ЦИФРОВІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

АВДЄЄВА Галина,
канд. наук, Науково-дослідний інститут вивчення проблем злочинності
імені академіка В.В. Сташиса, Україна,
ORCID ID: 0000-0003-4712-728x

Summary: *The definition of the term „digital evidence„ is formulated. The concepts of „electronic evidence„ and „digital evidence„ are separated. Based on the results of the generalization of judicial practice, it has been established that judges have certain difficulties in recognizing information in digital form as acceptable and reliable evidence. Proposals have been made to improve the efficiency of the use of digital evidence in criminal proceedings.*

Key words: *digital evidence, electronic evidence, admissibility of evidence, sources of evidence, digital information, criminal proceedings and fixation of evidence.*

Наприкінці минулого століття завдяки розвитку цифрових і мережевих технологій співробітники правоохоронних органів почали використовувати доказову інформацію в електронній (цифровій) формі, яка міститься в різного роду електронних пристроях та телекомунікаційних мережах, а саме: комп'ютерах, мобільних телефонах, фото- та відеокамерах, GPS-навігаторах, в соціальних мережах, на різних сайтах в мережі Інтернет та ін. Зокрема, за допомогою даних GPS можна встановити факт перебування підозрюваних осіб на місці вчинення злочину, а за текстовими повідомленнями та електронними листами, цифровими фотознімками, аудіо- та відеозаписами – причетність осіб до протиправної діяльності.

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

Сучасними завданнями цифрової криміналістики слугують пошук і аналіз цифрових слідів, їх аналіз, збирання доказової інформації у цифровому середовищі. Найбільш складними і масштабними є завдання щодо пошуку інформації у відкритому доступі та аналізу потенційних джерел доказів – величезної кількості загальнодоступних відео- та аудіо-записів, фото- та супутникових знімків, текстів, звітів, публікацій в соціальних мережах.

Електронні пристрої слугують сховищем цифрової інформації щодо різного роду подій і явищ, дій окремих осіб, загальної і особистої інформації, тощо. Завдяки тому, що сучасні мобільні телефони мають широкий набір функцій (здійснення і приймання дзвінків, телефонна книга, фото- і відеокамера, диктофон, доступ до інтернету, створення і редагування текстових файлів і повідомлень, електронна пошта, соціальні мережі, месенджери і сервіси спілкування та ін.), вони зберігають цифрові сліди користування цими функціями і слугують своєрідними архівами особистої ін.-формації. Така інформація може бути включена до доказової бази лише за умови її виявлення, вилучення, дослідження і процесуального закріплення із дотриманням прав людини та з урахуванням захисту персональних даних.

Науковці у галузі кримінально-правових наук одночасно використовують терміни „електронні”

та „цифрові” докази, але між ними існують відмінності. На сьогодні цифрові пристрої повністю витіснили аналогові і різниця між аналогової та цифровою інформацією полягає в тому, що аналогова інформація безперервна, а цифрова – дискретна. Термін „цифровий доказ” є більш точним для інформації, яка існує у вигляді бінарного (двійкового) коду, а термін „електронний доказ” більше підходить для електронних пристроїв, до складу яких входять електронні компоненти (радіодеталі). Електронними доказами можуть слугувати пристрої, за допомогою яких створюють, перетворюють, передають та зберігають цифрові докази.

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”. [1, с. 257]. 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 і 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.

У 2012 р. був прийнятий спеціальний міжнародний стандарт ISO/IEC 27037:2012 [2], 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.) встановили, що до авіакатастрофи с пасажирським Boeing-777 MH17 причетні конкретні особи.

Національний стандарт України ДСТУ ISO/IEC 27037:2017 [3] є єдиним в Україні офіційним документом, який стосується цифрових доказів. В ньому викладені настанови щодо ідентифікації, збирання, здобуття та збереження цифрових доказів, однак, законодавчого закріплення ці рекомендації поки що не мають.

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. [4, 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. Автори Протоколу надають рекомендації щодо визначення меж вирішуваного завдання з метою економії часу та забезпечення особистої безпеки свідків і потерпілих.

Останніми роками у судах України все частіше предметом дослідження стають цифрові докази, однак у суддів виникають певні труднощі щодо визнання інформації у цифровій формі допустимими і достовірними доказами. Часто адвокати заявляють клопотання про недопустимість цифрового доказу через те, що спочатку з телефона інформація копіювалася на комп'ютер, а лише згодом – на оптичний диск, який потім надавався до суду як процесуальний носій доказу. Захисники вважають, що така копія не відповідає оригіналу тому, що при зміні носіїв інформації змінюється формат файлу [5]. Це є хибним твердженням тому, що однією з основних ознак інформації у цифровій формі є те, що всі її копії, зафіксовані на різних носіях, є ідентичними оригіналу (повністю співпадають за всіма ознаками, включаючи формат файлу). Не зважаючи на це Верховний Суд (ВС) в Ухвалі за справою №397/2588/13-к підтримав рішення судів першої та апеляційної інстанції та визнав недопустимим доказом виконаний під час проведення оперативно-роз-

шукових заходів відео- та аудіозапис факту надання хабаря судді у його робочому кабінеті. Суд встановив, що записи були копіями, і як наслідок, протоколи про здійснення негласних слідчих (розшукових) дій (НСРД), додатком до якого слугував цей цифровий доказ, протокол огляду запису, де слідчий розшифрував текст розмов щодо надання хабаря, висновки трьох судових експертиз визнано недопустимими доказами, оскільки вони є похідними від вказаного запису. Обвинуваченого було виправдано [6].

Аналіз судової практики показав, що за однакових умов до недавнього часу судді приймали протилежні рішення. В одних випадках вони визнавали копії цифрових записів допустимими доказами, в інших – недопустимими (особливо – щодо корупційних злочинів). Однак, останнім часом судді намагаються підвищити свій рівень обізнаності щодо технічних характеристик цифрових доказів для уникнення судових помилок. Зокрема, суддя Касаційного кримінального суду Верховного Суду України (ККС ВС) Надія Стефанів наголошує на тому, що судді мають самостійно дбати про підвищення своїх професійних знань щодо використання електронних доказів та застосовувати їх відповідно до чинного процесуального законодавства [7].

Судові рішення останніх 2-3 років відрізняються від попередніх більш детальним розглядом і поясненням технічних характеристик цифрових доказів, що надає більше шансів для визнання допустимим доказом копії інформації у цифровій формі. Судді детально оцінюють достовірність висновків експерта та досліджують цифрові докази безпосередньо (в т.ч. – інформацію з мобільних телефонів) [8; 9].

Суди в Україні все частіше відхиляють клопотання сторони захисту щодо невизнання допустимими і достовірними копій цифрових доказів, протоколів їх огляду та висновків судових експертиз під час розгляду справ різних категорій. 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 від 22 травня 2003 року № 851-IV „Про електронні документи та електронний документообіг” 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. Той самий електронний документ (відеозапис) може існувати на різних носіях. Усі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення” [10]. Таке саме рішення викладене у Постанові ККС ВС від 19 серпня 2021 року у справі №756/8124/19 [11] та Ухвалі ККС ВС від 19 серпня 2021 року у справі №756/8124/19 [12], в яких залишено без руху скарги захисників щодо недопустимості копій цифрової інформації як доказів.

За результатами узагальнення практики суду касаційної інстанції з питань проведення та оцінювання результатів НСРД у кримінальному провадженні встановлено, що найчастіше причинами не визнання 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; не відкриття стороні захисту в порядку ст. 290 Кримінального процесуального кодексу (КПК) України доручення на проведення НСРД; відсутність процесуального оформлення рішення слідчого або прокурора про залучення до проведення НСРД „іншої особи” та ін. [13, с. 51].

Науковці Національного інституту юстиції США наголошують на важливості докладного протоколювання процесів аутентифікації (встановлення справжності) та всіх інших дій з 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 інфо-

рмації у первісному вигляді [14, с. 13].

Від компетенції та правильного рішення співробітників правозастосовних органів (слідчих, суддів, прокурорів, оперативних працівників) залежить, чи буде окремий цифровий доказ відігравати провідну роль у вирішенні конкретної справи. Вони повинні знати базові технологічні характеристики цифрових пристроїв і цифрової інформації. Відповідна методична і довідкова література має бути розроблена і включена до програм підвищення кваліфікації окремо для кожної категорії співробітників.

В КПК України відсутнє визначення терміну „цифрові докази”, не зазначений докладний порядок їх вилучення, огляду, фіксації і зберігання. Це може призвести до помилок у роботі з цифрової інформацією і невизнання її допустимим і достовірним доказом у суді.

КПК України бажано доповнити такими новелами: визначення поняття „цифрові докази” та їх процесуальних носіїв; розмежування понять „електронний доказ” і „цифровий доказ”; докладний порядок вилучення цифрової інформації, її огляду, фіксації і зберігання із зазначенням переліку обов'язкової інформації щодо цифрових доказів, яка має бути процесуально закріплена; порядок оцінки допустимості і достовірності цифрового доказу за певними критеріями.

Бібліографічні посилання:

1. Цехан Д.М. *Цифрові докази: поняття, особливості та місце у системі доказування*. В: Науковий вісник Міжнародного гуманітарного університету. Юриспруденція, Вип. 5, 2013. с. 256-260.
2. *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. https://www.iso.org/standard/44381.html.
3. 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., УкрНДНЦ, Київ, 2018. 31 с.
4. *Berkeley Protocol on Digital Open Source Investigations. United Nations Human Right*. New York and Geneva, 2022. 102 p. https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.
5. *Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду*. Верховний суд України: офіційний сайт. 28 жовтня 2021. https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/.
6. Ухвала ВС від 29.05.2018 р. Справа №397/2588/13-к. *Єдиний державний реєстр судових рішень*. http://reyestr.court.gov.ua/Review/74475933.
7. Стефанів Н. *Матеріальний носій – лише спосіб збереження інформації, який має значення тільки тоді, коли е-документ виступає речовим доказом. Інформаційне агентство „ADVOKAT POST”*. 02.11.2021. https://advokatpost.com/materialnyj-nosij-lyshe-sposib-zberezhennia-informatsii-iakyj-maie-znachennia-tilky-todi-koly-e-dokument-vystupaie-rechovym-dokazom-suddia-stefaniv/.
8. *Вирок Дзержинського районного суду м. Харкова від 21.06.2019 по справі №638/5928/18*. Провадження №1-кп/638/585/19. https://zakononline.com.ua/court-decisions/show/82552131.
9. *Вирок Вищого антикорупційного суду від 17.02.2022 по справі № 991/4996/20*. Провадження №1-кп/991/53/20. http://iplex.com.ua/doc.php?regnum=103409303&red=1000033ab78a5efaf99e232b33e4b495c626d6&d=5.
10. *Постанова ККС ВС України від 22 жовтня 2020 року у справі № 677/2040/16-к (провадження №51-5738км19)*. http://iplex.com.ua/doc.php?regnum=92458395&red=1000035e35a331e82f61d9818795df8ecd0762&d=5.
11. *Постанова ККС ВС від 25 січня 2021 року у справі №236/4268/18, провадження №51-3124км*

20. http://iplex.com.ua/doc.php?regnum=94905297&red=10000347f1960a9ea9dcf00a1e2414ca336-51f&d=5.

12. *Ухвала ККС ВС від 19 серпня 2021 року у справі № 756/8124/19 (провадження № 51-601 ск 21)*. http://iplex.com.ua/doc.php?regnum=94874011&red=1000037c6dddd0bd0c253b026e82724e953e47&d=5.
13. Тализіна Я.О. *Узагальнення практики суду касаційної інстанції з питань проведення та оцінювання результатів НСРД у кримінальному провадженні*. Тренінговий центр прокурорів України. 2021. 71 с. https://ptcu.gp.gov.ua/wp-content/uploads/2021/11/uzagalnennya_praktyky_sudu_po_nsrd_z_qrkodamy_1.pdf.
14. 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. https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf.