3. Lindsey A. Elkins (2003), Note, Five Foot Two With Eyes of Blue: Physical Profiling and the Prospect of a Genetics-Based Criminal Justice System, 17 NOTRE DAME J.L. ETHICS & PUB. POL'Y 269

4. Diana H. Fishbein (2000), Introduction to 1 THE SCIENCE, TREATMENT, AND PREVENTION OF ANTISOCIAL BEHAVIORS: APPLICATION TO THE CRIMINAL JUSTICE SYSTEM ch. 1

5. On state registration of human genomic information: Law of Ukraine dated 09.07.2022 No. 2391-IX. URL: https://zakon.rada.gov.ua/laws/show/2391–20#Text (accessed 27.02.2024).

ВЕРИФІКАЦІЯ ЦИФРОВИХ ДОКАЗІВ ЯК ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ, ПОВ'ЯЗАНИХ З ВІЙНОЮ

Галина АВДЄЄВА,
кандидат юридичних наук,
старший науковий співробітник,
провідний науковий співробітник
НДІ вивчення проблем злочинності НАПрН України

Сучасні цифрові технології забезпечують фіксацію, накопичення, систематизацію, зберігання і аналіз інформації, яка може слугувати доказами при розслідуванні воєнних злочинів. Для збирання, систематизації та оприлюднення верифікованої (перевіреної) інформації про воєнних злочинців рф та їхні злочини, скоєні на території України, створена база даних «Книга катів українського народу» [1], в якій всі ймовірні злочинці ідентифіковані правоохоронними органами України. База даних «T4P (Трибунал для Путіна)», створена у лютому 2022 р. міжнародними громадськими організаціями, на 18 лютого 2024 р. містить інформацію щодо 64460 злочинів, більшість яких (15973) вчинено в Харківській області [2].

Офіс Генерального прокурора України спільно з компанією «IT Defends» створили національну платформу WarCrimes.gov.ua, при-

значену для документування воєнних злочинів та злочинів проти людяності, вчинених російською федерацією в Україні.

Служба безпеки України в додатку Telegram запустила бот @russian_war_tribunal_bot та надала адресу електронної пошти tribunal.2022.02.24@gmail.com.ua, на які від фізичних осіб надходять відомості про воєнні злочини російських окупантів на території України. Ця інформація аналізується, систематизується і розміщується в цифровій базі даних.

Накопичення цифрової інформації про російських воєнних злочинців також здійснюється в базу даних «Воєнні злочинці рф» [3], яка дозволяє встановити географічне розташування ворожих сил та видів військ, встановити особи військових керівників та ін. важливу інформацію.

В міжнародній централізованій базі доказів міжнародних злочинів (CICED), створеній Агентством Європейського Союзу з питань судового співробітництва (Євроюстом), накопичено інформацію щодо 65 тисяч воєнних злочинів росіян в Україні. До цієї бази даних мають доступ правоохоронні органи 21 країни, в яких розслідуються воєнні злочини громадян рф в Україні.

Безумовно, накопичена в базах даних цифрова інформація є важливою у розслідуванні воєнних злочинів, однак, на жаль, не завжди вона може бути використувана в кримінальному провадженні як доказ навіть у випадках, коли в ній безпосередньо зафіксований факт вчинення злочину. За результатами узагальнення більше 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 [4, с. 132]. Не зважаючи на те, що кожна копія цифрового файлу ідентична оригіналу незалежно від виду носія, суди найчастіше не визнають цифрову інформацію належними і допустимими доказами через те, що до суду надається її копія на електронному носії, а не оригінал.

На сьогодні суди в Україні ухвалили лише 80 вироків щодо воєнних злочинів, скоєних російськими військовими в Україні. В судах перебувають 350 проваджень, а 512 підозрюваних вже ідентифіковано [5].

Науковці і працівники правоохоронних органів наголошують на тому, що у відкритих джерелах міститься безліч неправдивої цифрової інформації. Спецслужбами рф створюються фейкові (підроблені) новини для проведення інформаційно-психологічних атак. Вони супроводжуються підробленими фотознімками та відеозаписами, в т. ч. – створеними за допомогою штучного інтелекту. Тому для використання цифрової інформації у кримінальному провадженні її слід ретельно перевіряти на «істинність» (верифікувати).

Неповна верифікація (перевірка істинності) цифрової інформації 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.

Цифрова інформація може слугувати доказами при розслідуванні воєнних злочинів лише за умови її відповідності критеріям оцінки доказів (допустимість, належність, достовірність і достатність).

Допустимість доказу визначається законністю джерела походження та способу отримання і визначає його придатність для використання у судочинстві. Належність віддзеркалює здатність доказу підтверджувати або спростовувати будь-які обставини, що мають значення для справи. Достатнім є доказ, який відображає його здатність підтверджувати або спростовувати обставини, що мають значення для справи. Доказ вважається достовірним, якщо він відповідає дійсності. Тобто оцінка цифрових доказів без їх верифікації неможлива.

Першим етапом верифікації цифрової інформації є встановленні автора (власника, володільця, утримувача) цифрових аудіо та відеозаписів, які виявлені в інтернет-просторі або надіслані для розміщення в базі даних без засвідчення матеріалу кваліфікованим електронним підписом. 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 відкритих джерелах.

Питання щодо верифікації цифрової інформації, яка може підтвердити або спростувати певні події, часто вирішуються шляхом залучення експерта, який здійснює перевірку автентичності фотознімків і матеріалів аудіо- та відеозаписів.

Однак, навіть експерти не завжди здатні їх вирішити. Зокрема, встановлення автентичності матеріалів відео- та звукозапису здійснюється шляхом ідентифікації апаратури запису. На цій апаратурі здійснюється експериментальний запис, ознаки якого порівнюються з ознаками аналізованого запису. За відсутності апаратури встановити автентичність запису дуже складно [6]. При цьому судові експерти повідомляють, що на теперішній час складно створити конкретну методику автентифікації цифрових відео- та звукозаписів через їх різноманітність та відсутність наукових публікацій про їх характеристики. Через це можна лише охарактеризувати напрями виявлення певних ознак для вирішення питання щодо автентифікації цифрових записів [7, с. 57–58].

Європейським центром журналістики виданий посібник для верифікації (перевірки достовірності) цифрового контенту (фотознімків та відеозаписів), в якому містяться покрокові інструкції щодо встановлення автентичності цифрових зображень та відеозаписів, отриманих від фізичних осіб або виявлених у відкритих джерелах мережі Інтернет [8].

На сайті міжнародної спільноти журналістських розслідувань Bellingcat, що спеціалізується на верифікації цифрової інформації з відкритих джерел (OSINT), опубліковані посібники щодо верифікації цифрової інформації з відкритих джерел та встановлення певних фактів з їх використанням. Досить цікавими є публікації щодо використання сонця і тіні на фотознімках для встановлення геолокації, способу відстеження польотів літальних апаратів та ін. [9]. Одним із найвідоміших журналістських розслідувань Bellingcat є дослідження щодо збиття рейсу Malaysia Airlines Flight 17 в Україні. Групою журналістів Bellingcat встановлено, що зенітно-ракетний комплекс «Бук», яким було збито літак, входив до складу 53-ї зенітно-ракетної бригади збройних сил рф, що базується в місті Курськ (рф).

Перевірку автентичності цифрових зображень і відеозаписів в зазначених посібниках рекомендовано розпочинати з перевірки EXIF-даних (Exchangeable Image File Format) – метаданих (інформації про інформацію), 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 іншими 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.) [10].

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 його автором.

На жаль, перевірка метаданих файлу не може гарантувати його автентичності тому, що існують способи їх зміни. Зокрема програми, GroupDocs.Metadata або програми для редагування фотознімків на смартфоні, які дозволяють додавати та редагувати метадані [12]. 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» [13].

Ресурси веб-сайту 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 воно публікувалося раніше [12].

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 та помилки в пошкоджених файлах [8].

Автентичність цифрової інформації можна перевірити й за допомогою пошукових систем (Google, Bing та ін.). Наприклад, можна ввести ключові слова, пов'язані з фотознімком або відеозаписом, у пошукову систему, 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 наголошують 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»[1]. Судді об'єднаної палати Касаційного кримінального суду Верховного Суду України показали обізнаність у верифікації 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» [15].

У співробітників правозастосовних органів під час оцінки доказової інформації у цифровому вигляді та висновків експерта щодо дослідження цифрових доказів виникають певні труднощі через відсутність у них спеціальних знань в IT-сфері та спеціальної літератури. Тому посібники з верифікації цифрової інформації, створені відомими міжнародними журналістами-розслідувачами спільно зі спеціалістами у галузі IT, можуть використовуватися не лише журналістами, а й слідчими, суддями, адвокатами та судовими експертами. Однак, не зважаючи на те, що всі копії цифрового файлу є ідентичними оригіналу, для верифікації цифрової інформації слід використовувати виключно її копії, щоб не змінити метадані цифрового доказу.

В умовах повномасштабної війни рф проти України, коли в різних базах даних накопичена безліч цифрової інформації щодо воєнних злочинів, частина якої надійшла з непідконтрольних Україні територій, особливої актуальності набули проблеми верифікації такої інформації. Лише верифікована цифрова інформація може слугувати належними і достовірними доказами у кримінальному провадженні. Вирішити проблеми верифікації такої інформації до-

[1] 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).

поможе комплексний підхід, який включає перепідготовку та підвищення кваліфікації працівників правоохоронних органів щодо можливостей верифікації цифрової інформації, підвищення кваліфікації судових експертів щодо автентифікації та верифікації цифрових доказів, розроблення експертних методик щодо вирішення зазначених питань з використанням новітніх розробок журналістів-розслідувачів країн Європи та США.

Список використаних джерел:

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

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

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

4. 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. https://doi.org/10.32353/khrife.3.2022.08. С. 132.

5. Губа Роман. Костін: Суди ухвалили 80 вироків щодо воєнних злочинів рф. Deutsche Welle. 25.02.2024. URL: https://www.dw.com/uk/sudi-uhvalili-80-virokiv-sodo-voennih-zlocinciv-vijsk-rf-genprokuror/a-68369914?maca=ukr-rss-ukrnet-ukr-all-3816-xml

6. 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.– К.: ДУІКТ, 2013. 75 с.

7. 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. 144 с.

8. Посібник з верифікації цифрового контенту. Європейський центр журналістики. Європейський Центр Журналістики. Редактор: Крейг Сільверман, Інститут Пойнтера. 130 с. URL: https://verificationhandbook.com/book_ua/

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

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

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

12. 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/

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

14. 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/

15. 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 .