УДК 343.13 **DOI:** https://doi.org/10.32631/v.2023.3.43

Тетяна Григорівна Фоміна,
доктор юридичних наук, професор,
Харківський національний університет внутрішніх справ,
кафедра кримінального процесу та організації
досудового слідства (завідувач);
https://orcid.org/0000-0002-9513-1673,
e-mail: tatianafomina7777@gmail.com;

Олексій Олександрович Рачинський,
Харківський національний університет внутрішніх справ (курсант);
https://orcid.org/0000-0002-2830-2794,
e-mail: alexey.rachinskiy2003@gmail.com

ЕЛЕКТРОННІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: ПРОБЛЕМНІ ПИТАННЯ ТЕОРІЇ ТА ПРАКТИКИ

Узагальнено наукові напрацювання щодо поняття, сутності електронних доказів і надано авторське визначення поняття «електронний (цифровий) доказ» у кримінальному провадженні. Досліджено нормативно-правове регулювання використання електронних (цифрових) доказів у кримінальному провадженні. Проаналізовано слідчо-судову практику, а також практику Верховного Суду щодо визнання допустимості таких доказів у кримінальному провадженні.

Ключові слова: кримінальне провадження, докази, процес доказування, електронний доказ, цифровий доказ, допустимість доказів.

Оригінальна стаття

Постановка проблеми

XXI століття – епоха розвитку інформаційних технологій. Технологічний прогрес пронизує всі сфери нашого життя. Складно уявити побут сучасної людини без використання електронних пристроїв, гаджетів, адже вони стали своєрідним атрибутом сьогодення. Наприклад, популярність мобільного телефону зумовлена його компактністю та функціональністю, яка досягається за рахунок можливості прийому дзвінків, виходу в мережу Інтернет, здійснення фото-, відеозйомки і навіть використання телефону як файлової системи. Через те, що електронні пристрої стали архівом публічних та приватних даних, правоохоронні органи почали використовувати гаджети як можливість отримання інформації. Навіть за умови, коли електронний пристрій не застосовувався злочинцем, дії правопорушника могли потрапити в поле зору камер відеоспостереження або перебування особи на місці події могло бути зафіксовано за допомогою глобальної

системи позиціювання (GPS). Інформація, отримана з електронних пристроїв, може бути використана для побудови слідчих версій, встановлення злочинних зв'язків і навіть для підтвердження факту вчинення злочину.

Варто розуміти, що важлива для кримінального провадження інформація може міститися не лише на фото, відео- та звукозаписах, електронних документах у їх класичному розумінні (файл, створений за допомогою програм Word або Excel), а й у масивах даних, які містять відомості щодо роботи реєстрів, баз даних, телекомунікаційних мереж тощо.

Неабиякого значення інформація, отримана в цифровому вигляді, набуває під час розслідування воєнних злочинів, а також інших видів злочинів, учинених на території України внаслідок збройної агресії з боку російської федерації. Адже під час безперервних бойових дій, тимчасової окупації та анексії українських територій перспектива проведення належного досудового розслідування зводиться до мінімуму або в деяких випадках навіть унеможливлюється. Наприклад, аналіз записів із відеокамер, розташованих в окупованих містах, у поєднанні з інформацією, отриманою під час перегляду вебсторінок, месенджерів, а також соціальних мереж, дає можливість ідентифікувати особу воєнного злочинця або колаборанта. Тому виникає потреба в дослідженні електронних доказів у кримінальному провадженні.

Однак законодавці не встигають за стрімким розвитком сучасності, а серед науковців та правозастосувачів відсутній єдиний підхід щодо розуміння поняття, ознак електронних (цифрових) доказів та їх місця в системі процесуальних джерел доказів у кримінальному провадженні. Внаслідок чого електронні докази й досі не мають юридичного закріплення в національному кримінальному процесуальному законодавстві. Це породжує теоретико-правові проблеми, які слідчо-судова практика не в змозі врегулювати повною мірою.

Стан дослідження проблеми

Дослідженням питання щодо сутності електронних (цифрових) доказів займалися такі вчені, як Г. Авдєєва, Н. Ахтирська, А. Гутник, Д. Киценко, А. Коваленко, О. Костюченко, І. Крицька, В. Мурадов, Ю. Орлов, А. Ратнова, А. Столітній, Д. Цехан, А. Хитра та ін. Беручи до уваги дослідження вказаних науковців, а також враховуючи те, що електронні (цифрові) докази є відносно новим явищем у сучасному правовому полі, необхідно комплексно дослідити їхню правову природу.

Мета і завдання дослідження

Метою статті є отримання нових результатів у вигляді наукових висновків щодо сутності електронних (цифрових) доказів та можливості їх використання в процесі доказування під час кримінального

провадження. Досягнення поставленої мети передбачає вирішення таких *завдань*: 1) узагальнити наукові напрацювання щодо поняття, сутності електронних (цифрових) доказів та надати авторське визначення поняття «електронний (цифровий) доказ» у кримінальному провадженні; 2) дослідити нормативно-правове регулювання використання електронних (цифрових) доказів у кримінальному провадженні; 3) проаналізувати слідчо-судову практику, а також практику Верховного Суду щодо визнання допустимості таких доказів у кримінальному провадженні.

Наукова новизна дослідження

Стаття є роботою, у межах якої комплексно досліджено теоретико-прикладні питання електронних (цифрових) доказів у кримінальному провадженні та висвітлено авторське бачення щодо їх поняття, ознак і місця в системі процесуальних джерел доказів у кримінальному провадженні.

Виклад основного матеріалу

Наукове підґрунтя розуміння електронних доказів у кримінальному провадженні

Останнім часом проблематика щодо визначення сутності електронних доказів активно вивчається науковою спільнотою. Незважаючи на велику кількість інформації та численні обговорення цієї тематики серед учених, питання щодо їх місця у кримінальному провадженні залишається невирішеним. Аналізуючи наукову літературу, стає зрозуміло, що дослідники не мають єдності поглядів навіть у визначенні терміна, адже можна зустріти такі варіанти, як: «електронні докази» [1, с. 194; 2, с. 244], «цифрові докази» [3, с. 371; 4, с. 257], «електронні (цифрові) докази» [5, с. 5], «електронні документи» [6, с. 184], «електронні відображення» [7, с. 19] тощо. У наукових джерелах висловлюється й інша позиція щодо досліджуваної дефініції. Зокрема, А. Коваленко зауважує, що ані назва «цифрові», ані назва «електронні» не є оптимальними з технічної точки зору. Адже зараз існують системи кодування, що не засновані на використанні цифр, та обчислювальні пристрої і сучасні засоби передачі інформації, які не використовують рух електронів (квантові комп'ютери, передача даних за допомогою оптичних сигналів тощо). Також прогнозується, що з розвитком науки з'являться й інші технології, які, по суті, не відповідатимуть розглядуваним термінам [8, с. 49].

Отже, можемо констатувати, що вчені не мають одностайності в питанні визначення назви зазначеної категорії доказів. Ми дотримуємось позиції щодо доцільності використання саме терміна «електронний (цифровий) доказ». Обґрунтовуємо це тим, що «електронний» вказує на вид пристрою, за допомогою якого був створений і збережений

доказ, а «цифровий» – на тип запису інформації на відповідний пристрій. Але необхідно враховувати швидкоплинність технологічного прогресу, адже вже через певний проміжок часу можуть з'явитися як нові види пристроїв, так і нові типи запису інформації.

Не дійшли дослідники єдності і в питанні змістового наповнення досліджуваного терміна. В. Мурадов вважає, що особливість електронних доказів полягає в неможливості їх безпосереднього сприйняття, вони мають бути інтерпретовані певним чином, а також проаналізовані за допомогою спеціальних технічних засобів і програмного забезпечення [9, с. 314]. Тобто науковець наголошує на одній із ключових особливостей електронного (цифрового) доказу – дуальності, яка полягає в нематеріальній формі походження, але необхідності матеріального вираження для безпосереднього сприйняття суб'єктом. У наукових джерелах існують й інші визначення електронних доказів. Так, О. Котляревський та Д. Киценко електронні докази визначають як «сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах» [10, с. 73]. Д. Алєксєєва-Процюк і О. Брисковська вважають, що «електронні докази – це фактичні дані, які 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» [11, с. 250]. Деякі науковці вважають, що електронні докази – це докази у кримінальних провадженнях, які можна отримати в електронній формі [5, с. 8].

Отже, врахувавши дуальну природу електронних (цифрових) доказів, а також необхідність збереження суті доказу у кримінальному провадженні, ми пропонуємо електронні (цифрові) докази визначити як цифрову інформацію, що міститься на електронних носіях та відповідає вимогам ст. 84 Кримінального процесуального кодексу України (далі – КПК України).

Щодо доречності виокремлення електронних (цифрових) доказів у самостійне джерело доказів та їх місця в системі кримінального процесу також існує чимало різних думок. Зокрема, А. Столітній та І. Каланча вважають, що «створення інституту електронних доказів є помилковим, а сам інститут штучним і фактичною підміною електронної форми фіксації доказів. Виокремлення електронних доказів, як самостійного джерела доказів визнають недоречним, з огляду на існуючі у кримінальному процесі України джерела доказів та формат їх процесуального оформлення і рівень розвитку інформаційних технологій. Але не заперечують майбутньої перспективи розширення джерел доказів – електронними, враховуючи стрімкий розвиток інформаційних технологій» [12, с. 184]. А. Ратнова не погоджується із

твердженням про те, що електронний документ є лише способом фіксації інших доказів. Вчена розмежовує електронний документ як спосіб фіксації та як доказ [6, с. 184].

Якщо звертатися до думки А. Коваленка, то він цілком слушно наголошує на тому, що «існує нагальна потреба у формулюванні доктринального та легального визначень поняття електронний доказ у кримінальному процесі та в науковій розробці основних підходів до збирання, дослідження та використання електронних доказів із дальшим закріпленням таких підходів у КПК України» [13, с. 239]. Позиції щодо необхідності виокремлення електронних документів в окреме джерело доказів дотримуються і Ю. Орлов та С. Чернявський і наводять низку аргументів на підтримку своєї позиції [7, с. 15].

З вищезазначеного можемо зрозуміти, що серед підходів науковців до питань визначення місця електронних (цифрових) доказів у системі джерел доказів кримінального процесу відсутня єдність. Проте, безумовно, дослідники вбачають у цьому прогалини, що негативно впливають на якість і результативність кримінального провадження.

Нормативно-правове регулювання використання електронних (цифрових) доказів у кримінальному провадженні

Дослідження порушеного питання є неможливим без проведення аналізу КПК України. Так, поняття доказів закріплено в ч. 1 ст. 84 КПК України. У частині 2 ст. 84 КПК України визначено процесуальні джерела доказів, якими є показання, речові докази, документи, висновки експертів[1]. Отже, аналіз положень КПК України дає можливість зрозуміти, що електронні (цифрові) докази не закріплені серед джерел доказів. Як наслідок, після виявлення доказу із цифровою природою походження перед слідчими та прокурорами постає питання щодо визначення порядку його збирання.

У дослідженні питання електронних (цифрових) доказів важливим є проведення порівняльно-правового аналізу кримінального процесуального законодавства України з іншими процесуальними законодавствами України. Після доповнень, закріплених Законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 3 жовтня 2017 року № 2147VII[2], у цих нормативно-правових актах з'явилось

[1] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 01.08.2023).

[2] Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного

єдине законодавче закріплення поняття електронного доказу та сформульовано його місце в системі доказів (ст. 99 Кодексу адміністративного судочинства України[1], ст. 100 Цивільного процесуального кодексу України[2], ст. 96 Господарського процесуального кодексу України[3]).

Спробою законодавчо врегулювати використання електронних (цифрових) доказів у кримінальному провадженні є Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів від 1 вересня 2020 року № 4004[4]. У пояснювальній записці до цього проєкту 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. Тож доповнення КПК України положеннями, в яких були б визначені поняття і перелік електронних доказів, є послідовним кроком.

Показовим є те, що у Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021, визнається необхідність унормування електронних (цифрових) доказів. Так, для досягнення цілі С.3 Україна посилить спроможності у протидії кіберзлочинності, серед іншого, шляхом: 1) врегулювання на

судочинства України та інших законодавчих актів : Закон України від 03.10.2017 № 2147-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2147-19 (дата звернення: 01.08.2023).

[1] Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2747-15 (дата звернення: 01.08.2023).

[2] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1618-15 (дата звернення: 01.08.2023).

[3] Господарський процесуальний кодекс України : Закон України від 06.11.1991 № 1798-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1798-12 (дата звернення: 01.08.2023).

[4] Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : від 01.09.2020 № 4004 / ініціатори С. А. Мінько, О. С. Бакумов, Г. О. Михайлюк та ін. // БД «Законодавство України» / ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення: 01.08.2023).

законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики із цих питань Сполучених Штатів Америки, держав – членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки; 2) забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів[1].

Вбачаємо доцільним навести позицію Офісу Генерального прокурора щодо інформації з відкритих джерел у процесі доказування. У листі-орієнтуванні «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел» від 28 серпня 2021 року визнається, що для правоохоронних органів інформація з відкритих джерел може стати додатковою доказовою базою, а також надати слідчому чи дізнавачу більш комплексну картину події. Попри це правоохоронцям слід піддавати таку інформацію ретельній перевірці, адже вона може бути неправдивою, неточною і навіть хибною[2].

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)[3].

Базовим вважається стандарт ISO/IEC 27037:2012 «Guide for Collecting, Identifying, and Preserving Electronic Evidence», прийнятий у 2012 році. Важливим є те, що державний стандарт ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови

[1] Стратегія кібербезпеки України «Безпечний простір – запорука успішного розвитку країни» : затв. Указом Президента України від 26.08.2021 № 447/2021 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 01.08.2023).

[2] Лист-орієнтування Офісу Генерального прокурора «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел» : від 28.08.2021 № 18/1-386вих.515окв-21.

[3] List of ISO Standards for Digital Forensics // Digital Forensics Myanmar : сайт. URL: https://www.forensicsmyanmar.com/2020/01/list-of-iso-standards-for-digital.html (дата звернення: 01.08.2023).

для ідентифікації, збирання, здобуття та збереження цифрових доказів», який набув чинності 1 січня 2019 року[1], був укладений шляхом перекладу саме стандарту ISO/IEC 27037:2012. Відповідний стандарт містить настанови для специфічної діяльності з опрацювання потенційних цифрових доказів, які необхідні під час слідства задля дотримання цілісності цифрових доказів.

Показовим у питанні практичної корисності є те, що дотримуючись цього стандарту, як зазначає Г. Савченко, журналісти-розслідувачі інтернет-видання Bellingcat на основі аналізу цифрової інформації (телефонних розмов, відеозаписів, супутникових знімків та ін.) встановили, що до авіакатастрофи з літаком Boeing-777 MH17 причетні конкретні особи. Показовість прикладу полягає не лише у встановленні конкретних осіб, а й у тому, що матеріали, зібрані Bellingcat, цитувалися під час судового процесу щодо катастрофи [14]. Тобто Гаазький окружний суд у Схіпхолі, який розглядав справу щодо авіакатастрофи, визнав доказову базу, зібрану з дотриманням настанов ISO/IEC 27037:2012, такою, яка відповідає вимогам судочинства.

Задля ефективного використання цифрової інформації з відкритого доступу 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 цифрової інформації, враховуючи певні правові принципи.

Практика використання електронних (цифрових) доказів у кримінальному провадженні

Хоча електронні (цифрові) докази і не мають законодавчого закріплення в КПК України, проте перед слідчими, прокурорами все частіше постають питання щодо порядку збирання цих доказів, а перед суддями – щодо їх оцінки. Порядок оцінки електронного доказу та його допустимості розглядається у постановах Касаційного кримінального суду Верховного Суду (далі – ККС ВС). Серед прикладів слід навести такі.

[1] ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Київ, 2018. 31 с.

[2] Berkeley Protocol on Digital Open Source Investigations // Human Rights Center : сайт. URL: https://humanrights.berkeley.edu/programs-projects/tech-human-rights-program/berkeley-protocol-digital-open-source-investigations (дата звернення: 01.08.2023).

У постанові Третьої судової палати Касаційного кримінального суду від 11 березня 2020 року (справа № 149/754/14, провадження № 51-4269км19) з поміж інших вирішувалось питання щодо визнання допустимим доказом копій електронних доказів. За результатами розгляду суддями ККС ВС було визнано копії відеофонограм (фонограм) недопустимими доказами. В обґрунтування своєї позиції колегія суддів посилалася на положення ч. 3 ст. 99 КПК України, де закріплено, що «сторона кримінального провадження зобов'язана надати суду оригінал документа. Оригіналом документа є сам документ, а оригіналом електронного документа його відображення, якому надається таке ж значення, як документу»[1]. З висновку експерта було встановлено, що відеофонограми (фонограми) фіксації негласної (слідчої) розшукової дії, зафіксовані на оптичних дисках, на які посилається сторона обвинувачення, є копіями. Тож суд визнав такі оптичні диски разом з іншими похідними від них доказами, зокрема протоколами негласної слідчої (розшукової) дії аудіо-, відеоконтролю особи, недопустимими.

У постанові колегії суддів Першої палати ККС ВС від 30 вересня 2021 року (справа № 498/582/18, провадження № 51-2926км2) також вирішувалося питання щодо визнання допустимими копій електронних документів. Результатом було визнання «ототожнення електронного доказу як засобу доказування та матеріального носія такого документа – безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія» (п. 31 постанови)[2]. У доведенні своєї позиції суд посилався на статті 93, 98, 99 КПК України.

Постановою Об'єднаної палати ККС ВС від 29 березня 2021 року (справа № 554/5090/16-к, провадження № 51-1878кмо20) розтлумачено порядок оцінки електронного доказу та його допустимості. Зокрема, Об'єднана палата наголосила, що «для виконання завдань кримінального провадження, з огляду на положення Закону України "Про електронні документи та електронний документообіг", допустимість електронного документа як доказу не можна заперечувати виняткова на підставі того, що він має електронну форму (ч. 2 ст. 8).

[1] Постанова Третьої судової палати Касаційного кримінального суду Верховного Суду від 11.03.2020 : справа № 149/754/14, провадження № 51-4269км19 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/88265263 (дата звернення: 01.08.2023).

[2] Постанова колегії суддів Першої палати Касаційного кримінального суду Верховного Суду від 30.09.2021 : справа № 498/582/18, провадження № 51-2926км2 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/100109348 (дата звернення: 01.08.2023).

Відповідно до ст. 7 цього Закону 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. 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»[1].

У дослідженні порушеного питання вбачаємо за послідовне проаналізувати практику Європейського суду з прав людини (далі – ЄСПЛ), яка має бути врахована під час кримінального провадження. Наприклад, у справі «Georgia v. Russia (II)», заява № 38263/08 від 21 січня 2021 року[2], ЄСПЛ врахував цифрову інформацію, отриману з відкритих джерел. Суд посилався на доповідь, опубліковану Американською асоціацією сприяння розвитку науки (AAAS), «Супутникові знімки високої якості та конфлікт у Південній Осетії» від 9 жовтня 2008 року. Судом було враховано, що AAAS є міжнародною недержавною, некомерційною організацією, ціллю якої є сприяння розвитку науки у всьому світі. Аналіз супутникових знімків у вищенаведеній доповіді був врахований Судом як доказ (§ 66, 188, 205).

Проведений аналіз слідчої практики свідчить про те, що серед правозастосувачів неоднозначним є вирішення питання щодо допустимості протоколу огляду комп'ютерних даних. Згідно з чинними положеннями, які містяться в абз. 2 ч. 2 ст. 237 КПК України, відповідний огляд проводиться слідчим або прокурором шляхом фіксації у протоколі огляду інформації, яку вони містять, у вигляді, придатному для сприйняття їх змісту. Такий огляд може бути здійснено за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі[3]. Але враховуючи

[1] Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29.03.2021 : справа № 554/5090/16-к, провадження № 51-1878кмо20 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/96074938 (дата звернення: 01.08.2023).

[2] Case Georgia v. Russia (II) (Application No. 38263/08) : decision of the European Court of Human Rights from 21.01.2021 // HUDOC : сайт. URL: https://hudoc.echr.coe.int/eng?i=001-207757 (дата звернення: 01.08.2023).

[3] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 01.08.2023).

природу інформації, зафіксованої в електронній формі, і навіть сутності комп'ютерних даних, М. Гуцалюк та П. Антонюк визначають таке сприйняття безпосередньо суб'єктом розслідування фізично неможливим. Крім того, під час спроби відтворити певні комп'ютерні дані у протоколі огляду, як передбачено в КПК України, суб'єкт розслідування вже фактично вносить певні зміни в таку інформацію, залишаючи після себе «цифровий слід» (*digital footprint*), тобто незворотньо змінює фактичні дані, зафіксовані в цифровій формі [15, с. 119]. Науковці наголошують на тому, що ані прокурор, ані слідчий не зможуть належним чином відобразити комп'ютерні дані у протоколі огляду. Адже будь-яка цифрова інформація не має матеріального виразу, тому є доступною для сприйняття тільки після її обробки за допомогою відповідних пристроїв та програм. У результаті чого особисте сприйняття цифрової інформації унеможливлюється, а при спробі слідчого, прокуратура відобразити такі дані у протоколі є ризик залишити «цифровий слід».

Також при взаємодії з інформацією, яка має цифрову природу походження, є вірогідність зіштовхнутися з фото-, відео-, аудіозаписами, створеними за допомогою програмних редакторів. Так, у справі № 521/17136/19, яку розглядав Малиновський районний суд м. Одеси, внаслідок доведення судово-фототехнічною експертизою штучності виготовлення фотографій прокурор відмовився від підтримання публічного (державного) обвинувачення[1]. Цей випадок демонструє, що під час використання електронних доказів у кримінальному провадженні перед слідчим та прокурором постає питання, серед іншого, щодо автентичності походження таких доказів [16].

Висновки

Проведене дослідження дає можливість констатувати таке.

1. Сьогодні проблема унормування електронних (цифрових) доказів є актуальною. Аналіз КПК України дає можливість зрозуміти, що електронні (цифрові) докази майже не мають правового регулювання, що негативно впливає на якість і результативність кримінального провадження. Як наслідок, породжується низка законодавчих суперечностей. На відміну від інших процесуальних законодавств (господарського, цивільного та адміністративного), у кримінальному процесуальному законодавстві положення щодо електронних (цифрових) доказів відсутні. Водночас сьогодні на законодавчому рівні простежуються

[1] Ухвала Малиновського районного суду м. Одеси від 12.05.2023 : справа № 521/17136/19, провадження № 1-кп/521/344/23 // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110849148 (дата звернення: 01.08.2023).

позитивні тенденції щодо визнання необхідності унормування електронних (цифрових) доказів у кримінальному процесі.

2. Визначено, що нині серед науковців відсутній єдиний підхід щодо розуміння поняття, ознак і місця електронних доказів у системі джерел доказів у кримінальному провадженні. Запропоновано на законодавчому рівні використовувати термін «електронний (цифровий) доказ». Обґрунтовано це тим, що «електронний» вказує на вид пристрою, за допомогою якого був створений та збережений доказ, а «цифровий» – на тип запису інформації на відповідний пристрій.

3. Аналіз слідчо-судової практики висвітлив неоднозначність у розумінні правозастосувачів питання щодо збирання електронних доказів. Окреслене питання було предметом розгляду суддів ККС ВС (зокрема порядок оцінки електронного доказу та його допустимості розтлумачено в постанові Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к).

4. Врахування міжнародного досвіду щодо збирання електронних (цифрових) доказів дозволяє використовувати Протокол Берклі під час здійснення кримінального провадження в Україні, адже він активно застосовується міжнародною спільнотою та є актуальним в умовах збройної агресії рф проти України. Сьогодні правоохоронні органи внаслідок активних бойових дій, тимчасової окупації обмежені у проведенні належного досудового розслідування. Тож однією з можливостей збору доказової бази та документування воєнних злочинів є отримання інформації з відкритих інтернет-джерел. Міжнародні стандарти ISO у сфері роботи із цифровою інформацією стають серйозним підґрунтям для роботи з електронними (цифровими) доказами. Дотримання настанов і принципів роботи, викладені в зазначених стандартах, дають змогу правоохоронцям збирати цифрову інформацію задля її подальшого використання як доказу в суді.

Список бібліографічних посилань: 1. Ахтирська Н., Костюченко О. Процесуальні та організаційні аспекти збору електронних доказів під час міжнародного співробітництва. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2022. Т. 2, № 72. С. 192–198. DOI: https://doi.org/10.24144/2307-3322.2022.72.64. **2.** Перцова-Тодорова Л. «Електронний доказ» під час обшуку. *Підприємництво, господарство і право.* 2020. № 6. С. 243–247. DOI: https://doi.org/10.32849/2663-5313/2020.6.41. **3.** Авдєєва Г. Цифрові докази у кримінальному провадженні // Omul, Criminologia, Ştiinţa : Conferinţa ştiinţifică internaţională, ediţia a II-a (Chişinău, 24 martie 2023). Chişinău, 2023. Pp. 370–374. **4.** Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція.* 2013. Вип. 5. С. 256–260. **5.** Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / М. В. Гуцалюк,

В. Д. Гавловський, В. Г. Хахановський та ін. ; за заг. ред. О. В. Корнейка. 2-ге вид., допов. Київ : Вид-во НАВС, 2020. 104 с. **6.** Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філософії : 081. Львів, 2021. 220 с. **7.** Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 1 (13). С. 12–24. **8.** Коваленко А. В. Цифрові чи електронні? До питання йменування нової категорії доказів та слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2018. Вип. 4. С. 237–245. **9.** Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право.* 2013. № 3–2. С. 313–315. **10.** Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології та захист інформації.* 1998. № 2. С. 70–79. **11.** Алєксєєва-Процюк Д. О., Бриськовська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права.* 2018. № 2. С. 247–253. **12.** Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності.* 2019. № 146. С. 179–191. DOI: https://doi.org/10.21564/2414-990x.146.171218. **13.** 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 (84). С. 237–245. **14.** Савченко Г. Хто такі Bellingcat і чому про них так багато говорять // BBC News Україна : сайт. 15.03.2021. URL: https://www.bbc.com/ukrainian/news-56379529 (дата звернення: 01.08.2023). **15.** Гуцалюк М. В., Антонюк П. Є. Процесуальна спроможність використання електронної (цифрової) інформації як доказу в кримінальному провадженні. *Інформація і право.* 2022. № 2 (41). С. 116–122. DOI: https://doi.org/10.37750/2616-6798.2022.2(41).270373. **16.** Матвєєв В. Проблеми та виклики, пов'язані зі збором електронних доказів // JustTalk : сайт. 27.07.2023. URL: https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom-elektronnih-dokaziv (дата звернення 01.08.2023).

Надійшла до редколегії 09.08.2023

Прийнята до опублікування 30.08.2023

Fomina T. H., Rachynskyi O. O. Electronic evidence in criminal proceedings: problematic issues of theory and practice

The article summarises the scientific developments regarding the concept and essence of electronic evidence and provides the author's own definition to the concept of "electronic (digital) evidence" in criminal proceedings; examines the regulatory framework for the use of electronic (digital) evidence in criminal proceedings; analyses the investigative and judicial

practice and the practice of the Supreme Court regarding the admissibility of such evidence in criminal proceedings.

It has been admitted that today the problem of regulating electronic (digital) evidence is relevant. The analysis of the Criminal Procedure Code of Ukraine makes it possible to understand that electronic (digital) evidence has almost no legal regulation, which negatively affects the quality and effectiveness of criminal proceedings. As a result, a number of legislative contradictions arise. Unlike other procedural laws (commercial, civil and administrative), criminal procedural legislation does not contain any provisions on electronic (digital) evidence. At the same time, there are positive trends at the legislative level to recognise the need to regulate electronic (digital) evidence in criminal proceedings.

It has been determined that today there is no unified approach among scholars to understanding the concept, features and place of electronic evidence in the system of sources of evidence in criminal proceedings. It is proposed to use the term "electronic (digital) evidence" at the legislative level. This is substantiated by the fact that "electronic" indicates the type of device with which the evidence was created and stored, and "digital" refers to the type of recording the formation on the relevant device.

The analysis of investigative and judicial practice has highlighted the ambiguity in the understanding of law enforcement officers regarding the collection of electronic evidence. This issue was the subject for consideration by the judges of the Criminal Court of Cassation of the Supreme Court (in particular, the procedure for assessing electronic evidence and its admissibility was explained in the decision of the Joint Chamber of the Criminal Court of Cassation of the Supreme Court dated 29 March 2021 in case No. 554/5090/16-к).

Taking into account international experience in collecting electronic (digital) evidence allows the use of the Berkeley Protocol in criminal proceedings in Ukraine, as it is actively used by the international community and is relevant in the context of russia's armed aggression against Ukraine.

Key words: criminal proceedings, evidence, process of proof, electronic evidence, digital evidence, admissibility of evidence.