Розділ ІІ. ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ ЗАСТОСУВАННЯ ЗАКОНОДАВСТВА

DOI: 10.33766/2786-9156.105.33-48
УДК: 343.98

Авдєєва Г. К., *кандидатка юридичних наук, старша наукова співробітниця, провідна наукова співробітниця НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України (м. Харків, Україна)*
e-mail: gkavdeeva@gmail.com
ORCID iD : https://orcid.org/0000-0003-4712-728x

ПРОБЛЕМИ ВИЗНАЧЕННЯ ДОСТОВІРНОСТІ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

У статті розглянуто види цифрових доказів та їх сутність, проблеми визнання цифрової інформації процесуальними джерелами доказів у кримінальному провадженні. Показані особливості оцінки цифрових доказів за критерієм достовірності, обгрунтована необхідність належної фіксації цифрових доказів на різних стадіях кримінального провадження. Доведено, що метадані цифрових файлів на будь-якому етапі кримінального провадження дозволяють підтвердити їх автентичність та процесуальну значущість.

Дослідження показало, що суди України та США ухвалюють протилежні рішення щодо визнання інформації у цифровому вигляді процесуальними джерелами доказів, а рівень підготовки слідчих щодо програмно-технічних комплексів та складних програмних оболонок є низьким. Це негативно впливає на якість здійснення правосуддя тому, що в умовах глобальної цифровізації суспільства цифрові докази іноді є визначальними для об'єктивного вирішення справи і притягнення винних до відповідальності. Програми підготовки і підвищення кваліфікації співробітників правозастосовних органів запропоновано доповнити базовою підготовкою щодо роботи з цифровими доказами з використанням сучасних напрацювань правоохоронних органів, науковців і журналістів країн Європи та США.

Здійснено аналіз нормативно-правових актів України та США і рекомендацій, прийнятих різними інституціями ЄС та США щодо використання цифрових доказів у кримінальному провадженні та визнання їх процесуальними джерелами доказів. На законодавчому рівні в Україні запропоновано визначити порядок верифікації та критерії достовірності цифрової інформації.

Ключові слова: цифрова інформація, цифровий доказ, автентифікація цифрової інформації, верифікація цифрової інформації, достовірність цифрового доказу, кримінальне провадження.

Постановка проблеми. Сучасні цифрові технології забезпечують фіксацію, накопичення, систематизацію, зберігання і аналіз інформації, яка може слугувати доказами при розслідуванні злочинів. Такою інформацією слугують електронні записи, дані з комп'ютерів, мобільних пристроїв, соціальних мереж, електронної пошти, вебсайтів та ін. електронних джерел, у т.ч. баз даних. Вона

може включати відомості про злочини, комунікацію між підозрюваними, їх місцезнаходження, фінансові транзакції та ін.

На сьогодні в Україні та в інших країнах функціонують декілька платформ для фіксації злочинів, скоєних російськими військовими в Україні. Зокрема, база даних «Книга катів українського народу» [1], інформаційний ресурс Української Гельсінської Спілки з прав людини [2], база даних «T4P (Трибунал для Путіна)» [3], створена Офісом Генерального прокурора України спільно з компанією «IT Defends», національна платформа WarCrimes.gov.ua, аналітична база даних «Воєнні злочинці рф» [4], створена Агентством Європейського Союзу з питань судового співробітництва (Євроюстом), міжнародна централізована база доказів міжнародних злочинів (CICED) [5] та ін. Для захисту та представництва України в Європейському суді з прав людини та Міжнародному суді ООН функціонує міжурядова платформа для збирання та аналізу інформації про порушення прав людини військовими рф. Однак накопичена в базах даних цифрова інформація не завжди може використовуватися в кримінальному провадженні як доказ навіть у випадках, коли в ній зафіксований факт вчинення злочину. За результатами узагальнення більше як 50 постанов і рішень судів різних юрисдикцій України та США встановлено наявність проблем у визнанні інформації у цифровому вигляді джерелами доказів. Навіть за однакових умов судді ухвалюють протилежні рішення. В одних випадках вони визнають копії цифрових записів допустимими доказами, в інших – недопустимими [6, с. 132]. Це негативно впливає на якість здійснення правосуддя тому, що в умовах глобальної цифровізації суспільства цифрові докази іноді є визначальними для об'єктивного вирішення справи і притягнення винних до відповідальності. Через те вкрай важливим є дослідження проблем визнання цифрової інформації джерелами доказів у кримінальних провадженнях та визначення шляхів їх подолання.

Аналіз останніх досліджень і публікацій. Окремі проблемні питання використання цифрової інформації у кримінальному провадженні досліджували такі вітчизняні вчені, як: Н. М. Ахтирська, Н. В. Глинська, І. В. Гловюк, І. О. Крицька, В. В. Луцик, Ю. Ю. Орлов, А. В. Скрипник, А. В. Столітній, Д. М. Цехан, В. Ю. Шепітько, В. М. Шевчук та ін. науковці. У своїх публікаціях вчені 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 автентифікації цифрової інформації та визнання її процесуальними джерелами доказів у кримінальному провадженні.

Формулювання цілей. Метою статті є виокремлення проблемних питань щодо встановлення достовірності цифрових доказів у кримінальному провадженні, визначення шляхів автентифікації цифрової інформації та установлення порядку визнання її процесуальними джерелами доказів, а також формулювання пропозицій щодо подолання зазначених проблем.

Виклад основного матеріалу. Цифровими доказами є фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи [6, с. 131]. Цифрова інформація може слугувати доказами у кримінальному провадженні лише за умови її відповідності критеріям оцінки доказів (допустимість, належність, достовірність і достатність). Допустимість доказу визначається законністю джерела походження та способу отримання. Належність віддзеркалює здатність доказу підтверджувати або спростовувати будь-які обставини, що мають значення для справи. Достатнім є доказ, який віддзеркалює його здатність підтверджувати або спростовувати обставини, що мають значення для справи. Доказ вважається достовірним, якщо він відповідає дійсності [7].

Леонід Лобойко слушно зазначає, що значення терміна «достовірність» у кримінальному процесі та в точних науках відрізняється. У точних науках це – рівна одиниці «ймовірність», а в кримінальному процесі – «так звана «практична достовірність, якою переважна більшість людей, які перебувають у здоровому глузді, задовольняється в найбільш відповідальних ситуаціях повсякденного життя» [8, с. 187].

Важливо зазначити, що оцінка цифрових доказів має свої особливості. В окремих випадках виникають труднощі навіть у віднесенні їх до речових доказів або документів. У Кримінальному процесуальному кодексі України (КПК) відсутні положення про електронні (цифрові) докази, а інформацію в цифровій формі віднесено до документів / електронних документів як процесуальних джерел доказів (ч. 2 ст. 84) [9]. Документами також вважаються матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації, у тому числі комп'ютерні дані (п. 1 ч. 2 ст. 99 КПК) [9], і носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії (п. 3 ч. 2 ст. 99 КПК) [9]. Оригіналом електронного документа зазначено його відображення, якому надається таке ж значення, як документу (ч. 3 ст. 99 КПК) [9]. Дублікати документів та копії інформації в цифровій формі, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа (ч. 4 ст. 99 КПК) [9].

До документів як цифрових доказів відносться не лише текстові документи (електронні листи та повідомлення, електронні документи в застосунку «Дія» та ін.), графічні зображення, 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 внаслідок роботи електронних пристроїв і систем і не залежать від дій людини (інформація з навігаційно-моніторингових систем, електронний цифровий підпис, інформація мобільних операторів, мережева технологічна інформація тощо) [6, с. 132].

Ст. 237 КПК України містить норми щодо огляду комп'ютерних даних, які фіксуються в протоколі огляду у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або в паперовій формі) (абз. 2 ч. 2) [9]. Утім, там відсутній перелік інформації, яка має бути обов'язково зафіксована в протоколі та його

додатках. Неякісна та неповна фіксація цифрової інформації в подальшому може привести до не визнання її доказом у кримінальному провадженні. У КПК України взагалі відсутні норми щодо використання в кримінальному провадженні інформації з «відкритих» джерел мережі Інтернет.

Міжнародна організація Global Rights Compliance (заснована в Гаазі) видало «Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні» [10], у якому міститься інформація про основні правила розслідування, підготовку до документування, роботу з різними видами доказів (фізичними, документальними, цифровими, аудіовізуальними та інформацією з відкритих джерел). У виданні наведено характеристику та докладний порядок фіксації таких видів інформації в цифровому вигляді: фотографічної або відеоінформації, зокрема отриманої під час огляду місця події; інформації, вилученої з електронного пристрою (наприклад, телефону, ноутбука або камери); інформації, виявленої на місці злочину або такій, яка належить померлому потерпілому або ймовірному підозрюваному; інформації, отриманої від третіх осіб (наприклад, свідків) та ін.

Спільними зусиллями провідних наукових установ та правоохоронних органів США, Канади й деяких країн Європи створено міжнародну організацію щодо комп'ютерних доказів (International Organization on Computer Evidence, IOCE) [11] та Наукову робочу групу з їх дослідження (Scientific Working Group on Digital Evidence або SWGDE) [12], які досліджують цифрову інформацію та розробляють міждисциплінарні посібники й стандарти щодо фіксації, відновлення, збереження й дослідження цифрових доказів. Особливу увагу приділено процесуальній фіксації слідчих дій із використанням цифрових доказів, забезпеченню доступу до них усіх учасників процесу в умовах змагального судочинства, допущенню до дослідження цифрових доказів лише кваліфікованих IT-спеціалістів із метою максимального збереження їх цілісності [13].

До Федеральних правил доказування США (FRE USA) [14] неодноразово вносили зміни й доповнення щодо цифрових доказів з урахуванням розроблених науковцями сучасних стандартів і методологічних підходів до збирання, збереження й аналізу цифрових доказів та останніх судових рішень, у яких вони фігурували. Зокрема, до Правила 902 FRE USA додали п. 13 і 14 щодо перевірки справжності цифрових доказів та надання сторонам у справі можливості встановлювати (оскаржувати) достовірність метаданих (сукупність даних про певну інформацію) цифрових файлів. Оскарження справжності цифрових доказів може здійснюватися із залученням судового експерта або спеціаліста в IT-сфері.

У США суди встановлюють автентичність (справжність, достовірність) цифрових доказів відповідно до Правила 901 FRE USA за такою схемою: перевірка факту отримання цифрової інформації з конкретного електронного пристрою, встановлення повної відповідності з оригіналом або з першою процесуально зафіксованою копією, встановлення відсутності змін із моменту їх фіксації [15]. Для перевірки достовірності великого масиву цифрових даних використовується повна копія даних електронного пристрою, яка зберігає логічну структуру накопичувача інформації (включаючи видалені файли) та яку виготовляє

спеціально залучений судовий експерт або спеціаліст. Наявність такої копії (образу диску) дає змогу в подальшому провести судову експертизу, у т.ч. додаткову або повторну [16].

Автентичність (справжність) окремого цифрового 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 отриманої з точної копії накопичувача інформації пристрою, і файлу, який перевіряють, свідчать про їх ідентичність [17]. Для порівняння файлів за хеш-кодом залучають судового експерта або ІТ-спеціаліста, а достовірність показань або висновків експерта перевіряють за Daubert standard (Правило 702 FRE USA).

Суд може визначити достовірність цифрових доказів й за допомогою показань свідків [18]. Такими свідками, зокрема, можуть бути співробітники правоохоронних органів, які вилучали електронні пристрої або фіксували (копіювали) інформацію в цифровій формі [19, с. 11].

Під час оцінювання достовірності цифрової інформації завжди виникають проблеми у встановленні автора (власника, володільця, утримувача) цифрових аудіо- та відеозаписів, які виявлені в інтернет-просторі. Автора, в основному, визначають шляхом пошуку за IP-адресою (унікальною адресою комп'ютера або іншого пристрою, що підключено до мережі Інтернет або локальної мережі) або за допомогою сервіса Whois. У разі знищення правопорушником цифрової інформації з метою приховування протиправних дій судовим експертом здійснюється відновлення знищеного контенту за певним алгоритмом із використанням спеціальних програмних засобів [20, с. 26-43].

Петро Левуліс (Польща) під час узагальнення завершених кримінальних проваджень встановив, що цифрові докази розглядалися в 253 із 370 випадків, навіть у таких, у яких знаряддями злочинів не слугували комп'ютерна техніка і мережі. Лише у 19 провадженнях для дослідження цифрових доказів залучалися судові експерти, в інших випадках суди оцінювали їх самостійно шляхом дослідження роздруківок, наданих до суду сторонами по справі. Підтвердженням автентичності (справжності) роздруківок цифрових доказів слугували засвідчення їх нотаріусом, підписом особи, яка їх надавала до суду, отримання офіційної довідки від працівника поліції, який виконував роздруківку, або показання свідків, які підтверджували їх автентичність. У жодному з 370 випадків правоохоронці не забезпечили фіксацію цифрових доказів безпосередньо шляхом виготовлення перевіреної цифрової копії. Вони зазвичай обмежувались протоколюванням та роздруківками, а вилучені електронні пристрої, як правило, не були описані в протоколах достатньою мірою для того, щоб вони могли бути ідентифіковані в майбутньому (35 із 62 вилучених пристроїв були описані лише із зазначенням марки та кольору пристрою) [21]. Таке узагальнення свідчить про недостатній рівень обізнаності співробітників правозастосовних органів щодо роботи з цифровими доказами.

Науковці Національного інституту юстиції США наголошують на важливості докладного протоколювання процесів автентифікації (встановлення справжності) та всіх інших процесуальних дій із цифровими доказами (вилучення з

детальним описом електронного пристрою, вказівкою його власника та осіб, які мали до нього доступ, способів і засобів вилучення інформації, копіювання на зовнішній носій, дослідження з описом методів і засобів тощо). Це дозволяє довести факт зберігання інформації в первісному вигляді [22, с. 13].

Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини у 2020 р. представлений «Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права» (Протокол Берклі), який містить стандарти і методологічні підходи до збирання, збереження та аналізу інформації у відкритому доступі, яка може слугувати доказом у кримінальному провадженні. [23, с. 6]. У Протоколі Берклі викладені 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. [24, с. 15].

Національний стандарт України ДСТУ ISO/IEC 27037:2017 [25] є єдиним в Україні офіційним документом, який має належність до цифрових доказів. У ньому викладені настанови щодо ідентифікації, збирання, здобуття та збереження цифрових доказів, однак законодавчого закріплення ці рекомендації поки що не мають. Для допомоги в оцінюванні допустимості, належності і достовірності цифрових доказів слідчі і судді зазвичай звертаються до судових експертів, однак навіть останні не завжди здатні вирішити завдання щодо встановлення автентичності матеріалів відео- та звукозапису, яке зазвичай базується на ідентифікації апаратури запису. На цій апаратурі здійснюється експериментальний запис, ознаки якого порівнюються з ознаками аналізованого файлу. За відсутності апаратури запису встановити автентичність запису вкрай складно [26]. Експерти констатують, що через швидкий розвиток інформаційних технологій і зміну форматів цифрових файлів існуючі методики судової компютерно-технічної експертизи швидко «застарівають» і вимагають постійного доопрацювання [27, с. 5]. Вони наголошують на тому, що нині взагалі складно створити конкретну методику автентифікації цифрових відео- та звукозаписів через різноманітність та відсутністість наукових публікацій про їх характеристики. Унаслідок чого можна лише охарактеризувати напрями виявлення певних ознак для вирішення питання щодо автентифікації (верифікації) цифрових записів [28, с. 57-58].

Європейським центром журналістики виданий посібник для верифікації (перевірки достовірності) цифрового контенту (фотознімків та відеозаписів), у якому містяться покрокові інструкції щодо встановлення автентичності цифрових зображень та відеозаписів, отриманих від фізичних осіб або виявлених у відкритих джерелах мережі Інтернет [29]. Судові експерти у своїй роботі, у т. ч. під час створення експертних методик, можуть використовувати напрацювання міжнародних спільнот журналістів щодо боротьби з дезінформацією.

У 2015 році створено міжнародний проєкт із боротьби з дезінформацією в інтернеті First Draft, до якого приєдналися Facebook, Instagram, Twitter, Youtube, LinkedIn та ін. У межах цього проєкту проводяться дослідження, створюються і безкоштовно оприлюднюються інструменти та різного роду посібники щодо перевірки справжності цифрової інформації.

На сайті міжнародної спільноти журналістських розслідувань Bellingcat опубліковані посібники щодо верифікації цифрової інформації з відкритих джерел (OSINT) з метою встановлення певних фактів з її використанням. Досить цікавими є публікації щодо використання світла сонця і тіні на фотознімках для встановлення геолокації, способу відстеження польотів літальних апаратів та ін. [30]. Одним із найвідоміших проєктів Bellingcat є дослідження авіакатастрофи в Україні літака, який виконував рейс Malaysia Airlines Flight 17. Групою Bellingcat встановлено, що зенітно-ракетний комплекс «Бук», яким було збито літак, входив до складу 53-ї зенітно-ракетної бригади зс рф, що базується в місті Курськ (рф).

Перевірку автентичності цифрових зображень і відеозаписів у посібниках щодо верифікації цифрової інформації рекомендовано розпочинати з перевірки EXIF-даних (Exchangeable Image File Format) – метаданих, які «вбудовані» в цифрові файли та можуть містити дату й час зйомки, місце зйомки, тип камери тощо. Для перевірки метаданих вручну рекомендовано відкрити зображення або відео у програмі для перегляду метаданих (наприклад, Adobe Photoshop, ExifTool та ін.), перевірити різні поля метаданих (автор, дата створення, камера, географічні координати тощо) та порівняти ці дані з відомими фактами або ін. джерелами. Також існують безкоштовні онлайн-інструменти (Jeffrey's Exif Viewer або Metapicz), які дозволяють завантажити зображення та переглянути його метадані (модель камери, тип об'єктиву, витримку, діафрагму, дату створення файлу, географічні координати та ін.) [31].

Деякі фотознімки та відеозаписи можуть мати цифровий підпис, який підтверджує їх автентичність. Програма для перевірки цифрових підписів GnuPG дозволяє виявити зміни підпису після створення файлу. На жаль, перевірка метаданих файлу не може гарантувати його автентичності тому, що існують способи їх зміни. Зокрема, додавати та редагувати метадані можна за допомогою програм Adobe Lightroom, Capture One, Jeffrey's Exif Viewer, Findexif.com [29, с. 40], GroupDocs.Metadata [32] та програм для редагування фотознімків на смартфоні [33]. Для цього лише потрібно відкрити фотознімок у програмі редагування, натиснути на вкладку «Метадані» або «Інформація про зображення» та ввести необхідну інформацію. У Windows 10 можна додати метадані до зображень, натиснувши правою кнопкою миші на файлі, вибравши «Властивості», а потім перейшовши на вкладку «Деталі» [34].

Ресурси вебсайту Foto Forensics дозволяють виявити ділянки редагування на фотознімках (прибирання окремих елементів зображення або їх додавання). Спеціальні пошукові сервіси Google Search by Image та TinEye дозволяють знайти оригінальне джерело зображення та перевірити, де раніше воно публікувалося [33].

Програма JPEGSnoop, яка працює лише в операційній системі Windows, дозволяє переглядати метадані не лише зображень, але й форматів AVI, DNG, PDF та ін. Вона також допомагає виявити редаговані фрагменти файлів [29].

Автентичність цифрової інформації також можливо перевірити за допомогою пошукових систем (Google, Bing та ін.). Наприклад, можна ввести в пошукову систему ключові слова, пов'язані з фотознімком або відеозаписом, переглянути результати пошуку і знайти додаткову інформацію про зображення або відеозапис. Пошук за зображенням за допомогою Google Images або Bing Images також може допомогти знайти оригінальне або схоже зображення та визначити «надійність» ресурсу, на якому він розміщений.

Останнім часом судді намагаються підвищити свій рівень обізнаності щодо технічних характеристик цифрових доказів для уникнення судових помилок. Вони вважають, що «…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» [35]. Судді показують обізнаність в оцінці цифрових доказів і зазначають, що «питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами - CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень» [36].

Науковці в галузі кримінально-правових наук вважають, що сьогодні рівень підготовки слідчих у роботі із програмно-технічними комплексами та складними програмними оболонками є низьким. У зв'язку з цим потрібно обов'язково залучати спеціаліста під час роботи з «цифровими доказами», оскільки найменша некваліфікована дія може призвести до втрати важливої доказової чи орієнтуючої інформації [37].

Поліцейські академії США задля попередження слідчих помилок при роботі з цифровими доказами в програму підготовки (перепідготовки) співробітників поліції додали дисципліну щодо роботи з цифровими доказами на основі настанов щодо роботи з ними [38]. Розробники цих програм зазначають, що цифрові докази можуть бути марними без встановлення їх достовірності і докладної фіксації «ланцюжка зберігання доказів». Ними було розроблено алгоритми протоколювання процесуальних дій із використанням цифрових доказів та зазначено перелік питань, які мають бути висвітлені в протоколах [39, p. 15-17].

Автори настанов щодо роботи з цифровими доказами особливу увагу приділяють таким проблемам:

- необхідності постійного підвищення кваліфікації слідчих і прокурорів щодо технічних аспектів цифрових доказів [39, p. 23];
- наданню рекомендацій щодо перевірки справжності електронних листів [39, p. 31];
- перевірці достовірності роздруківок інформації з комп'ютера, поясненню понять «оригінал», «копія» і «дублікат» цифрової інформації [39, p. 33];

- формуванню алгоритму встановлення автентичності цифрових фотознімків та ін. [39, p. 50].

Висновки. Використання цифрових доказів у кримінальному провадженні є потужним інструментом для підвищення якості та ефективності розслідування злочинів. Документування слідчих дій і фіксація доказів супроводжується цифровими фотозйомкою, аудіо- та відеозаписом, а метадані цифрових файлів на будь-якому етапі кримінального провадження дозволяють підтвердити їх автентичність та процесуальну значущість.

Правоохоронні органи під час розслідування воєнних злочинів активно використовують цифрову інформацію з відкритих джерел. Така інформація в основному використовується як орієнтуюча та допомагає складати план розслідування й будувати слідчі та судові версії. За умови відповідності такої інформації критеріям оцінки доказів, вона може слугувати процесуальним джерелом доказів для встановлення фактів вчинення злочинів, з метою ідентифікації злочинців і потерпілих, для розшуку зниклих безвісти осіб та ін.

Суди України та США ухвалюють протилежні рішення щодо визнання інформації у цифровому вигляді процесуальними джерелами доказів. Навіть за однакових умов судді в одних випадках визнають копії цифрових записів допустимими доказами, в інших – недопустимими. Це негативно впливає на якість здійснення правосуддя тому, що в умовах глобальної цифровізації суспільства цифрові докази іноді є визначальними для об'єктивного вирішення справи і притягнення винних до відповідальності.

Для допомоги в оцінюванні допустимості, належності і достовірності цифрових доказів слідчі і судді зазвичай звертаються до судових експертів, однак навіть останні не завжди здатні вирішити завдання щодо встановлення автентичності матеріалів відео- та звукозапису тому, що через швидкий розвиток інформаційних технологій існуючі методики судової комп'ютерно-технічної експертизи швидко «застарівають» і вимагають постійного доопрацювання.

Правоохоронні органи США, Канади й деяких країн Європи спільно з провідними науковими установами розробили міждисциплінарні посібники і стандарти щодо фіксації, відновлення, збереження й дослідження цифрових доказів, а міжнародні об'єднання журналістів – алгоритми верифікації цифрової інформації. Такі сучасні напрацювання допоможуть судовим експертам під час розроблення методик щодо автентифікації цифрової інформації та в їх практичній діяльності.

Рівень підготовки слідчих щодо програмно-технічних комплексів та складних програмних оболонок є низьким, тому залучення спеціаліста під час роботи з цифровими доказами є обов'язковим. Недостатній рівень знань може привести до псування цифрової інформації або безповоротньої її втрати.

В Україні програми підготовки і підвищення кваліфікації співробітників правозастосовних органів слід доповнити базовою підготовкою щодо роботи з цифровими доказами із використанням сучасних напрацювань науковців і журналістів країн Європи та США.

У законодавстві США цифрові докази виокремлені в окрему групу та визначений порядок оцінки їх допустимості та достовірності з використанням метаданих цифрового файлу.

У законодавстві України відсутні визначення цифрового доказу, порядок фіксації цифрової інформації з переліком даних, які мають бути обов'язково зафіксовані в протоколі процесуальної дії та його додатках. Неякісна та неповна фіксація цифрової інформації в подальшому може привести до не визнання її процесуальним джерелом доказів у кримінальному провадженні. На сьогодні в Україні ще не склався єдиний підхід щодо визначення достовірності цифрових доказів, вилучених як з матеріальних носіїв інформації, так і з мережі Інтернет. Існує необхідність урегулювання цього питання як на законодавчому рівні, так і шляхом розроблення методичних рекомендацій для співробітників правозастосовних органів щодо фіксації та автентифікації цифрової інформації з використанням сучасних напрацювань науковців і журналістів міжнародних спільнот щодо боротьби з дезінформацією в цифровому просторі. До КПК України слід внести доповнення щодо визначення поняття цифрових доказів та їх процесуальних носіїв, докладного порядку вилучення цифрової інформації, її огляду, фіксації і зберігання із зазначенням переліку обов'язкової інформації щодо цифрових доказів, яка має бути процесуально закріплена. Порядок верифікації і критерії достовірності цифрової інформації також мають бути визначені на законодавчому рівні.

Перспективними завданнями щодо подолання проблем визнання достовірності цифрових доказів у кримінальному провадженні в Україні є такі:

- розроблення алгоритму ідентифікації, збирання, здобуття та збереження цифрових доказів, т. ч. цифрової інформації з відкритих джерел, для співробітників правоохоронних органів на основі міжнародних стандартів;
- створення експертних методик для верифікації цифрової інформації, яка відповідатиме сучасному розвитку інформаційних технологій та включатиме відповідні напрацювання науковців, журналістів та ІТ-спеціалістів країн Європи та США.

Використані джерела:

1. Книга катів українського народу : база російських військових, які чинили злочини в Україні. URL : https://russian-torturers.com/.

2. Задокументовані воєнні злочини впродовж січня 2024: огляд. *Українська Гельсінська Спілка з прав людини. 15.02.2024.* URL : https://www.helsinki.org.ua/articles/zadokumentovani-voienni-zlochyny-vprodovzh-sichnia-2024-ohliad/.

3. Статистика бази даних воєнних злочинів T4P. URL : https://t4pua. org/stats.

4. Воєнні злочинці рф. *Головне управління розвідки міністерства оборони України : офіційний сайт.* URL: https://gur.gov.ua/content/war-criminals-rf.html.

5. Імовірні воєнні злочини Росії проти України розслідує 21 країна – Євроюст оголосив про запуск загальної бази даних доказів. *Freedom (uatv.ua).* URL : https://uatv.ua/uk/imovirni-voyenni-zlochyny-rosiyi-proty-ukrayiny-rozsliduye-21-krayina-yevro-yust-ogolosyv-pro-zapusk-zagalnoyi-bazy-danyh-dokaziv/.

6. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики* : зб. наук. пр. Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2023. Вип. 1 (30). С. 126-143. URL : https://doi.org/10. 32353/khrife.3.2022.08

7. Пільков К. М. Властивості доказів та критерії їх оцінювання. *Господарське право і процес.* 2020. № 4. С. 88-93. DOI : https://doi.org/10.32849/2663-5313/2020.4.14.

8. Лобойко Л. М., Банчук О. А. Кримінальний процес: Навчальний посібник. Київ: Ваіте, 2014. 280 с.

9. 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.

10. Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні. *Global Rights Compliance*. Амстердам: GRC, 2023. 552 с.

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

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

13. 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: https://doi.org/10.15394/jdfsl.2011.1088.

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

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

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

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

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

19. 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. 32 p. URL : https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf.

20. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації / Авт. колектив: А. В. Захарко, А. Г. Гаркуша, В. В. Рогальська, І. В. Краснобрижий, О. В. Брягін. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. 73 с.

21. Lewulis Piotr. Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. January 2021. *International Journal of Electronic Security and Digital Forensics* 13(4):403. DOI : https://doi.org/10.1504/IJESDF.2021.10034988

22. Sean E. Goodison, Robert C. Davis, and Brian A. Jackson. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. *Research report (Rand Corporation).* RAND Corporation, 2015. 32 p. URL : https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf.

23. Berkeley Protocol on Digital Open Source Investigations. *Unated Nations Human Right.* New York and Geneva, 2022. 102 p. URL : https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.

24. Авдєєва Г. К. Цифрова інформація як доказ у кримінальному провадженні. *Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану* : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квітня 2023 р.) : у двох томах. Том 1 / голов. ред. В. Ф. Пузирний ; Академія Державної пенітенціарної служби. Чернігів : Академія ДПтС, 2023. С. 13-17.

25. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT). Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Чинний від 01.01.2019 р. Київ : УкрНДНЦ, 2018. 31 с.

26. Методика ідентифікаційних і діагностичних досліджень матеріалів та апаратури цифрового й аналогового звукозапису зі застосуванням програмного забезпечення «Фрактал» при проведенні експертиз матеріалів та засобів відео та звукозапису: наук.-мет. посіб. / Рибальський О. В., Соловйов В. І., Журавель В. В., Татарнікова Т. О. Київ : ДУІКТ, 2013. 75 с.

27. Климчук М. П., Комиссарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. Львів: Львівський державний університет внутрішніх справ, 2022. 112 с.

28. Брендель О. І. Дослідження автентичності цифрових відео- та звукозаписів. *Використання цифрових технологій у криміналістиці та судовій експертизі* : матеріали Міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р. : електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К. Авдєєва] ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2024. С. 56-60.

29. Посібник з верифікації цифрового контенту. *Європейський центр журналістики.* Редактор: Крейг Сільверман. Інститут Пойнтера. Амстердам, 2022. 130 с. URL: https://verificationhandbook.com/book_ua/.

30. Guides. Bellingcat. URL : https://web.archive.org/web/20210110210248/; https://www.bellingcat.com/category/resources/how-tos/.

31. Як перевірити зображення на достовірність з Verify? *Громадський простір.* URL: https://www.prostir.ua/?kb=yak-z-verify-pereviryty-zobrazhennya-na-dostovirnist.

32. Редактор метаданих фотографій. *Продукти GroupDocs.* URL: https://products.groupdocs.app/uk/metadata/photo.

33. Дорош Марина. 13 онлайн-інструментів для перевірки контенту. URL : https://ms.detector.media/how-to/post/1707/2014-02-05-13-onlayn-instrumentiv-dlya - perevirky-kontentu/.

34. Як додати метадані до зображень у Windows 10. URL : https://altitude tvm. com/uk/windows-10/3157-cara-menambahkan-metadata-pada-gambar-di-windows-10. html.

35. 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/.

36. Постанова Верховного Суду від 29.03.2021 р. у справі № 554/5090/16-к. URL : http://iplex.com.ua/doc.php?regnum=96074938&red=10000382305f3f5d2c0c6c7594f0b5f8dae19c&d=5.

37. Кіберзлочинність та електронні докази = Cybercrime and digital evidence: навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

38. David W. Hagy. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. Paperback – July 19, 2012 by U.S. Department of Justice (Author), Office of Justice Programs (Author), National Institute of Justice (Author). 90 pages. URL : https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-eviden ce-courtroom-guide-law-enforcement-and-prosecutors.

39. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U.S. Department of Justice Office of Justice Programs. January 2007. Washin-gton. 81 pages. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors.

References:

1. Knyha kativ ukrainskoho narodu : baza rosiiskykh viiskovykh, yaki chynyly zlochyny v Ukraini. (N. b.) N. p. URL: https://russian-torturers.com. [in Ukrainian].

2. Zadokumentovani voienni zlochyny vprodovzh sichnia 2024: ohliad. – Documented war crimes during January 2024: an overview. *Ukrainska Helsinska Spilka z prav liudyny.* 15.02.2024. (2024) N. p. URL : https://www.helsinki.org.ua/articles/zadokumen-tovani-voienni-zlochyny-vprodovzh-sichnia-2024-ohliad. [in Ukrainian].

3. Statystyka bazy danykh voiennykh zlochyniv T4P. (N. b.) N. p. URL: https://t4pua.org/stats. [in Ukrainian].

4. Voienni zlochyntsi rf. *Holovne upravlinnia rozvidky ministerstva oborony Ukrainy : ofitsiinyi sait - The Main Directorate of Intelligence of the Ministry of Defense of Ukraine: official we bsite.* (N. b.) N. p. URL: https://gur.gov.ua/content/war-criminals-rf.html. [in Ukrainian].

5. Imovirni voienni zlochyny Rosii proty Ukrainy rozsliduie 21 kraina – Yevroiust oholosyv pro zapusk zahalnoi bazy danykh dokaziv. *Freedom (uatv.ua).* URL : https://uatv.ua/uk/imovirni-voyenni-zlochyny-rosiyi-proty-ukrayiny-rozsliduye-21-krayina-ye vroyust-ogolosyv-pro-zapusk-zagalnoyi-bazy-danyh-dokaziv. [in Ukrainian].

6. Avdieieva, H., Zhyvutska-Kozlovska, E. (2023). Problemy vykorystannia tsyfrovykh doka-ziv u kryminalnomu sudochynstvi Ukrainy ta SShA. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky : zb. nauk. pr. Kharkiv : NNTs «ISE im. Zasl. prof. M. S. Bokariusa» - Theory and practice of forensic examination and criminology: collection. of science pr. Kharkiv: NSC "ISE named after Ex. Prof. M. S. Bokarius", issue 1 (30), 126-143.* URL : https://doi.org/10.32353/khrife.3.2022.08. [in Ukrainian].

7. Pilkov, K. M. (2020). Vlastyvosti dokaziv ta kryterii yikh otsiniuvannia. *Hospodarske pravo i protses - Commercial law and process, 4, 88-93.* DOI : https://doi.org/10.32849/2663-5313/2020.4.14. [in Ukrainian].

8. Loboiko, L. M., Banchuk, O. A. (2014) Kryminalnyi protses: Navchalnyi posibnyk. Kyiv: Vaite. [in Ukrainian].

9. Kryminalnyi protsesualnyi kodeks Ukrainy vid 13.04.2012 r. № 4651-VI. (2012) N. p. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text. [in Ukrainian].

10. Kerivnytstvo z bazovykh standartiv rozsliduvannia dlia dokumentuvannia mizhnarodnykh zlochyniv v Ukraini. (2023) *Global Rights Compliance*. Амстердам: GRC. [in Ukrainian].

11. International Organization on Computer Evidence (IOCE). (N. d.) *UIA. Global Civil Society Database.* N. p. URL : https://uia.org/s/or/en/1100029648. [in English].

12. Scientific Working Group on Digital Evidence (SWGDE). (N. d.) N. p. URL: https://www.swgde.org. [in English].

13. 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. Pp. 54-72. DOI: https://doi.org/10.15394/jdfsl.2011.1088. [in English].

14. Federal Rules of Evidence (FRE). Dec 1, 2020. (2020) *Legal Informational Institute.* N. p. URL : https://www.law.cornell.edu/rules/fre. URL : https://www.law.cornell.edu/rules/fre. [in English].

15. United States v. Budziak, 697 F.3d 1105 (2012) / *Caselaw Access Project.* URL: https://cite.case.law/f3d/697/1105/. [in English].

16. United States v. Burdulis, 753 F.3d 255 (1st Cir. 2014). N. p. URL : https://casetext.com/case/united-states-v-burdulis. [in English].

17. United States v. R. Burke. 633 F.3d 984 (10th Cir. 2011). N. p. URL : https://casetext.com/case/united-states-v-r-burke. [in English].

18. United States v. Bush. 727 F.3d 1308 (11th Cir. 2013). URL : https://casetext.com/case/united-states-v-bush-30. [in Ukrainian].

19. Goodison S. E., Davis R. C., Jackson B. A. (2015). Digital Evidence and the U. S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. RAND Corporation. 32 p. URL : https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf. [in Ukrainian].

20. Vykorystannia elektronnykh nosiiv informatsii z media-kontentom u yakosti dzherel dokaziv: metodychni rekomendatsii (2019) / A. V. Zakharko, A. H. Harkusha, V. V. Rohalska, I. V. Krasnobryzhyi, O. V. Briahin (Eds.). Dnipro: Dnipropetrovskyi derzha vnyi universytet vnutrishnikh sprav. [in Ukrainian].

21. Lewulis Piotr. Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. January 2021. *International Journal of Electronic Security and Digital Forensics, 13(4):403.* DOI : https://doi.org/10.1504/IJESDF.2021.10034988. [in English].

22. Sean, E. Goodison, Robert ,C. Davis, & Brian, A. Jackson. (2015) Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. *Research report (Rand Corporation). RAND Corporation.* N. p. URL : https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf. [in En-glish].

23. Berkeley Protocol on Digital Open Source Investigations. *Unated Nations Human Right.* (2022) New York and Geneva. N. p. URL : https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf. [in English].

24. Avdieieva, H. K. (2023). Tsyfrova informatsiia yak dokaz u kryminalnomu provadzhenni. *Aktualni pytannia teorii ta praktyky v haluzi prava, osvity, sotsialno-humanitarnykh ta povedinkovykh nauk v umovakh voiennoho stanu : materialy mizhnar. nauk.-prakt. konf. (m. Chernihiv, 25–26 kvitnia 2023 r.) : u dvokh tomakh. Tom 1 - Aktualni pytannia teorii ta praktyky v haluzi prava, osvity, sotsialno-humanitarnykh ta povedinkovykh nauk v umovakh voiennoho stanu : materialy mizhnar. nauk.-prakt. konf. (m. Chernihiv, 25–26 kvitnia 2023 r.) : (Vol. 1-2 ; Vol. 1), 13-17.* Akademiia Derzhavnoi penitentsiarnoi sluzhby. Chernihiv. [in Ukrainian].

25. DSTU ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT). (2018) Informatsiini tekhnolohii. Metody zakhystu. Nastanovy dlia identyfikatsii, zbyrannia, zdobuttia ta zberezhennia tsyfrovykh dokaziv. Chynnyi vid 01.01.2019 r. Kyiv : UkrNDNTs. [in Ukrainian].

26. Metodyka identyfikatsiinykh i diahnostychnykh doslidzhen materialiv ta aparatury tsyfrovoho y analohovoho zvukozapysu zi zastosuvanniam prohramnoho zabezpechennia «Fraktal» pry provedenni ekspertyz materialiv ta zasobiv video ta zvukozapysu : nauk.-met. posib. (2013) Kyiv : DUIKT. [in Ukrainian].

27. Klymchuk, M. P., Komissarchuk, Yu. A., Marko, S. I., Stetsyk, B. V. (2022). Sudova kompiuterno-tekhnichna ekspertyza u kryminalnomu provadzhenni : navch. posib. Lviv : Lvivskyi derzhavnyi universytet vnutrishnikh sprav. [in Ukrainian].

28. Brendel, O. I. (2024). Doslidzhennia avtentychnosti tsyfrovykh video- ta zvukozapysiv. *Vykorystannia tsyfrovykh tekhnolohii u kryminalistytsi ta sudovii ekspertyzi : materialy Mizhnar. nauk.-prakt. kruhloho stolu, m. Kharkiv, 11 hrud. 2023 r. : elektron. nauk. vyd. Nats. akad. prav. nauk Ukrainy- Vykorystannia tsyfrovykh tekhnolohii u kryminalistytsi ta sudovii ekspertyzi : materialy Mizhnar. nauk.-prakt. kruhloho stolu, m. Kharkiv, 11 hrud. 2023 r. : elektron. nauk. vyd. Nats. akad. prav. nauk Ukrainy, 56-60*; [redkol.: V. Yu. Shepitko, H. K. Avdieieva (Eds.)] NDI vyvch. problem zlochynnosti im. akad. V. V. Stashysa NAPrN Ukrainy. Kharkiv : Pravo. [in Ukrainian].

29. Posibnyk z veryfikatsii tsyfrovoho kontentu. (2022) *Yevropeiskyi tsentr zhurnalistyky - Yevropeiskyi tsentr zhurnalistyky*. Redaktor: Kreih Silverman. Instytut Pointera. Amsterdam. URL : https://verificationhandbook.com/book_ua/. [in Ukrainian].

30. Guides. Bellingcat. (N. d.) N. p. URL : https://web.archive.org/web/20210110210248/https://www.bellingcat.com/category/resources/how-tos/. [in Ukrainian].

31. Yak pereviryty zobrazhennia na dostovirnist z Verify? *Hromadskyi prostir - Hromadskyi prostir*. (N. d.) N. p. URL : https://www.prostir.ua/?kb=yak-z-verify-perevi ryty-zobra zhennya-na-dostovirnist. [in Ukrainian].

32. Redaktor metadanykh fotohrafii. *Produkty GroupDocs.* (N. d.) N. p. URL : https://products.groupdocs.app/uk/metadata/photo. [in Ukrainian].

33. Dorosh Maryna. 13 onlain-instrumentiv dlia perevirky kontentu. (N. d.) N. p. URL: https://ms.detector.media/how-to/post/1707/2014-02-05-13-onlayn-instru-mentiv-dly a-perevirky-kontentu. [in Ukrainian].

34. Yak dodaty metadani do zobrazhen u Windows 10. (N. d.) N. p. URL : https://altitudetvm.com/uk/windows-10/3157-cara-menambahkan-metadata-pada-gambar-di-windows-10.html. [in Ukrainian].

35. Stefaniv, N. (2021) Materialnyi nosii - lyshe sposib zberezhennia informatsii, yakyi maie znachennia tilky todi, koly E-dokument vystupaie rechovym dokazom. 02.11.2021. N. p. 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].

36. Postanova Verkhovnoho Sudu vid 29.03.2021 r. u spravi № 554/5090/16-к. (2021) N. p. URL : http://iplex.com.ua/doc.php?regnum=96074938&red=10000382305f3f5d2c0c6c7594f0b5f8dae19c&d=5. [in Ukrainian].

37. Kiberzlochynnist ta elektronni dokazy = Cybercrime and digital evidence: navch. posibnyk (2022) / [B. M. Holovkin, O. I. Denkovych, V. V. Lutsyk, D. M. Tsekhan (Eds.)] ; za red. kand. yuryd. nauk, dots. Olhy Denkovych, d-r prava, prof. Habriele Shmeltser. Elektron. vyd. Lviv : LNU im. Ivana Franka. [in Ukrainian].

38. David, W. Hagy. (2012) Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. Paperback – July 19, 2012 by U.S. Department of Justice (Author), Office of Justice Programs (Author), National Institute of Justice (Author). 90 pages. N. p. URL : https://www.ojp.gov/ncjrs/virtual-library/abstracts/ digital-evide-nce-courtroom-guide-law-enforcement-and-prosecutors. [in English].

39. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. (2007) U.S. Department of Justice Office of Justice Programs. January 2007. Washington. 81 pages. N. p. URL : https://www.ojp.gov/ncjrs/virtual-library/abstracts /digital-evidence-courtroom-guide-law-enforcement-and-prosecutors. [in English].

Стаття надійшла до редколегії 06.03.2024

Avdeeva G., *PhD in Law, Senior Staff Scientist, Leading researcher of Academician Stashis Scientific Research Institute for the Study of Crime Problems of National academy legal sciences of Ukraine (Kharkiv, Ukraine)*

PROBLEMS OF DETERMINING THE RELIABILITY OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

The article discusses the types of digital evidence and their essence, the problems of recognizing digital information as procedural sources of evidence in criminal proceedings. The features of the assessment of digital evidence according to the criterion of reliability are shown, the need for proper recording of digital evidence at different stages of criminal proceedings is substantiated. It has been proven that the metadata of digital files at any stage of criminal proceedings can confirm their authenticity and procedural significance.

The study showed that the courts of Ukraine and the United States make opposite decisions on the recognition of information in digital form as procedural sources of evidence, and the level of training of investigators in working with software and hardware complexes and complex software shells is low. This has a negative impact on the quality of the administration of justice, because in the context of the global digitalization of society, digital evidence is sometimes decisive for the objective resolution of a case and bringing the perpetrators to justice. It is proposed to supplement the training and advanced training programs for law enforcement officers with basic training in working with digital evidence using modern developments of law enforcement agencies, scientists and journalists from Europe and the United States.

The author analyzes the normative legal acts of Ukraine and the United States and the recommendations adopted by various EU and US institutions regarding the use of digital evidence in criminal proceedings and the recognition of them as procedural sources of evidence. At the legislative level in Ukraine, it is proposed to fix the verification procedure and criteria for the reliability of digital information.

Keywords: digital information, digital evidence, authentication of digital information, verification of digital information, reliability of digital evidence, criminal proceedings.