оформлення.

4. Відповідно до Постанови від 06.12.2021 по справі № 756/4855/17 Касаційного кримінального суду: «…відповідно до ч. 3 ст. 99 КПК України оригіналом документа є сам документ, а оригіналом

електронного документа його відображення, якому надається таке ж значення, як документу. Відповідна норма дозволяє використовувати електронні документи, інформацію, розміщену в мережі Інтернет, без отримання безпосереднього доступу до фізичних носіїв такої інформації. Це може бути пов`язано як з тим, що відповідна інформація перебуває у вільному доступі, у зв`язку із чим виключається необхідність застосування процедури тимчасового доступу до речей і документів, яка передбачена главою 15 КПК України, так і неможливістю застосування такої процедури через те, що, наприклад, сервери, на яких розміщені електронні документи, які мають значення для кримінального провадження, можуть бути розміщені в будь-якому місці світу, що значно ускладнює процес отримання доступу до таких серверів та завдає шкоди кримінальному провадженню.

У зв`язку із цим веб-сторінка з електронним документом, що оглядаються, можуть бути роздруковані та в письмовому вигляді додані до протоколу огляду. Якщо електронний документ містить фото-, відео-, аудіо матеріали, відповідні частини електронного документа можуть бути збережені та записані на фізичний носій інформації, який також стає невід`ємною частиною протоколу огляду електронного документа…» [7].

У вказаній постанові Касаційний кримінальний суд формулює одну з ключових позицій щодо обігу електронних документів і даних з мережі Інтернет у кримінальному провадженні. Суть правової позиції полягає у визнанні легітимності електронного документа без доступу до фізичного носія та допустимості паперової фіксації або перенесення цифрових даних на фізичний носій як способу їх документування в межах процесуального огляду.

Суд також визнає, що інформація, яка перебуває у вільному доступі, не потребує звернення із клопотанням про тимчасовий доступ до речей і документів, що відповідає принципам процесуальної економії та

обґрунтованої мінімізації формалізму. Вказана постанова чітко фіксує допустимі способи документування цифрових джерел, зокрема, шляхом оформлення протоколу огляду електронного документа з додатками (роздруківками веб-сторінок, тощо) та перенесення виявленого мультимедійного контенту (фото, відео, аудіо) на фізичний носій.

Тож, на підставі дослідження наведеної судової практики варто стверджувати про важливість саме належної процесуальної фіксації електронних доказів, що мають доказове значення у кримінальних провадженнях, оскільки порядок такого закріплення не висвітлено в нормативно-правових актах України належним чином.

Зокрема, відповідно до ч. 1 ст. 103 КПК України, процесуальні дії під час кримінального провадження можуть фіксуватися у протоколі, на носії інформації або у журналі судового засідання, однак чітких приписів щодо особливостей фіксації саме електронних доказів, отриманих із відкритих цифрових джерел КПК України не містить [1].

У зв'язку з цим виникає потреба у вивченні міжнародних стандартів, зокрема положень Протоколу Берклі (The Berkeley Protocol on Digital Open Source Investigations), який встановлює вимоги до процесів збирання, перевірки, аналізу та збереження цифрової інформації, отриманої з відкритих джерел - інтернет-ресурсів, соціальних мереж, хмарних сервісів, месенджерів та інших цифрових платформ.

Протокол Берклі має рекомендаційний характер та був підготовлений Центром з прав людини при Каліфорнійському університеті в Берклі спільно з Офісом Верховного комісара ООН з прав людини. Його поява стала відповіддю на виклик часу - стрімку цифровізацію суспільних процесів, зокрема у сфері фіксації масових порушень прав людини, воєнних злочинів, злочинів проти людяності, а також загалом у контексті збирання доказів у міжнародних та національних кримінальних провадженнях.

Відповідно до принципів, викладених у Протоколі, використання цифрових джерел у слідчій та правозастосовній діяльності повинно передбачати чітко структурований, багатоетапний процес, що охоплює низку ключових стадій: онлайн-запити, слідчий аналіз, попередню оцінку, перевірку, збір та збереження.

Першим етапом фіксації електронних доказів є онлайн-запити, що реалізовуються у формі активного пошуку (англ. active search) або пасивного моніторингу (passive monitoring) цифрового контенту [12]. Активний пошук включає перегляд вебресурсів, архівів, відеохостингів тощо, з метою виявлення та фіксації потенційно релевантної інформації. Моніторинг же передбачає відслідковування динамічно змінюваного контенту в часі, зокрема, наприклад, соціальних мереж конкретних осіб чи новинних стрічок. На даному етапі необхідно ретельно документувати усі дії слідчого чи спеціаліста, що включають фіксацію кожного кроку виявлення відповідного матеріалу, включаючи операторів та пошукові системи, які використовувались. Такий підхід дозволяє забезпечувати прозорість методології дослідження та створює можливість перевірки ланцюга пошуку у ході подальшого судового розгляду.

Другий етап передбачає проведення аналітичної обробки зібраної інформації. Слідчий аналіз охоплює порівняння цифрових даних, перевірку їх внутрішньої логіки, ідентифікацію зображень і відео, визначення ймовірних осіб, залучених до подій та мережеву аналітику (у тому числі аналіз взаємодії в соціальних мережах), що дозволяє встановити прогалини для подальшого дослідження.

Наступним етапом є попередня оцінка інформації з урахуванням її потенційної релевантності (prima facie), надійності, можливості вилучення з відкритого доступу та рівня безпеки її зберігання. В подальшому вже відбувається етап повної перевірки достовірності виявлених даних, що включає багаторівневий аналіз: оцінюється джерело походження

інформації, здійснюється порівняння даних з іншими незалежними джерелами, досліджується зміст на наявність змін, маніпуляцій, фальсифікацій, втручання у метадані або структуру файлу. Визначаються унікальні характеристики відео, зображень, аудіозаписів чи текстових документів, перевіряється геолокація та хронолокація (тобто відповідність місця і часу події), здійснюється аналіз змістовної та внутрішньої логічної узгодженості. Додатково досліджується, чи може інформація бути об'єктивно підтверджена альтернативними способами.

Збір цифрових доказів є технічно важливим процесом, який вимагає точності та дотримання передбачених процедур автентифікації. Залежно від характеру інформації, може застосовуватись знімок екрана, конвертація у PDF, експертне завантаження за допомогою спеціалізованих програм або інших засобів фіксації. Якщо матеріал передбачається використовувати як доказ у судовому провадженні, метод збору має бути обґрунтованим, відтворюваним та захищеним від можливих спроб його зміни. У процесі збору особливо важливо зафіксувати наступні відомості:

– точну веб-адресу/ідентифікатор (URL або URI) цифрового об'єкта;

– HTML-код сторінки, який містить технічну інформацію про вміст і структуру веб-ресурсу;

– знімок екрана цільової веб-сторінки із зазначенням дати та часу (скріншот);

– мультимедійні елементи (зображення, відео, аудіо), вбудовані на сторінці;

– вбудовані метадані (ідентифікатор користувача, дата й час завантаження, геотеги, хештеги, анотації тощо);

– контекстуальні дані, які дозволяють зрозуміти обставини створення чи публікації інформації;

– технічні дані збору (ім'я того, хто зібрав виявлену інформацію, IP-адресу пристрою, яка використовувалася під час пошуку, точний час, тощо);

– хеш-значення - криптографічний контрольний код, який підтверджує цілісність об'єкта та неможливість його зміни після збору [12].

Окрема увага приділяється збереженню цифрових доказів, оскільки саме правильне збереження повинно забезпечити незмінність, доступність, цілісність, зрозумілість і придатність об'єкта до використання у правовому контексті. З цією метою рекомендовано створювати хронологічну документацію, що фіксує кожен етап збереження, а також резервні копії цифрових об'єктів, які містять усю супровідну метаінформацію. Крім того, Протоколом передбачено складання технічного звіту, в якому фіксується наведена інформація, що дозволяє не лише засвідчити автентичність об'єкта, але й створити так званий «ланцюг збереження» (chain of custody), що є критично важливим для подальшого використання матеріалу як доказу в судовому провадженні. Усі зміни до цифрового носія, включаючи копіювання, мають бути обґрунтовані та зафіксовані в протоколі, оскільки збереження цілісності цифрового доказу є головноюумовою його допустимості [12].

Протокол Берклі формує всебічну, міжнародно визнану методологію роботи з відкритими цифровими джерелами, поєднуючи технічні та юридичні компоненти щодо виявлення, збирання, перевірки достовірності та збереження цифрової інформації, отриманої з відкритих джерел, з урахуванням принципів належного процесу, дотримання прав людини та забезпечення безпеки даних. Висвітлені положення Протоколу дозволяють створити передумови для визнання цифрової інформації доказом у суді, навіть у випадках, коли вона отримана з нестандартних або нетрадиційних вебресурсів, зокрема соціальних мереж, хмарних сервісів чи інтерактивних платформ.

Водночас чинне процесуальне законодавство України, зокрема ст. 104 КПК України, яка встановлює вимоги до протоколу, в якому фіксуються хід і результати проведення процесуальної дії, містить виключно загальні положення, серед яких вимога зазначати послідовності проведених дій та відображення відомостей, отриманих у результаті їх здійснення [1]. Аналогічно й ст. 237 КПК України, щодо проведення огляду комп'ютерних даних не містить конкретизованих методів роботи з цифровими ресурсами чи критеріїв належної фіксації електронних даних, що призводить до ситуації, коли якість документування цифрових доказів значною мірою залежить від індивідуальної компетентності слідчого або спеціаліста, а не від чітко врегульованих стандартів.

Саме тому, імплементація положень Протоколу у національну кримінальну процесуальну систему України має важливе значення у світлі актуальних викликів, зокрема у зв'язку з воєнними злочинами, фіксацією злочинів проти людяності, гібридної агресії, розслідувань пов'язаних із колабораційною діяльністю, дезінформацією або протидією кіберзлочинності.

В умовах відсутності розгорнутого процесуального регулювання щодо поводження з електронними доказами в КПК України, постає нагальна потреба у розробці відповідного спеціального підзаконного нормативного акта, що передбачатиме стандартизовану процедуру документування, збереження, передачі та перевірки цифрових доказів із урахуванням міжнародних стандартів.

Висновки та перспективи подальших досліджень. На підставі проведеного аналізу встановлено, що чинне кримінальне процесуальне законодавство України, зокрема КПК України, не містить нормативно закріпленого поняття «електронний доказ», що створює умови для неоднозначного тлумачення, що, у свою чергу, призводить до ускладнень у правозастосовній практиці. У зв'язку з цим виникає об'єктивна

необхідність внесення змін до КПК України, шляхом доповнення його окремою статтею, яка б визначала поняття електронного доказу, особливості його процесуального оформлення, допустимості та використання у кримінальному провадженні.

Зокрема, пропонується законодавчо визначити, що електронний доказ - це фактичні дані в електронній (цифровій) формі, які містять відомості, отримані за допомогою електронних пристроїв або технологій, і можуть бути використані для встановлення обставин, що мають значення для кримінального провадження.

До форм електронних доказів доцільно віднести: електронні файли (у тому числі фото-, відео-, аудіофайли); електронне листування; комп'ютерні дані; метадані; інформацію з цифрових платформ, вебсайтів, соціальних мереж, хмарних середовищ, месенджерів тощо.

Необхідно також передбачити, що електронний доказ може зберігатися на будь-якому електронному носії, а кожна ідентична за змістом копія вважається оригіналом. При цьому автентичність електронного доказу має підтверджуватись за допомогою технічних засобів, зокрема: хеш-функцій (контрольних сум), електронного цифрового підпису, експертного дослідження або іншого передбаченого законом способу.

Попри наявність окремих правових підходів до електронних доказів у судовій практиці, відсутність належного нормативного регулювання їх збирання, оцінки та використання зумовлює серйозну правову невизначеність. У зв'язку з цим доцільним є доповнення глави 20 КПК України спеціальною статтею, що регламентуватиме окремий порядок огляду електронних доказів із урахуванням сучасних міжнародних стандартів, зокрема Конвенції про кіберзлочинність та Протоколу Берклі (The Berkeley Protocol on Digital Open Source Investigations).

Також нагальною є розробка та законодавче закріплення механізму роботи з доказами, що походять з мережі Інтернет та відкритих цифрових

джерел. Саме тому, пропонується передбачити можливість використання як джерел доказування: скріншотів вебсторінок і цифрових платформ, архівних копій сайтів, повідомлень і даних з месенджерів (Telegram, Viber), соціальних мереж, відеоплатформ (YouTube) тощо - за умови їх належної процесуальної фіксації.

Окремо слід передбачити рівні процесуальні можливості як для сторони обвинувачення, так і для сторони захисту у збиранні, поданні та використанні електронних доказів. Зокрема, забезпечити: право сторони захисту на самостійне збирання електронних доказів, можливість фіксації інформації з використанням технічних засобів, звернення до провайдерів, адміністраторів цифрових сервісів, залучення фахівців у сфері інформаційних технологій для підтвердження автентичності таких доказів.

Нарешті, ключовим завданням є розробка уніфікованої методики роботи з електронними доказами, яка включатиме: процедуру пошуку, виявлення, документування, вилучення, зберігання та перевірки цифрових даних; шаблони процесуальних документів (протоколів огляду, фіксації хеш-сум, тощо); порядок огляду веб-сторінок; алгоритми автентифікації цифрових матеріалів; стандарти дій для слідчих, прокурорів та адвокатів.

Усі вищезазначені пропозиції спрямовані на усунення правової невизначеності, що наразі існує у сфері використання електронних доказів. Їх імплементація дозволить підвищити ефективність кримінального провадження, мінімізувати процесуальні зловживання та гарантувати дотримання стандартів справедливого судового розгляду.

Література

1. Кримінальний процесуальний кодекс України № 4651-VI від 13.04.2012. URL: https://zakon.rada.gov.ua/laws/show/4651-17/conv (дата звернення 23.07.2025).

2. Про електронні документи та електронний документообіг: Закон України № 851-IV від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення 23.07.2025).

3. Про електронні комунікації: Закон України № 1089-IX від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення 23.07.2025).

4. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#top (дата звернення 23.07.2025)

5. ДСТУ 7157:2010. Основні види та вихідні відомості. 2010 рік. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTY1/dsty_7157-2010.pdf (дата звернення 23.07.2025).

6. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU _ISO_IEC_27037-2017.pdf (дата звернення 23.07.2025).

7. Постанова Касаційного кримінального суду від 06.12.2021 по справі № 756/4855/17. URL: https://reyestr.court.gov.ua/Review/100919101 (дата звернення 22.07.2025)

8. Постанова Касаційного кримінального суду від 19.09.2023 по справі № 756/8251/19. URL: https://reyestr.court.gov.ua/Review/113651233 (дата звернення 22.07.2025)

9. Постанова Касаційного кримінального суду від 04.10.2023 по справі № 159/1506/20. URL: https://reyestr.court.gov.ua/Review/114052575 (дата звернення 22.07.2025)

10. Постанова Касаційного кримінального суду від 12.06.2024 по справі № 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340 (дата звернення 22.07.2025)

11. Постанова Касаційного кримінального суду від 23.01.2025 по справі № 638/6886/22. URL: https://reyestr.court.gov.ua/Review/124718072 (дата звернення 22.07.2025)

12. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних, у перекладі виконаному Зюзь О.В. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення 22.07.2025).

13. Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС.* 2023. № 3 (102). URL:https://www.researchgate.net/publication/376181942_Electronic_evidence_in_criminal_proceedings_problematic_issues_of_theory_and_practice (дата звернення 24.07.2025).

14. Поліщук А., Киливник К. Використання електронних доказів: іноземна практика. *Юридична газета.* № 50 (704). URL: https://yur-gazeta.com/publications/practice/sudova-praktika/vikoristannya-elektronnih-dokaziv-inozemna-praktika.html (дата звернення 24.07.2025).

15. Гарасимів О.І., Марко С.І., Ряшко О.В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету. Серія: Право.* Вип. 75 (2023): частина 2. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/276174/271037 (дата звернення 24.07.2025).

16. Мілімко Л.В., Жидовцев Я.В. Електронні докази в кримінальному судочинстві України. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Вип. 88: частина 3. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/330827/320168 (дата звернення 24.07.2025).

17. Смаль І. А. Проблемні аспекти застосування електронних доказів у кримінальному судочинстві. *Періодичні наукові видання НАВС. Право і суспільство.* 2021. № 4. URL:

https://elar.navs.edu.ua/server/api/core/bitstreams/2810abbd-a0ef-4976-b897-ec3170a1afc6/content (дата звернення 24.07.2025).

18. Тагієв С. Р. Проблемні питання правового регулювання використання електронних доказів у кримінальному процесі. *Академічні візії.* 2025. (41). URL: https://academy-vision.org/index.php/av/article/view/1742 (дата звернення 24.07.2025).

References

1. Criminal Procedure Code of Ukraine № 4651-VI of April 13, 2012. URL: https://zakon.rada.gov.ua/laws/show/4651-17/conv (accessed: 23.07.2025).

2. Law of Ukraine «On Electronic Documents and Electronic Document Flow» № 851-IV of May 22, 2003. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (accessed: 23.07.2025).

3. Law of Ukraine «On Electronic Communications» № 1089-IX of 16 December 2020. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (accessed: 23.07.2025).

4. Convention on Cybercrime of November 23, 2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#top (accessed: 23.07.2025).

5. DSTU 7157:2010. Main Types and Output Data. 2010. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTY1/dsty_7157-2010.pdf (accessed: 23.07.2025).

6. DSTU ISO/IEC 27037:2017. Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL /DSTU5/DSTU_ISO_IEC_27037-2017.pdf (accessed: 23.07.2025).

7. Ruling of the Cassation Criminal Court of December 6, 2021, in case № 756/4855/17. URL: https://reyestr.court.gov.ua/Review/100919101 (accessed: 22.07.2025).

8. Ruling of the Cassation Criminal Court of September 19, 2023, in case № 756/8251/19. URL: https://reyestr.court.gov.ua/Review/113651233 (accessed: 22.07.2025).

9. Ruling of the Cassation Criminal Court of October 4, 2023, in case № 159/1506/20. URL: https://reyestr.court.gov.ua/Review/114052575 (accessed: 22.07.2025).

10. Ruling of the Cassation Criminal Court of June 12, 2024, in case № 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340 (accessed: 22.07.2025).

11. Ruling of the Cassation Criminal Court of January 23, 2025, in case № 638/6886/22. URL: https://reyestr.court.gov.ua/Review/124718072 (accessed: 22.07.2025).

12. The Berkeley Protocol on Open Source Investigations (translated by O. V. Zyuz). URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (accessed: 22.07.2025).

13. Fomina, T. H., Rachynskyi, O. O. (2023). Electronic Evidence in Criminal Proceedings: Problematic Issues of Theory and Practice. Bulletin of Kharkiv National University of Internal Affairs, 3(102). URL: https://www.researchgate.net/publication/376181942_Electronic_evidence_in_criminal_proceedings_problematic_issues_of_theory_and_practice (accessed: 24.07.2025).

14. Polishchuk, A., Kilyvnyk, K. Use of Electronic Evidence: Foreign Practice. Yurydychna Hazeta, № 50 (704). URL: https://yur-gazeta.com/publications/practice/sudova-praktika/vikoristannya-elektronnih-dokaziv-inozemna-praktika.html (accessed: 24.07.2025).

15. Harasymiv, O. I., Marko, S. I., Riashko, O. V. (2023). Digital Evidence: Some Problematic Issues Regarding Their Concept and Use in Criminal Proceedings. Scientific Bulletin of Uzhhorod National University. Law Series, Issue 75, Part 2. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/276174/271037 (accessed: 24.07.2025).

16. Milimko, L. V., Zhydovtsev, Ya. V. (2025). Electronic Evidence in Criminal Proceedings in Ukraine. Scientific Bulletin of Uzhhorod National University. Law Series, Issue 88, Part 3. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/330827/320168 (accessed: 24.07.2025).

17. Smal, I. A. (2021). Problematic Aspects of Using Electronic Evidence in Criminal Proceedings. Periodical Scientific Publications of the National Academy of Internal Affairs. Law and Society, № 4. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/2810abbd-a0ef-4976-b897-ec3170a1afc6/content (accessed: 24.07.2025).

18. Tagiyev, S. R. (2025). Problematic Issues of Legal Regulation of Electronic Evidence Use in Criminal Procedure. Academic Visions, (41). URL: https://academy-vision.org/index.php/av/article/view/1742 (accessed: 24.07.2025).