# Проблеми використання цифрових доказів у кримінальному судочинстві України та США

**Галина Авдєєва * [a], Ельжбета Живуцька-Козловська ** [b]**

* Канд-ка юрид. наук, ст. наук. співробітн., НДІ вивчення проблем злочинності НАПрН України, м. Харків, Україна, ORCID: https://orcid.org/0000-0003-4712-728x, e-mail: gkavdeeva@gmail.com
** Канд-ка юрид. наук, асоц. професорка права, Вармінсько-Мазурський університет, м. Ольштин, Республіка Польща, ORCID: https://orcid.org/0000-0002-6039-5580, e-mail: malerude@poczta.onet.pl

[a] Написання оригінального рукопису, методологія, формальний аналіз, адміністрування проєкту, ресурси.
[b] Методологія, формальний аналіз, ресурси.

DOI: 10.32353/khrife.1.2023.07 УДК [342.98:004.67](477+73)
Надійшло 15.02.2023 / Рецензовано 13.03.2023 / Прийнято до друку 14.03.2023 / Доступно онлайн 31.03.2023

*Розглянуто актуальні проблеми використання цифрових доказів у кримінальному судочинстві України та США й надано пропозиції щодо їх розв'язання, для чого застосовано методи теоретичного аналізу й синтезу, формально-юридичного аналізу, порівняльно-правовий метод, спеціальні методи пізнання. Розмежовано поняття «електронний доказ» і «цифровий доказ». Аналіз 64 рішень українських судів кримінальної юрисдикції та 31 рішення Апеляційного й Верховного Суду США показав, що визнання допустимими та достовірними доказами інформації у цифровій формі спричиняє певні труднощі. Досвід судочинства США може стати в пригоді реформуванню законодавства України й розробленню методичних рекомендацій із використання цифрових доказів. Запропоновано доповнити Кримінальний процесуальний кодекс України нормами, які б містили визначення поняття «цифрові докази» і їх процесуальних носіїв; розмежування понять «електронний доказ» і «цифровий доказ»; докладний порядок вилучення цифрової інформації, її огляду, фіксування і зберігання (із зазначенням переліку обов'язкової інформації щодо цифрових доказів, яку має бути процесуально закріплено); алгоритм оцінювання достовірності цифрового доказу й висновку експерта за певними критеріями. З'ясовано, що швидка зміна технологій із виявлення, вилучення, фіксування й дослідження цифрової інформації*

*спричиняє певні труднощі для слідчих, суддів, прокурорів і співробітників оперативно-розшукових органів України. Поліпшити ефективність використання цифрових доказів у судочинстві рекомендовано шляхом розроблення настанов щодо роботи із ними та відповідного підвищення кваліфікації співробітників правозастосовних органів.*

***Ключові слова:*** *цифрові докази; електронні докази; електронні пристрої; допустимість доказів; джерела доказів; цифрова інформація; кримінальне провадження; фіксація доказів.*

## Постановка наукової проблеми

На початку 1990-х років завдяки розвиткові цифрових і мережевих технологій співробітники правозастосовних органів почали працювати з доказовою інформацією в електронній (цифровій) формі з різноманітних електронних пристроїв і телекомунікаційних мереж, а саме: комп'ютерів, мобільних телефонів, фото- й відеокамер, *GPS*-навігаторів, соціальних мереж, різних інтернет-сайтів та ін. Зокрема, використання даних *GPS* дає змогу встановити факт перебування підозрюваних осіб на місці вчинення злочину, а аналіз електронних листів і текстових повідомлень, цифрових фотознімків, аудіо- й відеозаписів — причетність осіб до протиправної діяльності.

Розвиток інформаційних технологій, виникнення нових галузей їх застосування та поява нових електронних пристроїв збільшили кількість видів цифрової інформації та способів її кодування й перетворення. Для перегляду й дослідження окремих видів інформації недостатньо звичайної комп'ютерної техніки зі стандартним програмним забезпеченням: для цього необхідні спеціальні електронні пристрої та спеціальне програмне забезпечення. Це спричиняє певні труднощі для слідчих, суддів, прокурорів, адвокатів, експертів та ін.

Особливої актуальності проблеми використання цифрових доказів у кримінальному судочинстві набули після відкритого повномасштабного збройного вторгнення військ РФ на територію України, що грубо порушило права громадян України, закріплені в розд. I Конвенції про захист прав людини й основоположних свобод (далі — *Конвенція*) і її протоколах, а саме: право на життя (ст. 2 Конвенції), заборона катувань (ст. 3 Конвенції), заборона рабства (ст. 4 Конвенції), заборона дискримінації (ст. 14 Конвенції), право на власність (ст. 1 Протоколу № 1), право на освіту (ст. 2 Протоколу № 1), право на свободу і особисту недоторканність (ст. 5 Конвенції), право на справедливий суд (ст. 6 Конвенції), заборона покарання без закону (ст. 7 Конвенції) та ін. [1]

Спільними зусиллями правоохоронних органів України та правозахисних організацій світу створено декілька електронних ресурсів для збирання відомостей про воєнні злочини. За даними Генеральної прокуратури України станом на грудень 2022 р. зафіксовано цифрову інформацію щодо приблизно

1 Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) : від 04.11.1950 р.; ратифік. Законом України від 17.07.1997 р. № 475/97-ВР; чинна для України з 11.09.1997 р. (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 02.02.2023).

70 тисяч таких злочинів [2], яка згодом (разом з іншими доказами) дасть змогу не лише довести, що ці злочини було вчинено, а й пов'язати їх із конкретними особами (злочинцями), висунути їм обґрунтовані обвинувачення та притягнути до відповідальності. Однак у слідчих і суддів часто виникають труднощі у збиранні й оцінюванні цифрових доказів через відсутність у законодавстві України їх визначення, порядку фіксування й оцінки. Також суди України іноді не визнають цифрових доказів допустимими, а напрацюваннями у цьому напрямі науковців і юристів ЄС та США найчастіше послуговуються журналісти-розслідувачі. Тобто законодавство України не встигає за стрімким розвитком інформаційних технологій, а прогалини правового регулювання часто доводиться заповнювати судовою практикою.

Дослідження позитивного досвіду використання цифрових доказів у судочинстві США дасть змогу визначити напрями подолання зазначених проблем у судочинстві України.

## Мета статті

Метою дослідження є аналіз співвідношення понять «електронний доказ» і «цифровий доказ», уточнення поняття «цифровий доказ», узагальнення судової практики України та США з метою виокремлення проблем, які виникають під час використання цифрових доказів у кримінальному судочинстві обох країн, порівняння законодавства України та США щодо використання цифрової інформації в судочинстві, визначення шляхів підвищення ефективності використання цифрових доказів у кримінальному судочинстві України. Метою статті авторки також убачають надання пропозицій щодо вдосконалення кримінального процесуального законодавства України в частині досліджуваних проблем.

## Методи дослідження

Для досягнення цілей дослідження проаналізовано 11 ухвал, 9 рішень і 25 постанов Верховного Суду України (далі — *ВС України*), 18 рішень місцевих судів м. Харкова та Харківської області, 17 рішень Харківського апеляційного суду й Апеляційного суду Харківської області, 12 рішень Апеляційного суду США та 19 рішень Верховного Суду США (далі — *ВС США*), розміщених на відповідних офіційних вебсайтах. Окрім того, вивчено результати аналізу судової практики Харківського апеляційного суду щодо використання електронних доказів, здійснено аналіз позицій суддів Касаційного кримінального суду у складі ВС України (далі — *ККС ВС України*) щодо проблеми допустимості цифрових доказів, опрацьовано міжнародний і національний стандарти роботи із цифровими доказами (ISO/IEC 27037:2012 [3] і ДСТУ ISO/IEC 27037:2017 [4]), досліджено

2 Офіс Генерального прокурора / Офіц. сайт. URL: https://gp.gov.ua/ (дата звернення: 08.02.2023).

3 ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (дата звернення: 07.02.2023).

4 ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) : прийнято наказом ДП «УкрНДНЦ» від 06.12.2017 р. № 400. [Чинний від 01.01.2019]. Київ, 2018. 31 с. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (дата звернення: 07.02.2023).

публікації вітчизняних науковців та окремі напрацювання Наукової робочої групи з дослідження цифрових доказів (англ. *Scientific Working Group on Digital Evidence, USA*) щодо ефективного використання цифрової інформації в судочинстві (зокрема, Протокол Берклі з ведення розслідувань із використанням відкритих цифрових даних [5] (далі — *Протокол Берклі*), Настанови для правоохоронних органів та прокурорів щодо використання цифрових доказів у залі суду (далі — *Настанови щодо використання цифрових доказів*) та ін.). Аналізу також піддано норми вітчизняного законодавства (зокрема, Кримінальний процесуальний кодекс України, далі — *КПК*) і Федеральні правила про докази США (англ. *Federal Rules of Evidence* [6], далі — *FRE USA*) щодо використання цифрових доказів у кримінальному судочинстві.

Для дослідження змісту правових норм і понять, що їх містять нормативно-правові акти й рішення судів, наукові публікації закордонних і вітчизняних дослідників, використано методи теоретичного аналізу й синтезу. Окремі питання потребували застосування методу системного аналізу (передусім зі з'ясування проблем оцінки достовірності цифрових доказів в Україні та США й визначення шляхів їх подолання в Україні).

Формально-юридичний аналіз норм законодавства України та США щодо використання електронних (цифрових) доказів у судочинстві дав змогу виявити властиві правовим актам недоліки й надати пропозиції з удосконалення правового регулювання (зокрема щодо підвищення ефективності використання цифрових доказів у кримінальних провадженнях). За допомогою порівняльно-правового методу досліджено досвід використання цифрових доказів у кримінальному провадженні в Україні та США. Розв'язанню завдань дослідження також сприяли спеціальні методи пізнання: формально-логічний (для типізації підстав щодо визнання цифрового доказу недопустимим), функційний (для встановлення залежності ефективності використання цифрових доказів у судочинстві від якості їх фіксування) та ін.

## Аналіз основних досліджень і публікацій

2012 р. прийнято спеціальний міжнародний стандарт *ISO/IEC 27037:2012* [7], який містить настанови щодо роботи із цифровими доказами. Дотримуючи цього стандарту, журналісти-розслідувачі інтернет-видання *Bellingcat* на основі аналізу цифрової інформації (телефонних розмов, відеозаписів, супутникових знімків та ін.) установили, що до авіакатастрофи пасажирського *Boeing-777 MH17* причетні конкретні військові РФ. Національний стандарт України ДСТУ *ISO/IEC 27037:2017* [8] є єдиним в Україні офіційним документом, який стосується цифрових доказів. У ньому викладено

5 Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних / Управлін. Верховн. комісара ООН з прав людини та Центру з прав людини Каліфорн. ун-ту в Берклі, Юрид. шк., 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 11.02.2023).

6 Federal Rules of Evidence (FRE). Dec 1, 2020 / Legal Informational Institute. URL: https://www.law.cornell.edu/rules/fre (дата звернення: 05.02.2023).

7 ISO/IEC 27037:2012. URL: https://www.iso.org/standard/44381.html (дата звернення: 07.02.2023).

8 ДСТУ ISO/IEC 27037:2017. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (дата звернення: 07.02.2023).

настанови щодо ідентифікації, збирання, здобуття та збереження цифрових доказів, однак законодавчого закріплення ці рекомендації поки що не мають.

Офіс Верховного комісара ООН із прав людини та Центр з прав людини Каліфорнійського університету в Берклі 2020 р. представили *«практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права»*, який містить стандарти й методологічні підходи до *«збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах»* [9]. У Протоколі Берклі викладено алгоритми пошуку, накопичення, аналізу та збереження цифрової інформації з відкритих джерел із дотриманням принципів об'єктивності, компетентності, підзвітності, відповідності законодавству, безпеки, точності, незалежності, прозорості, дотримання прав людини та ін. Автори Протоколу Берклі надають рекомендації щодо визначення меж вирішуваного завдання з метою економії часу й убезпечення свідків і потерпілих, а також апаратного і програмного забезпечення.

Окремі питання використання електронних (цифрових) доказів у кримінальному судочинстві досліджували такі вітчизняні науковці: М. Гуцалюк, Ю. Орлов, С. Столітній, В. Хахановський, Д. Цехан, В. Шевчук, В. Шепітько та ін. Співробітники Національного інституту юстиції США (Шон Е. Гудісон, Роберт К. Девіс, Брайан А. Джексон, Гарі С. Кеслер, Мартін Новак та ін.) у своїх публікаціях наводять результати досліджень із виявлення та визначення пріоритетів потреб кримінального правосуддя, пов'язаних зі збиранням, управлінням, аналізом і використанням цифрових доказів. Незважаючи на значну кількість публікацій із проблем використання цифрових доказів у судочинстві, окремі питання потребують подальшого дослідження. Зокрема, невирішеними залишаються проблеми законодавчого закріплення поняття «цифровий доказ», процесуального регламентування їх вилучення, фіксування та зберігання з урахуванням досвіду США.

## Викладення основного матеріалу дослідження

Сучасними завданнями цифрової криміналістики є пошук і аналіз цифрових слідів, аналіз даних (зокрема — метаданих [10]), збирання доказової інформації у цифровому середовищі. Найбільш складними й масштабними є завдання із пошуку у відкритому доступі й аналізу потенційних джерел доказів — величезної кількості загальнодоступних відео- та аудіозаписів, фото- та супутникових знімків, текстів, звітів, публікацій у соціальних мережах. Електронні пристрої є сховищем загальної та особистої інформації, цифрової інформації про різного роду події та явища, дії окремих осіб тощо. Оскільки сучасні мобільні телефони мають широку добірку функцій (здійснення і приймання дзвінків, телефонна книга і диктофон, фото- і відеокамера, створення і редагування текстових файлів та повідомлень, інтернет-пошук і використання хмарних сховищ, електронна пошта і соціальні мережі, месенджери і сервіси спілкування та ін.), вони зберігають цифрові сліди користування цими функціями

9 Протокол Берклі … . С. 6. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 11.02.2023).

10 Метадані — це дані, що характеризують або пояснюють інші дані.

і є своєрідними архівами особистої інформації. 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.

Науковці в галузі кримінально-правових наук одночасно використовують терміни «електронні» та «цифрові» докази, хоча ці терміни не є тотожними. Сьогодні цифрові пристрої цілком витіснили аналогові, а різниця між аналоговою та цифровою інформацією полягає в тому, що аналогова інформація безперервна, а цифрова — дискретна. Слід погодитися з думкою Н. Зозулі про те, що термін «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*», а «*пристрої та машини, які здійснюють обробку та збереження цифрової інформації, слід називати електронними*» [11]. Якщо точніше, то доказами є «*фактичні дані, отримані з належних джерел, а їх матеріальною основою слугує вже не саме джерело, а штучно створений відповідний процесуальний носій. <…> Доказ являє собою єдність фактичних даних та їх процесуальних носіїв*» [12].

Д. М. Цехан під цифровими доказами розуміє «*фактичні дані, представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ*» [13]. Це визначення потребує уточнення. Зокрема, не всі носії здатні зберігати інформацію у цифровій формі (папір і магнітна плівка також є носіями інформації). Також для розшифровування й дослідження деяких видів цифрової інформації потрібні не ЕОМ, а спеціальні електронні прилади зі спеціальним програмним забезпеченням (наприклад, для перегляду записів бортових реєстраторів літальних апаратів). Тому ***цифровими доказами*** *слід вважати фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи.*

На відміну від Цивільного процесуального кодексу України (ст. 100) [14],

11 Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. *Українське право*. 08.05.2018. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva (дата звернення: 02.02.2023).

12 Тертишник В. М. Кримінальний процес України. Загальна частина : підручник. Академічне видання. Київ, 2014. С. 288. URL: https://rd.ua/storage/lessons/434/512%D0%A2%D0%B5%D1%80%D1%82%D0%B8%D1%88%D0%BD%D0%B8%D0%BA%20%D0%92.%20%D0%9C.%20-%20%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%-D1%8C%D0%BD%D0%B8%D0%B8%CC%86%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%20%D0%A3%D0%BA%D1%80%D0%B0%D1%96%CC%88%D0%BD%D0%B8.%20%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%20%D1%87%D0%B0%D1%81%D1%82%D0%B8%D0%BD%D0%B0,%20%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.%20%D0%90%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D1%96%D1%87%D0%BD%D0%B5%20%D0%B2%D0%B8%D0%B4%D0%B0%D0%BD%D0%BD%D1%8F.pdf (дата звернення: 02.02.2023).

13 Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 257. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58 (дата звернення: 02.02.2023).

14 Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 02.02.2023).

Господарського процесуального кодексу України (ст. 96) [15] і Кодексу адміністративного судочинства України (ст. 99) [16], у КПК відсутні положення про електронні (цифрові) докази. Інформація в цифровій формі у КПК належить до документів / електронних документів як процесуальних джерел доказів (ч. 2 ст. 84) [17]. До документів також належать «*матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані)*» (п. 1 ч. 2 ст. 99 КПК) [18] і «*носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії*» (п. 3 ч. 2 ст. 99 КПК) [19]. Оригіналом електронного документа зазначено «*його відображення, якому надається таке ж значення, як документу*» (ч. 3 ст. 99 КПК) [20]. Дублікати документів та копії інформації у цифровій формі, виготовлені «*слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа*» (ч. 4 ст. 99 КПК) [21].

Документами як цифровими доказами є не лише текстові документи, малюнки, фотознімки, аудіо- та відеозаписи, а й комп'ютерні програми та бази даних. Вони різняться не лише за формою та змістом, а й за джерелом походження. Частину документів створює людина, інші виникають у результаті роботи електронних пристроїв і систем та не залежать від дій людини (інформація з навігаційно-моніторингових систем, електронний цифровий підпис, інформація мобільних операторів, мережева технологічна інформація тощо).

У ст. 237 КПК регламентовано огляд комп'ютерних даних, який «*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)*» (абз. 2 ч. 2) [22]. Утім, там бракує обов'язкового переліку інформації для фіксування цифрових доказів.

Останніми роками в судах України все частіше предметом дослідження стають цифрові докази, однак під час розгляду справ у судах різних юрисдикцій у суддів виникають певні труднощі щодо визнання інформації в цифровій формі допустимими й достовірними доказами. Часто адвокати заявляють клопотання про недопустимість цифрового доказу через те, що спочатку з телефона інформацію копіювали на комп'ютер і лише згодом — на оптичний диск, який потім надали до суду як процесуальний носій доказу. Захисники вважають, що така копія не відповідає оригіналу тому, що в разі зміни носіїв інформації змінюється

15 Господарський процесуальний кодекс України від 06.11.1991 р. № 1798-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text (дата звернення: 02.02.2023).
16 Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (дата звернення: 02.02.2023).
17 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 02.02.2023).
18 Там само.
19 Там само.
20 Там само.
21 Там само.
22 Там само.

формат файлу [23]. Це твердження є хибним, оскільки одна з основних ознак інформації в цифровій формі — це ідентичність оригіналові (цілковитий збіг за всіма ознаками, включно з форматом файлу) усіх його копій, зафіксованих на різних носіях. Незважаючи на це, ВС України в ухвалі за справою № 397/2588/13-к підтримав рішення судів першої та апеляційної інстанцій і визнав недопустимим доказом виконаний під час проведення оперативно-розшукових заходів відео- й аудіозапис факту давання хабаря судді у його робочому кабінеті. Суд ухвалив, що записи є копіями і, як наслідок, визнав недопустимими доказами протоколи про здійснення негласних слідчих (розшукових) дій (далі — *НСРД*), додатком до яких є цей цифровий доказ, протокол огляду запису, де слідчий навів текст розмов щодо давання хабаря, висновки трьох судових експертиз, оскільки вони є похідними від цього запису. Обвинуваченого виправдали [24].

У Постанові ВС України від 18.12.2019 р. у справі № 588/1199/16-к суд визнав недопустимими протокол аудіо-, відеоконтролю особи із додатками, протоколом огляду отриманих під час проведення НСРД носіїв інформації та постановою про визнання їх речовими доказами. Підставою такого рішення стало клопотання сторони захисту про невідкриття їй стороною обвинувачення в порядку ст. 290 КПК доручення на проведення НСРД, під час яких здійснено відеозапис. Цього разу службову особу, підозрювану в хабарництві, також виправдали [25].

ВС України у Постанові за справою № 426/12149/17 щодо наркотичних засобів наголосив на тому, що «*відсутність у матеріалах кримінального провадження саме оригіналів технічних носіїв інформації, на які фіксувалась процесуальна дія, за практикою Верховного Суду, є підставою визнавати такі докази (відеофонограми) недопустимими <…> обов'язковість наявності оригіналів відеозаписів, здійснених під час негласних слідчих (розшукових) дій, зокрема контролю за вчиненням злочину, покликана забезпечити можливість експертним шляхом встановити достовірність інформації, відображеної у відеозаписі*» [26].

У справі № 675/1046/18 (ч. 3 ст. 369 Кримінального кодексу України — надання неправомірної вигоди службовій особі [27]) ВС України, навпаки, відмовив стороні захисту в клопотанні про призначення експертизи відео- та звукозапису на предмет монтажу цифрового відеозапису НСРД, а дослідив запис самостійно і не знайшов підстав для призначення експертизи [28].

23 Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. 28.10.2021 / ВСУ. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/ (дата звернення: 03.02.2023).

24 Ухвала ВСУ від 29.05.2018 р. Справа № 397/2588/13-к. Провадження № 51-3650км18 / Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/74475933 (дата звернення: 05.01.2023).

25 Постанова ВСУ від 18.12.2019 р. Справа № 588/1199/16-к. Провадження № 51-3127км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/86505861 (дата звернення: 06.01.2023).

26 Постанова ВСУ від 17.03.2020 р. Справа № 426/12149/17. Провадження № 51-112км20 / ЄДРСР. URL: http://www.reyestr.court.gov.ua/Review/88401663 (дата звернення: 05.01.2023).

27 Кримінальний кодекс України від 05.04.2001 р. № 2341- III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 02.02.2023).

28 Постанова ВСУ від 18.12.2019 р. Справа № 675/1046/18. Провадження № 51-3942км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/86505906 (дата звернення: 05.01.2023).

Розглядаючи справи про хабарництво, ВС України в окремих випадках *«не вбачає жодних перепон у можливості надання до 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, які визнаються судом як оригінал документа»* [29].

У справі про зловживання владою під час розгону акцій протесту поліцією ВС України визнав цифрові відеозаписи подій допустимим доказом навіть без зазначення того, хто їх здійснював і як їх залучено до кримінального провадження. Цей доказ став підґрунтям для обвинувального вироку службовій особі [30].

ВС України також визнав копії цифрових відеозаписів розбійного нападу на ломбард із камер відеоспостереження (на *DVD*-дисках) допустимим доказом, хоча в Постанові не зазначено, у який спосіб слідство отримало копії цих записів. Висновок судової експертизи щодо ідентифікації особи за цим відеозаписом став підставою для обвинувального вироку [31]. В іншій справі щодо грабежу копію відеозапису з камери відеоспостереження (на *DWD-RW*-диску), добровільно видану співробітником ломбарду, суд також визнав допустимим доказом, незважаючи на заперечення сторони захисту. Суд зазначив, що матеріали провадження містять запит на видачу відеозапису, супровідний лист до *DVD*-диска та протокол його огляду, за яким диск визнано речовим доказом (на думку суда — *«у передбачений КПК спосіб»*) [32].

У справі щодо незаконного обігу наркотичних засобів цивільні особи передали слідству зроблений ними відеозапис правопорушення. Слідчий оформив протокол огляду відеозапису, продемонструвавши запис обвинуваченому, його захиснику та понятим. Таке процесуальне оформлення дало суду змогу визнати відеозапис допустимим доказом [33].

В одному з випадків відеозапис із двох камер відеоспостереження суд визнав належним доказом у справі про порушення правил безпеки дорожнього руху, хоча не було встановлено технічних характеристик пристроїв, на які здійснено відеозаписи, їх сертифікації та порядку передання відомостей на сервер [34]. В іншому випадку копію запису камери відеоспостереження й автотехнічну експертизу, проведену на її підставі, суд визнав недопустимими доказами через те, що *«за копією встановити технологічні властивості відеограми за відсутності оригіналу та оригінального пристрою неможливо»* і висновок

29 Див., наприклад: Постанова ВСУ від 15.01.2020 р. Справа № 161/5306/16-к. Провадження № 51-3498км19 / ЄДРСР. URL: http://www.reyestr.court.gov.ua/Review/87053591 (дата звернення: 03.01.2023).

30 Постанова ВСУ від 20.02.2018 р. Справа № 750/4139/15-к. Провадження № 51-36км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72460327 (дата звернення: 04.01.2023).

31 Постанова ВСУ від 27.02.2018 р. Справа № 759/8643/16-к. Провадження № 51-1031км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72642168 (дата звернення: 03.01.2023).

32 Постанова ВСУ від 02.10.2019 р. Справа № 159/2377/17. Провадження № 51-4466км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/84788575 (дата звернення: 03.01.2023).

33 Постанова ВСУ від 15.03.2018 р. Справа № 760/11451/15-к. Провадження № 51-727км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72909394 (дата звернення: 22.12.2022).

34 Ухвала ВСУ від 25.03.2019 р. Справа № 754/2178/18. Провадження № 51-920ск19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/80716282 (дата звернення: 27.12.2022).

експерта «*ґрунтується на неправильних даних, здобутих з копії відеозапису*» [35].

У кримінальному провадженні щодо крадіжки суд визнав копію (на *DVD*-диску) відеозапису події недопустимим доказом через те, що без ухвали слідчого судді слідство отримало її від потерпілої [36]. Не визнав суд допустимим доказом і копію відеозапису крадіжки з камери відеоспостереження через те, що в матеріалах кримінального провадження відсутні запит про витребування цього відеозапису й відомості про особу, яка їх отримала [37]. Недопустимим доказом суд також визнав копію відеозапису з камери відеоспостереження щодо іншої крадіжки через те, що вони не є оригіналами [38].

Тобто за однакових умов донедавна судді ухвалювали протилежні рішення. В одних випадках вони визнавали копії цифрових записів допустимими доказами, в інших — недопустимими (особливо щодо корупційних злочинів). Утім, останнім часом судді намагаються підвищити свій рівень обізнаності щодо технічних характеристик цифрових доказів для уникнення судових помилок. Зокрема, суддя ККС ВС України Надія Стефанів наголошує на тому, що «*судді відповідають за підвищення власних професійних знань стосовно використання електронних доказів. Суддя сам має дбати про те, щоб бути в курсі всіх останніх новин щодо документів і стандартів та застосовувати їх відповідно до чинного процесуального законодавства*» [39].

Останнім часом судді всіх юрисдикцій намагаються дотримуватися у своїй роботі Керівних принципів Комітету Міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних провадженнях [40]. Суди в Україні все частіше відхиляють клопотання сторони захисту щодо невизнання допустимими й достовірними копій цифрових доказів, протоколів їх огляду та висновків судових експертиз під час розгляду справ різних категорій. Судді докладно оцінюють достовірність висновків експерта й досліджують цифрові докази безпосередньо (зокрема, інформацію з мобільних телефонів) [41].

35 Постанова ВСУ від 31.10.2019 р. Справа № 404/700/17. Провадження № 51-4451км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/85390646 (дата звернення: 28.12.2022).

36 Постанова ВСУ від 12.04.2018 р. Справа № 366/1400/15-к. Провадження № 51-1528км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/73438093 (дата звернення: 21.12.2022).

37 Постанова ВСУ від 04.09.2019 р. Справа № 369/3713/18. Провадження № 51-3536км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/84120855 (дата звернення: 22.12.2022).

38 Постанова ВСУ від 15.11.2018 р. Справа № 140/2668/15-к. Провадження № 51-624км17 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/78110946 (дата звернення: 23.12.2022).

39 Стефанів Н. Матеріальний носій — лише спосіб збереження інформації, який має значення тільки тоді, коли Е-документ виступає речовим доказом / Інформагентство «ADVOKAT POST». 02.11.2021. URL: https://advokatpost.com/materialnyj-nosij-lyshe-sposib-zberezhennia-informatsii-iakyj-maie-znachennia-tilky-todi-koly-e-dokument-vystupaie-rechovym-dokazom-suddia-stefaniv/ (дата звернення: 02.02.2023).

40 Керівні принципи Комітету Міністрів Ради Європи CM(2018)169-add1final щодо електронних доказів у цивільних та адміністративних провадженнях : прийнято Ком. Міністр. 30.01.2019 р. на 1335-му засід. заст. міністр. / Мін'юст України. URL: https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi (дата звернення: 12.02.2023).

41 Див., напр.: Вирок Дзержинського райсуду м. Харкова від 21.06.2019 р. Справа № 638/5928/18. Провадження № 1-кп/638/585/19. URL: https://zakononline.com.ua/court-decisions/show/82552131 (дата звернення: 12.02.2023) ; Вирок Вищ. антикорупц. суду від

Судові рішення останніх 2—3 років відрізняються від попередніх більш докладним розглядом і поясненням технічних характеристик цифрових доказів, що надає більше шансів для визнання допустимим доказом копії інформації у цифровій формі. Зокрема, у справі № 677/2040/16-к касаційну скаргу захисника щодо невизнання копій відеозаписів допустимим доказом суд залишив без задоволення та зазначив:

*«Відповідно до ст. 7 Закону України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV, у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважається оригіналом електронного документа.*

*Матеріальний носій — лише спосіб збереження інформації, який має значення, тільки коли електронний документ є речовим доказом. Головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Один і той же електронний документ (відеозапис) може існувати на різних носіях. Всі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення»* [42].

Таке саме рішення містять Постанова ККС ВС України від 25.01.2021 р. у справі № 236/4268/18 [43] та ухвала ККС ВС України від 19.08.2021 р. у справі № 756/8124/19 [44], у яких суд відмовив у задоволенні скарг захисників щодо недопустимості копій цифрової інформації як доказів.

За результатами узагальнення практики суду касаційної інстанції з питань проведення й оцінювання результатів НСРД у кримінальному провадженні з'ясовано, що найчастіше причинами невизнання судом допустимими доказами цифрових аудіо- та відеозаписів, здійснених під час їх проведення, є такі: надання до суду копій цифрової інформації, а не оригіналів; проведення НСРД співробітниками оперативного підрозділу без доручення на те слідчого, прокурора та без ухвали слідчого судді; невідкриття стороні захисту в порядку ст. 290 КПК доручення на проведення НСРД; відсутність процесуального оформлення рішення слідчого або прокурора про залучення до проведення НСРД «іншої особи»; невиконання вимог ч. 4 ст. 271 КПК щодо негайного складання протоколу за результатами проведення контролю за вчиненням злочину в присутності особи, щодо якої проведено НСРД, одразу після відкритого фіксування під час завершальної стадії контролю за

17.02.2022 р. Справа № 991/4996/20. Провадження № 1-кп/991/53/20. URL: http://iplex.com.ua/doc.php?regnum=103409303&red=1000033ab78a5efaf99e232b33e4b495c626d6&d=5#:~:text=%D0%B7%D0%B0%20%D1%87.,%D0%B2%D0%B8%D0%BA%D0%BE%D (дата звернення: 22.02.2022).

42 Постанова ККС ВСУ від 22.10.2020 р. Справа № 677/2040/16-к. Провадження № 51-5738км19. URL: http://iplex.com.ua/doc.php?regnum=92458395&red=1000035e35a331e82f61d9818795df8ecd0762&d=5 (дата звернення: 22.12.2022).

43 Постанова ККС ВСУ від 25.01.2021 р. Справа № 236/4268/18. Провадження № 51-3124км20. URL: http://iplex.com.ua/doc.php?regnum=94905297&red=10000347f1960a9ea9dcf00a1e2414ca33651f&d=5 (дата звернення: 22.12.2022).

44 Ухвала ККС ВСУ від 19.08.2021 р. Справа № 756/8124/19. Провадження № 51-601ск21. URL: http://iplex.com.ua/doc.php?regnum=94874011&red=1000037c6dddd0bd0c253b026e82724e953e47&d=5 (дата звернення: 22.12.2022).

вчиненням злочину з фактичним її затриманням [45].

У законодавстві США питання використання цифрових доказів є менш «зарегульованим». Ще наприкінці XX ст. цифрові докази у США виокремили у групу доказів у зв'язку з особливостями їх створення, зберігання, виявлення, дослідження й оцінки їх допустимості та достовірності. 1995 р. спільними зусиллями правоохоронні органи США, Канади й деяких країн Європи створили міжнародну організацію з комп'ютерних доказів (англ. *International Organization on Computer Evidence, IOCE*) [46], а 1998 р.— Наукову робочу групу з дослідження цифрових доказів (англ. *Scientific Working Group on Digital Evidence*, далі — *SWGDE*) [47], яка об'єднала роботу правоохоронних, академічних і комерційних організацій у галузі цифрової криміналістики з метою розроблення міждисциплінарних посібників і стандартів щодо відновлення, збереження й дослідження цифрових доказів. Група *SWGDE* розробила основні стандарти та принципи роботи з цифровими доказами, що забезпечує належність і допустимість цих доказів у судочинстві. Особливу увагу приділили процесуальному фіксуванню всіх операцій з такими доказами, забезпеченню доступу до них усіх учасників процесу, допущенню до дослідження цифрових доказів лише кваліфікованих *IT*-спеціалістів із метою максимального збереження їх цілісності [48].

До *FRE USA* [49], які прийнято ще 1975 р. та які регулюють роботу з доказами у цивільному і кримінальному процесах у федеральних судах США, неодноразово вносили зміни й доповнення щодо цифрових доказів з урахуванням розроблених науковцями стандартів і методологічних підходів до збирання, збереження й аналізу цифрових доказів [50] та останніх судових рішень, у яких вони фігурували. Зокрема, до Правила 902 [51] *FRE USA* додали п. 13 і 14 щодо процедури визначення справжності певних цифрових доказів (окрім показань свідка) і надання сторонам у справі можливості встановлювати (оскаржувати) достовірність сертифікованих записів, створених за допомогою електронних систем і даних та скопійованих з електронного пристрою або носія. У поясненнях до цих пунктів зауважено, що для оскарження справжності цифрових доказів

45 Узагальнення практики суду касаційної інстанції з питань проведення та оцінювання результатів НСРД у кримінальному провадженні (оновлено). Тренінговий центр прокурорів України. 2021. С. 51. URL: https://ptcu.gp.gov.ua/wp-content/uploads/2021/11/uzagalnennya_praktyky_sudu_po_nsrd_z_qrkodamy_1.pdf (дата звернення: 12.02.2023).

46 International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648 (дата звернення: 02.02.2023).

47 Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/ (дата звернення: 12.02.2023).

48 Kessler G. C. Judges' Awareness, Understanding, and Application of Digital Evidence. *Journal of Digital Forensics, Security and Law*. 2011. Vol. 6. No. 1. Art. 4. Pp. 54—72. DOI: 10.15394/jdfsl.2011.1088 (дата звернення: 12.02.2023).

49 Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre (дата звернення: 05.02.2023).

50 Протокол Берклі … . URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 11.02.2023).

51 Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre (дата звернення: 05.02.2023).

може знадобитися технічна інформація, здобута шляхом залучення судового експерта або спеціаліста в *IT*-сфері. До того ж у Правилі 702 обумовлено, що експертами можна залучати не лише осіб, які мають знання і навички в техніці й науці та певну освіту, а й тих, хто має досвід роботи в певних галузях (лікарів, банкірів, архітекторів, фізиків та ін.) [52]. Водночас показання та висновки експертів мають бути достовірними (відповідати *Daubert standard* [53]) і допустимими згідно з принципами Правила 104(a) [54] *FRE USA*.

Суди США встановлюють автентичність (справжність, достовірність) цифрових доказів згідно з Правилом 901 [55] *FRE USA*. Зокрема, суд перевіряє інформацію про те, що цифрові докази «*були отримані з конкретного комп'ютера або іншого електронного пристрою, чи було зафіксовано повну та точну їх копію і вони залишилися незмінними з моменту їх фіксації*» [56]. Достовірність значного масиву даних у цифровому вигляді часто потребує дослідження повної копії даних електронного пристрою, яку створює спеціально залучений судовий експерт або спеціаліст. Така копія зберігає логічну структуру накопичувача інформації й навіть видалені файли. Це дає змогу надалі провести додаткову або повторну експертизу [57].

Справжність окремого файлу, його частини або групи файлів перевіряють за їхнім хеш-кодом (унікальним кодом для кожного такого об'єкта). Однакові значення хеш-коду для оригіналу файлу (зокрема, з точної копії диску) і файлу, який перевіряють, свідчать про їхню ідентичність [58]. Для порівняння файлів за хеш-кодом залучають судового експерта або *IT*-спеціаліста, а достовірність показань або висновків експерта перевіряють за *Daubert standard* (Правилом 702).

Суд може визначити справжність цифрових доказів також за допомогою показань свідків навіть за відсутності в матеріалах справи або протоколах відповідних даних [59]. Такими свідками, зокрема, можуть бути співробітники правоохоронних органів, які вилучали електронні пристрої або фіксували

52 Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre (дата звернення: 05.02.2023).

53 *Daubert standard* сформовано на основі трьох судових справ — Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U. S. 579 (1993). URL: https://supreme.justia.com/cases/federal/us/509/579/ (дата звернення: 07.01.2023); General Electric Co. v. Joiner, 522 U. S. 136 (1997). URL: https://supreme.justia.com/cases/federal/us/522/136/ (дата звернення: 07.01.2023) та Kumho Tire Co. v. Carmichael, 526 U. S. 137 (1999). URL: https://supreme.justia.com/cases/federal/us/526/137/ (дата звернення: 07.01.2023) — і призначено для встановлення достовірності показань і висновків експерта.

54 Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre (дата звернення: 05.02.2023).

55 Ibid.

56 United States v. Budziak, 697 F.3d 1105 (2012) / Caselaw Access Project. URL: https://cite.case.law/f3d/697/1105/ (дата звернення: 07.01.2023).

57 United States v. Burdulis, 753 F.3d 255 (1st Cir. 2014). URL: https://casetext.com/case/united-states-v-burdulis (дата звернення: 05.01.2023).

58 United States v. R. Burke. 633 F.3d 984 (10th Cir. 2011). URL: https://casetext.com/case/united-states-v-r-burke (дата звернення: 03.01.2023).

59 United States v. Bush. 727 F.3d 1308 (11th Cir. 2013). URL: https://casetext.com/case/united-states-v-bush-30 (дата звернення: 02.01.2023).

(копіювали) інформацію в цифровій формі [60].

Науковці Національного інституту юстиції США наголошують на важливості докладного протоколювання процесів автентифікації (визначення справжності) і всіх інших дій із цифровими доказами (вилучення з докладним описом електронного пристрою, зазначенням його власника й осіб, які мали до нього доступ, способів і засобів вилучення інформації, копіювання на зовнішній носій, дослідження з описом задіяних методів і засобів тощо). Це дає змогу довести факт зберігання інформації в первісному вигляді [61]. Сторона обвинувачення також зобов'язана своєчасно відкрити стороні захисту цифрові докази, інакше суд поверне матеріали на дослідування.

З метою запобігання помилкам під час роботи з цифровими доказами поліцейські академії США розширили навчальну програму з цифрових доказів на підставі настанов щодо роботи з такими доказами [62]. Автори настанов наголошують на тому, що цифрові докази марні без визначення їхньої достовірності й докладного фіксування «ланцюжка зберігання доказів», тому вони розробили алгоритм протоколювання дій із цифровими доказами та навели перелік питань, які потрібно зазначити в протоколах [63].

Окрему увагу автори настанов приділяють таким питанням:

- необхідності підвищення кваліфікації слідчих і прокурорів щодо технічних аспектів цифрових доказів; [64]
- порадам щодо перевірки справжності електронних листів; [65]
- процесуальному значенню роздруківок інформації з комп'ютера, поясненню понять «оригінал», «копія» і «дублікат» цифрової інформації; [66]
- порядку визначення справжності цифрових фотознімків та ін. [67]

До 2014 р. співробітники правоохоронних органів США під час арешту осіб вилучали в них мобільні телефони й досліджували вміщену там інформацію. Утім, ВС США постановив, що обшук і вилучення цифрової інформації з телефона без відповідного ордера протирічить Конституції США й порушує права громадян [68]. Додатково ситуацію з отриманням інформації з мобільних телефонів ускладнили відмови

60 Goodison S. E., Davis R. C., Jackson B. A. Digital Evidence and the U. S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. RAND Corporation, 2015. P. 11. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf (дата звернення: 25.12.2022).

61 Ibid. P. 13.

62 Hagy D. W. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U. S. Department of Justice. Office of Justice Programs. National Institute of Justice. Washington, Jan 2007. 81 p. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors (дата звернення: 23.12.2022).

63 Ibid. Pp. 15—17.

64 Ibid. P. 23.

65 Ibid. P. 31.

66 Ibid. P. 33.

67 Ibid. P. 50.

68 Riley v. California, 573 U. S. 373 (2014). URL: https://supreme.justia.com/cases/federal/us/573/373/ (дата звернення: 23.12.2022).

представників компаній *Apple* та *Google* надавати доступ до інформації про користувачів навіть за офіційними запитами правоохоронних органів. Це спонукає сторони у справі приділяти більше уваги цифровим слідам, залишеним мобільними пристроями в інтернеті. Завданням суб'єктів доказування є ретельне фіксування таких цифрових доказів, аналізування їх повноти, справжності й надійності, а також оцінка допустимості та достовірності.

Дослідники Національного інституту юстиції США шляхом опитування співробітників правозастосовних органів з'ясували, що респонденти стикаються з безліччю проблем під час роботи з цифровими доказами. Зокрема, їм не вистачає знань про технічні характеристики цифрової інформації, правила її вилучення та зберігання. Слідчі потребують комплектів науково-технічних засобів для роботи з цифровими доказами, зокрема сумок Фарадея для ізолювання електронних пристроїв. На тлі швидкого розвитку технологій цифрових пристроїв і способів вилучення з них цифрової інформації виникають значні труднощі з оцінкою цифрового доказу за критерієм достовірності (його відповідності *Daubert standard*) [69]. Дослідники стверджують, що прокурори (через недостатню обізнаність із технічними характеристиками цифрових доказів) намагаються вилучити більше інформації, аніж це необхідно, і перевантажують судових експертів непотрібною роботою, а деяким суддям бракує знань про методи оброблення та вилучення цифрових доказів. Поліцейські й детективи часто не знають, як фіксувати та зберігати цифрові докази, а судові експерти потребують сучасних методик їх дослідження. Ці проблеми запропоновано розв'язати розробленням настанов для роботи з цифровими доказами (для кожного відомства — окремо) і підвищенням кваліфікації всіх співробітників правозастосовних органів, які у своїй роботі стикаються з цифровими доказами [70].

Отже, слідчі, судді, прокурори, оперативні співробітники й судові експерти у США під час роботи із цифровими доказами певною мірою стикаються з тими самими проблемами, які виникають у відповідних співробітників усіх рівнів кримінального правосуддя України. Водночас, на відміну від КПК, *FRE USA* містять розгалужену систему поправок, які стосуються порядку вилучення цифрових доказів, їх фіксування, зберігання, автентифікації (перевірки справжності), оцінки допустимості й достовірності тощо. Достовірність цифрових доказів, наукових показань спеціалістів і висновків експертів щодо них у США визначають за *Daubert standard*. Співробітники всіх рівнів кримінального правосуддя США в роботі з цифровими доказами керуються Протоколом Берклі й Настановами щодо використання цифрових доказів.

У КПК відсутнє визначення терміна «цифрові докази», не наведено докладного порядку їх вилучення, огляду, фіксування та зберігання. Це може спричинити помилки в роботі із цифрової інформацією й невизнання її допустимим і достовірним доказом у суді.

Викладене вище свідчить про те, що судочинство США має більше можливостей для ефективного використання цифрових доказів, аніж судочинство України.

69 Goodison S. E., Davis R. C., Jackson B. A. Op. cit. P. 16. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf (дата звернення: 21.12.2022).

70 Ibid. P. 25.

## Висновки

Сьогодні аналогові пристрої цілком поступилися місцем цифровим (тобто безперервна інформація — дискретній). Тому термін «цифровий доказ» є більш точним і краще віддзеркалює сутність інформації в цифровій формі (у формі бінарного коду), а пристрої, засоби й машини, які створюють, передають, обробляють і зберігають цифрову інформацію, слід називати електронними. ***Цифровими доказами*** *слід вважати фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи.*

Слідчі, судді, прокурори, співробітники оперативно-розшукових органів і судові експерти України та США під час роботи із цифровими доказами зазнають певних труднощів через швидкі розвиток і зміну технологій цифрових пристроїв та, як наслідок, — зміну технологій виявлення, вилучення, фіксування й дослідження цифрової інформації.

Суди кримінальної юрисдикції України іноді ухвалюють протилежні рішення щодо визнання цифрової інформації допустимим доказом за тих самих умов. Причини невизнання судом допустимими доказами цифрової інформації: надання суду копії цифрової інформації, а не оригіналу; проведення НСРД та отримання цифрової інформації без доручення на те слідчого, прокурора й без ухвали слідчого судді; невідкриття стороні захисту доручення на проведення НСРД; відсутність процесуального оформлення рішення слідчого або прокурора про залучення до проведення НСРД «іншої особи» та ін.

Судочинство США має більше можливостей для ефективного використання цифрових доказів, аніж судочинство України. Нормативно-правові акти й методична література щодо використання цифрових доказів, якими послуговуються в судочинстві США, є гідним орієнтиром для реформування законодавства України та розроблення методичних рекомендацій із цих питань.

Оскільки від компетенції та правильного рішення співробітників правозастосовних органів (слідчих, суддів, прокурорів, оперативних працівників) залежить, чи відіграватиме окремий цифровий доказ провідну роль у вирішенні конкретної справи, ці співробітники мають знати базові технологічні характеристики цифрових пристроїв і цифрової інформації. Тож слід розробити відповідну методичну й довідкову літературу та додати її до програм підвищення кваліфікації окремо для кожної категорії таких співробітників.

КПК бажано доповнити такими новелами: визначенням поняття «цифрові докази» і їхніх процесуальних носіїв; розмежуванням понять «електронний доказ» і «цифровий доказ»; докладним порядком вилучення цифрової інформації, її огляду, фіксування та зберігання (із зазначенням переліку обов'язкової інформації щодо цифрових доказів, яку слід процесуально закріпити); порядком оцінки допустимості й достовірності цифрового доказу та висновку експерта за певними критеріями.

## Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA

***Galina Avdeeva,***
***Elzbieta Żywucka-Kozlowska***

*Current issues of using digital evidence in criminal justice of Ukraine and the USA have been considered and proposals have been provided for their resolution. For this purpose, methods of theoretical analysis and synthesis, formal legal analysis, comparative legal method, and special methods of cognition*

*have been applied. The concepts of "electronic evidence" and "digital evidence" have been differentiated. Analysis of 64 decisions of Ukrainian courts of criminal jurisdiction and 31 decisions of the US Court of Appeal and the Supreme Court has revealed certain challenges in recognizing information in digital format as admissible and veracious evidence. The experience of the US judiciary can be useful for reforming Ukrainian legislation and the development of methodological guidelines for digital evidence use. It has been proposed to amend the Criminal Procedural Code of Ukraine with regulations that would contain the definition for the digital evidence concept and its procedural media; differentiation of the concepts of "electronic evidence" and "digital evidence"; introduction of a detailed procedure for seizing digital information, its review, recording and storage (with indication of the list of mandatory information on digital evidence which must be procedurally established); an algorithm for assessing veracity of digital evidence and an expert conclusion relying on certain criteria. It has been proved that a rapid change in technologies for detecting, seizing, recording and researching digital information has presented certain challenges for investigators, judges, prosecutors and employees of investigative agencies of Ukraine. It is recommended to improve the efficiency of using digital evidence in court proceedings by developing guidelines for working with such evidence and correspondingly improving qualifications of employees in law enforcement agencies.*

***Keywords:*** *digital evidence; electronic evidence; electronic devices; admissibility of evidence; sources of evidence; digital information; criminal proceedings; recording evidence.*

**Фінансування**
Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному чи некомерційному секторах.

**Відмова від відповідальності**
Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію чи підготовку рукопису.

**Учасники**
Авторки внесли свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової практики, написання та редагування, і беруть на себе відповідальність за її зміст і тлумачення.

**Декларація щодо конфлікту інтересів**
Авторки заявляють, що у них відсутній конфлікт інтересів.

## References

Federal Rules of Evidence (FRE). Dec 1, 2020 / Legal Informational Institute. URL: https://www.law.cornell.edu/rules/fre.

International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648.

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html.

Hagy, D. W. (2007). Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U. S. Department of Justice. Office of Justice Programs. National Institute of Justice. Washington. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors.

Kessler, G. C. (2011). Judges' Awareness, Understanding, and Application of Digital Evidence. Journal of Digital Forensics, Security and Law. Vol. 6. No. 1. Art. 4. DOI: 10.15394/jdfsl.2011.1088.

Protokol Berkli z vedennia rozsliduvan z vykorystanniam vidkrytykh tsyfrovykh danykh (2020) [The Berkeley Protocol on Digital Open Source Investigations]/ Upravlin. Verkhovn. komisara OON z prav liudyny ta Tsentru z prav liudyny Kaliforn. un-tu v Berkli, Yuryd. shk. URL: https://www.law.berkeley.edu/wp-content/

uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf [in Ukrainian].

Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/.

Stefaniv, N. (2021). Materialnyi nosii — lyshe sposib zberezhennia informatsii, yakyi maie znachennia tilky todi, koly E-dokument vystupaie rechovym dokazom [Physical medium is only a way of storing information, which is important only when the E-document acts as physical evidence] / Informahentstvo «ADVOKAT POST». URL: https://advokatpost.com/materialnyj-nosij-lyshe-sposib-zberezhennia-informatsii-iakyj-maie-znachennia-tilky-todi-koly-e-dokument-vystupaie-rechovym-dokazom-suddia-stefaniv/ [in Ukrainian].

Tertyshnyk, V. M. (2014). Kryminalnyi protses Ukrainy. Zahalna chastyna [Criminal Procedure in Ukraine. General Part]: pidruchnyk. Akademichne vydannia. Kyiv. URL: https://rd.ua/storage/lessons/434/512%D0%A2%D0%B5%D1%80%D1%82%D0%B8%D1%88%D0%BD%D0%B8%D0%BA%20%D0%92.%20%D0%9C.%20-%20%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%-D1%8C%D0%BD%D0%B8%D0%B8%CC%86%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%20%D0%A3%D0%BA%D1%80%D0%B0%D1%96%CC%88%D0%BD%D0%B8.%20%D0%97%D0%B0%D0%B3%D0%B0%D0-%BB%D1%8C%D0%BD%D0%B0%20%D1%87%D0%B0%D1%81%D1%82%D0%B8%D0%BD%D0%B0,%20%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.%20%D0%90%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D1%96%D1%87%D0%BD%D0%B5%20%D0%B2%D0%B8%D0%B4%D0%B0%D0%BD%D0%BD%D1%8F.pdf [in Ukrainian].

Tsekhan, D. M. (2013). Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia [Digital evidence: concepts, characteristics and place in the proof system]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Yurysprudentsiia.* Vyp. 5. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58 [in Ukrainian].

Zozulia, N. (2018). Elektronni chy tsyfrovi dokazy: udoskonalennia zmin do protsesualnoho zakonodavstva [Electronic or digital evidence: improving amendments in procedural legislation]. *Ukrainske pravo.* URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva [in Ukrainian].

Авдєєва, Г., Живуцька-Козловська, Е. (2023). Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. Вип. 1 (30). С. 126—143. DOI: 10.32353/khrife.1.2023.07.