СЕКЦІЯ 1
АКТУАЛЬНІ ПИТАННЯ ГАЛУЗЕВИХ ЮРИДИЧНИХ НАУК ТА ПРАВОВИХ ПРАКТИК

Авдєєва Галина Костянтинівна,
кандидат юридичних наук, старший науковий співробітник,
провідний науковий співробітник НДІ
вивчення проблем злочинності
імені академіка В. В. Сташиса НАПрН України

ЦИФРОВА ІНФОРМАЦІЯ ЯК ДОКАЗ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

У 90-х рр. XX ст. завдяки розвитку цифрових і мережевих технологій співробітники правоохоронних органів почали використовувати доказову інформацію в електронній (цифровій) формі, яка міститься в різного роду електронних пристроях і телекомунікаційних мережах, а саме: комп'ютерах, мобільних телефонах, фото- та відеокамерах, GPS-навігаторах, у соціальних мережах, на різних сайтах у мережі Інтернет та ін.

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.

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 інформації. Така інформація може бути внесена

до доказової бази лише за умови її виявлення, вилучення, дослідження і процесуального закріплення з дотриманням прав людини та з урахуванням захисту персональних даних.

Науковці в галузі кримінально-правових наук одночасно використовують терміни «електронні» та «цифрові» докази, але між ними існують відмінності. На сьогодні цифрові пристрої повністю витіснили аналогові, різниця між аналоговою 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.

Цехан Д. М. 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 теж 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 ухвалений спеціальний міжнародний стандарт ISO/IEC 27037:2012 [2], який містить настанови щодо роботи з 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 з 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. У 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 з дотриманням принципів об'єктивності, компетентності, підзвітності, відповідності законодавству, безпеки, точності, незалежності, прозорості, дотримання прав людини та ін. Автори Протоколу надають рекомендації щодо визначення меж виконуваного завдання з метою економії часу та забезпечення особистої безпеки свідків і потерпілих.

Останніми роками в 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 певного пристрою для запису 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 хибне твердження, оскільки однією з основних ознак інформації у цифровій формі є те, що всі її копії, зафіксовані на різних носіях, ідентичні оригіналу (повністю збігаються за всіма ознаками, включно з форматом файлу). Незважаючи на це, Верховний Суд (ВС) в ухвалі за справою № 397/2588/13-к підтримав рішення судів першої та апеляційної інстанції і визнав недопустимим доказом виконаний під час проведення оперативно-розшукових

заходів відео- та аудіозапис факту надання хабаря судді в 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 [6].

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 інформації у первісному вигляді [7, 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 й довідкова література має бути розроблена і внесена до програм підвищення кваліфікації окремо для кожної категорії співробітників.

У Кримінальному процесуальному кодексі (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 цифровою 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 й достовірності цифрового доказу за певними критеріями.

Список використаних джерел

1. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.* 2013. Вип. 5. С. 256–260.

2. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: 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. Київ : УкрНДНЦ, 2018. 31 с.

4. 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.

5. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. Верховний суд України : офіційний сайт. 28 жовтня 2021. URL: 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. URL: http://reyestr.court.gov.ua/Review/74475933.

7. 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.