

її недопустимим доказом через те, що задля надання можливості дослідити відеофайл за допомогою комп'ютерної техніки, формат файлу міг бути змінений. Аналогічне рішення викладено і в Постанові Верховного Суду України від 17.03.2020 р. за справою №426/12149/17 щодо наркотичних засобів.

Для підвищення ефективності використання цифрової інформації у розкритті злочинів до КПК України бажано внести зміни і доповнення щодо більш чіткого визначення цифрових доказів, їх копій та носіїв, закріпити порядок оцінки цифрових доказів на предмет їх допустимості та достовірності.

## ===== 2.3. Сутність цифрових доказів і проблеми їх використання у кримінальному провадженні

На початку 1990-х років завдяки розвитку 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 скоєння 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.

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, фіксації та зберігання з урахуванням досвіду США.

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.<sup>1</sup>

Спільними зусиллями правоохоронних органів України та правоохоронних 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 70 тисяч таких злочинів<sup>2</sup>, яка згодом (разом з іншими доказами) дасть змогу не лише довести, що ці злочини було скоєно, 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 фіксації й оцінки. Також суди України іноді не визнають цифрових доказів допустимими, а напрацюваннями у цьому напрямі науковців і юристів ЄС та США

---

<sup>1</sup> 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 доп.). URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text)

<sup>2</sup> Офіс Генерального прокурора / Офіц. сайт. URL: <https://gp.gov.ua/>

найчастіше послуговуються журналісти-розслідувачі. Тобто законодавство України не встигає за стрімким розвитком інформаційних технологій, а прогалини правового регулювання часто доводиться заповнювати судовою практикою.

У 2012 р. прийнято спеціальний міжнародний стандарт ISO / IEC 27037:2012<sup>1</sup>, який містить настанови щодо роботи із цифровими доказами. Дотримуючись 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<sup>2</sup> є єдиним в Україні офіційним документом, який стосується цифрових доказів. У ньому викладено настанови щодо ідентифікації, збирання, здобуття та збереження цифрових доказів, однак законодавчого закріплення ці рекомендації поки що не мають.

Офіс Верховного комісара ООН з 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»*<sup>3</sup>. 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

---

<sup>1</sup> ISO / IEC 27037:2012. URL: <https://www.iso.org/standard/44381.html>

<sup>2</sup> ДСТУ ISO / IEC 27037:2017. URL: [http://online.budstandart.com/ua/catalog/doc-page?id\\_doc=74978](http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978)

<sup>3</sup> Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. С. 6. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>

економії часу й убезпечення свідків і потерпілих, а також апаратного і програмного забезпечення.

Сучасними завданнями цифрової криміналістики є пошук і аналіз цифрових слідів, аналіз даних (зокрема – метаданих<sup>1</sup>), 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 й соціальні мережі, месенджери і сервіси спілкування та ін.), вони зберігають цифрові сліди користування цими функціями 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»*<sup>2</sup>. Якщо точніше,

---

<sup>1</sup> Метадані – це дані, що характеризують або пояснюють інші дані.

<sup>2</sup> 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\\_protseusualnogo\\_zakonodavstva](https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protseusualnogo_zakonodavstva)

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»<sup>1</sup>.

Д. М. Цехан під цифровими доказами розуміє «фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для прийняття людиною»<sup>2</sup>. 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)<sup>3</sup>, Господарського процесуального кодексу України (ст. 96)<sup>4</sup> і Кодексу адміністративного судочинства України (ст. 99)<sup>5</sup>, 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)<sup>6</sup>. До документів також належать «матеріали фотозйомки, звукозапису, відеозапи-

---

<sup>1</sup> Тертишник В. М. Кримінальний процес України. Загальна частина : підручник. Академічне видання. Київ, 2014. С. 288.

<sup>2</sup> 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](http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58)

<sup>3</sup> 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>.

<sup>4</sup> 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>

<sup>5</sup> 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>.

<sup>6</sup> 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>.

су та інші носії інформації (у тому числі комп'ютерні дані)» (п. 1 ч. 2 ст. 99 КПК)<sup>1</sup> і «носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії» (п. 3 ч. 2 ст. 99 КПК)<sup>2</sup>. Оригіналом електронного документа зазначено «його відображення, якому надається таке ж значення, як документу» (ч. 3 ст. 99 КПК)<sup>3</sup>. Дублікати документів та копії інформації у цифровій формі, виготовлені «слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа» (ч. 4 ст. 99 КПК)<sup>4</sup>.

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. Частина документів створює людина, інші виникають внаслідок 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)<sup>5</sup>. Утім, там бракує обов'язкового переліку інформації для фіксації 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

---

<sup>1</sup> 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>.

<sup>2</sup> Там само.

<sup>3</sup> Там само.

<sup>4</sup> Там само.

<sup>5</sup> Там само.

надали до суду як процесуальний носій доказу. Захисники вважають, що така копія не відповідає оригіналу тому, що в разі зміни носіїв інформації змінюється формат файлу<sup>1</sup>. 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<sup>2</sup>.

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 якої здійснено відеозапис. Цього разу службову особу, підозрювану в хабарництві, також виправдали<sup>3</sup>.

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 інфор-*

<sup>1</sup> 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/>.

<sup>2</sup> 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>

<sup>3</sup> Постанова ВСУ від 18.12.2019 р. Справа № 588/1199/16-к. Провадження № 51-3127км19 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/86505861>.

*мації, на які фіксувалась процесуальна дія, за практикою Верховного Суду, є підставою визнавати такі докази (відеофонограми) недопустимими <...> обов'язковістю 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»<sup>1</sup>.*

У справі № 675/1046/18 (ч. 3 ст. 369 Кримінального кодексу України – надання неправомірної вигоди службовій особі<sup>2</sup>) 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<sup>3</sup>.

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»*<sup>4</sup>.

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<sup>5</sup>.

ВС України також визнав копії цифрових відеозаписів розбійного нападу на ломбард із камер відеоспостереження (на DVD-дисках) до-

---

<sup>1</sup> Постанова ВСУ від 17.03.2020 р. Справа № 426/12149/17. Провадження № 51-112км20 / ЄДРСР. URL: <http://www.reyestr.court.gov.ua/Review/88401663>.

<sup>2</sup> 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>.

<sup>3</sup> Постанова ВСУ від 18.12.2019 р. Справа № 675/1046/18. Провадження № 51-3942км19 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/86505906>.

<sup>4</sup> 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>.

<sup>5</sup> Постанова ВСУ від 20.02.2018 р. Справа № 750/4139/15-к. Провадження № 51-36км18 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/72460327>

пустимим 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<sup>1</sup>. В іншій справі щодо грабежу копія відеозапису з камери відеоспостереження (на DVD-RW-диску), добровільно видана 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»*)<sup>2</sup>.

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<sup>3</sup>.

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 сертифікацію та порядок передання відомостей на сервер<sup>4</sup>. В іншому випадку копію запису камери відеоспостереження й автотехнічну експертизу, проведenu 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 експерта *«ґрунтується на неправильних даних, здобутих з копії відеозапису»*<sup>5</sup>.

---

<sup>1</sup> Постанова ВСУ від 27.02.2018 р. Справа № 759/8643/16-к. Провадження № 51-1031км18 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/72642168>.

<sup>2</sup> Постанова ВСУ від 02.10.2019 р. Справа № 159/2377/17. Провадження № 51-4466км18 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/84788575>

<sup>3</sup> Постанова ВСУ від 15.03.2018 р. Справа № 760/11451/15-к. Провадження № 51-727км18 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/72909394>

<sup>4</sup> Ухвала ВС від 25.03.2019 р. Справа № 754/2178/18. Провадження № 51-920ск19 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/80716282>

<sup>5</sup> Постанова ВСУ від 31.10.2019 р. Справа № 404/700/17. Провадження № 51-4451км19 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/85390646>

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<sup>1</sup>. 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<sup>2</sup>. Недопустимим доказом суд також визнав копію відеозапису з камери відеоспостереження щодо іншої крадіжки через те, що вони не є оригіналами<sup>3</sup>.

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 dbати про те, щоб бути в курсі всіх останніх новин щодо документів і стандартів та застосовувати їх відповідно до чинного процесуального законодавства»*<sup>4</sup>.

Останнім часом судді всіх юрисдикцій намагаються дотримуватися у своїй роботі Керівних принципів Комітету Міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних провадженнях<sup>5</sup>. Суди в Україні все частіше відхиляють клопотання

---

<sup>1</sup> Постанова ВСУ від 12.04.2018 р. Справа № 366/1400/15-к. Провадження № 51-1528км18 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/73438093>

<sup>2</sup> Постанова ВСУ від 04.09.2019 р. Справа № 369/3713/18. Провадження № 51-3536км19 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/84120855>

<sup>3</sup> Постанова ВСУ від 15.11.2018 р. Справа № 140/2668/15-к. Провадження № 51-624км17 / ЄДРСР. URL: <http://reyestr.court.gov.ua/Review/78110946>

<sup>4</sup> 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/>

<sup>5</sup> Керівні принципи Комітету Міністрів Ради Європи CM(2018)169-add1final щодо електронних доказів у цивільних та адміністративних провадженнях : прийнято Ком.

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)<sup>1</sup>.

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»<sup>2</sup>.*

Мініст. 30.01.2019 р. на 1335-му засід. заст. мініст. / Мін'юст України. URL: <https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi>

<sup>1</sup> Див., напр.: Вирок Держинського 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>; Вирок Вищого антикорупційного суду від 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>

<sup>2</sup> 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>

Таке саме рішення містить і Постанова ККС ВС від 25.01.2021 р. у справі №236/4268/18<sup>1</sup> та ухвала ККС ВС від 19.08.2021 р. у справі №756/8124/19<sup>2</sup>, 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 скоєнням злочину в присутності особи, щодо якої проведено НСРД, одразу після відкритого фіксування під час завершальної стадії контролю за скоєнням злочину з фактичним її затриманням<sup>3</sup>.

У законодавстві США питання використання цифрових доказів є менш «зарегульованим». Ще наприкінці ХХ 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*

---

<sup>1</sup> 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>

<sup>2</sup> 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=1000037c6dadd0bd0c253b026e82724e953e47&d=5>

<sup>3</sup> 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\\_nsrdd\\_z\\_qrkodamy\\_1.pdf](https://ptcu.gp.gov.ua/wp-content/uploads/2021/11/uzagalnennya_praktyky_sudu_po_nsrdd_z_qrkodamy_1.pdf)

on Computer Evidence, IOCE)<sup>1</sup>, а 1998 р. – Наукову робочу групу з дослідження цифрових доказів (англ. *Scientific Working Group on Digital Evidence*, далі – *SWGDE*)<sup>2</sup>, 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 процесуальній фіксації 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<sup>3</sup>.

До *FRE USA*<sup>4</sup>, 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<sup>5</sup> та останніх судових рішень, у яких вони фігурували. Зокрема, до Правил 902<sup>6</sup> *FRE USA* додали п. 13 і 14 щодо процедури визначення справжності певних цифрових доказів (окрім показань свідка) та 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 може знадобитися

---

<sup>1</sup> International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: <https://uia.org/s/or/en/1100029648>

<sup>2</sup> Scientific Working Group on Digital Evidence (**SWGDE**). URL: <https://www.swgde.org/>

<sup>3</sup> 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.

<sup>4</sup> Federal Rules of Evidence ... URL: <https://www.law.cornell.edu/rules/fre>

<sup>5</sup> Протокол Берклі ... URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>

<sup>6</sup> Federal Rules of Evidence ... URL: <https://www.law.cornell.edu/rules/fre>

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 й навички в техніці та науці і певну освіту, а й тих, хто має досвід роботи в певних галузях (лікарів, банкірів, архітекторів, фізиків та ін.). Водночас показання та висновки експертів мають бути достовірними (відповідати *Daubert standard*<sup>1</sup>) і допустимими згідно з принципами Правила 104(a)<sup>2</sup> *FRE USA*.

Суди США встановлюють автентичність (справжність, достовірність) цифрових доказів згідно з Правилем 901<sup>3</sup> *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»<sup>4</sup>. 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<sup>5</sup>.

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 їх ідентичність<sup>6</sup>. Для порівняння файлів за хеш-кодом залучають

---

<sup>1</sup> *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/>; *General Electric Co. v. Joiner*, 522 U. S. 136 (1997). URL: <https://supreme.justia.com/cases/federal/us/522/136/> та *Kumho Tire Co. v. Carmichael*, 526 U. S. 137 (1999). URL: <https://supreme.justia.com/cases/federal/us/526/137/> – і призначено для встановлення достовірності показань і висновків експерта.

<sup>2</sup> Federal Rules of Evidence ... . URL: <https://www.law.cornell.edu/rules/fre>

<sup>3</sup> Ibid.

<sup>4</sup> *United States v. Budziak*, 697 F.3d 1105 (2012) / Caselaw Access Project. URL: <https://cite.case.law/f3d/697/1105/>

<sup>5</sup> *United States v. Burdulis*, 753 F.3d 255 (1st Cir. 2014). URL: <https://casetext.com/case/united-states-v-burdulis>

<sup>6</sup> *United States v. R. Burke*. 633 F.3d 984 (10th Cir. 2011). URL: <https://casetext.com/case/united-states-v-r-burke>

судового експерта або ІТ-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<sup>1</sup>. Такими свідками, зокрема, можуть бути співробітники правоохоронних органів, які вилучали електронні пристрої або фіксували (копіювали) інформацію в цифровій формі<sup>2</sup>.

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<sup>3</sup>. Сторона обвинувачення також зобов'язана своєчасно відкрити стороні захисту цифрові докази, інакше суд поверне матеріали на дослідження.

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<sup>4</sup>. Автори настанов наголошують на тому, що цифрові докази марні без визначення їх достовірності й докладної фіксації «ланцюжка зберігання доказів», тому вони розробили алгоритм протоколювання дій із цифровими доказами та навели перелік питань, які потрібно зазначити в протоколах<sup>5</sup>.

---

<sup>1</sup> United States v. Bush. 727 F.3d 1308 (11th Cir. 2013). URL: <https://casetext.com/case/united-states-v-bush-30>

<sup>2</sup> 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>

<sup>3</sup> Ibid. P. 13.

<sup>4</sup> 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>

<sup>5</sup> Ibid. Pp. 15–17.

Окрему увагу автори настанов приділяють таким питанням: необхідності підвищення кваліфікації слідчих і прокурорів щодо технічних аспектів цифрових доказів<sup>1</sup>; порадам щодо перевірки справжності електронних листів<sup>2</sup>; процесуальному значенню роздруківок інформації з комп'ютера, поясненню понять «оригінал», «копія» і «дублікат» цифрової інформації<sup>3</sup>; порядку визначення справжності цифрових фотознімків та ін.<sup>4</sup>

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 ордеру протирічить Конституції США й порушує права громадян<sup>5</sup>. Додатково ситуацію з отриманням інформації з мобільних телефонів ускладнили відмови 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 ретельна фіксація 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 достовір-

---

<sup>1</sup> Ibid. P. 23.

<sup>2</sup> Ibid. P. 31.

<sup>3</sup> Ibid. P. 33.

<sup>4</sup> Ibid. P. 50.

<sup>5</sup> *Riley v. California*, 573 U. S. 373 (2014). URL: <https://supreme.justia.com/cases/federal/us/573/373/>

ності (його відповідності *Daubert standard*)<sup>1</sup>. 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 ми пропонуємо 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<sup>2</sup>.

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 фіксації, 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 України відсутнє визначення терміна «цифрові докази», не наведено докладного порядку їх вилучення, огляду, фіксації та зберігання. Це може спричинити помилки в роботі із цифровою 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.

---

<sup>1</sup> Goodison S. E., Davis R. C., Jackson B. A. Op. cit. P. 16. URL: <https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf>

<sup>2</sup> Ibid. P. 25.