УДК 343
DOI 10.36919/ELJ.1.2023.64

М. О. Тимошенко,
доктор юридичних наук,
доцент,професор кафедри права,
ПВНЗ «Європейський університет»
ORCID ID 0000-0002-6567-2321;

О. В. Сіренко,
кандидат юридичних наук,доцент,
доцент кафедри кримінального права та процесу,
Державний податковий університет
ORCID ID 0000-0003-2584-5731

ЕЛЕКТРОННІ СЛІДИ ЯК ДЖЕРЕЛО ДОКАЗІВ

Стаття присвячена розгляду електронних слідів як джерела доказів. Встановлено, що слід, який злочинець залишає в інформаційно-телекомунікаційній системі, має ряд унікальних особливостей та існує у формі електронного відображення. Фіксація електронних слідів є досить складним завданням, яке виконують у визначений спосіб залежно від виду електронних слідів та їх змінюваності в часі, обставин виявлення тощо.

Наголошується, що оскільки електронні докази легше змінити чи підробити, ніж традиційні форми доказів, то до них повинні ставитися більш жорсткі вимоги, тому що для їх оцінки потрібні спеціальні пристрої, а також особи, які володіють вузькоспеціалізованими науковими знаннями.

Крім того, враховуючи особливості електронних слідів, зокрема таких як незалежність від матеріального носія, змінюваність у часі, їх оцінка має відбуватися комплексно з іншими доказами у кримінальному провадженні. Водночас оцінка електронних слідів (відображень) має бути всебічною, повною та неупередженою.

Ключові слова: *електронні сліди, докази, криміналістичне дослідження, джерело доказів, матеріальні сліди.*

Постановка проблеми та її актуальність. Із розвитком інформаційних технологій світ постійно розвивається, відбувається оновлення усіх сфер життя. Виникають нові види злочинів, які тісно пов'язанні із застосуванням інформаційних технологій. Смартфони, комп'ютери, портативні пристрої геолокації, відеореєстратори, вебкамери, платіжні системи та ряд інших цифрових (електронних) пристроїв усе частіше використовуються злочинцями, і сліди неправомірних дій залишаються в інформаційному просторі.

Такі сліди мають специфічні умови виникнення, існування, копіювання та зберігання. Також виникають труднощі з їх візуалізацією, гарантованим зберіганням. Водночас електронні сліди як джерело доказів іноді стають єдиною можливістю здійснити правосуддя.

Аналіз останніх досліджень і публікацій. Окремі аспекти використання у доказовому процесі електронних слідів загалом і, зокрема, проблеми їх збирання, вилучення досліджували такі науковці, як: Г. К. Авдєєва, П. Є. Антонюк, С. В. Стороженко, Н. М. Ахтирська, М. В. Гуцалюк, І. А. Смаль, В. Г. Хахановський, Є. С. Хижняк, Д. М. Цехан та інші.

Метою статті є дослідження електронних слідів як джерела доказів.

Виклад основного матеріалу дослідження. Слід, який злочинець залишає в інформаційно-телекомунікаційній системі, має ряд унікальних особливостей, які необхідно встановити й описати на науковому рівні.

По-перше, слід в інформаційно-телекомунікаційній системі фізично існує у вигляді певних змін на магнітному або електронному носієві, який міститься у складі мережевого сервера, окремого комп'ютера, термінала мобільного зв'язку або ж є автономним.

По-друге, особливості «хмарних» технологій, які використовують в інформаційно-телекомунікаційних мережах, передбачають, зокрема, автоматичний (не контрольований людиною) перезапис інформації з одного носія на інший під час обчислювального процесу з метою його оптимізації. Отже, слід в інформаційно-телекомунікаційній мережі в загальному випадку не прив'язаний до конкретного матеріального носія. На відміну від класичного

об'єкта трасології матеріальний слід в елементарному носієві інформації позбавлений будь-яких індивідуальних криміналістичних ознак, які традиційно визначені саме носієм. Такий слід є інформацією в «чистому вигляді».

По-третє, стан окремого елементарного носія інформації не можна вважати слідом у загальноприйнятому значенні, оскільки він сам по собі не містить криміналістичної інформації. Тобто природа матеріальних слідів в інформаційно-телекомунікаційній системі є інтегральною.

По-четверте, кожен матеріальний слід в інформаційно-телекомунікаційній системі, не маючи індивідуальних криміналістичних ознак у класичному їх розумінні, є унікальним через свою інтегральну (комбінаторну) природу. Це дає підстави стверджувати, що матеріальні сліди в інформаційно-телекомунікаційній системі принципово можуть бути використані для виконання завдань із криміналістичної ідентифікації після розроблення відповідних методик [4, с. 16].

На думку Ю. Ю. Орлова, «...на відміну від класичних слідів-відображень, матеріальний слід в інформаційно-телекомунікаційній системі неможливо спостерігати безпосередньо. Людина може сприймати його лише у вигляді віртуальної моделі на екрані комп'ютерного монітора чи монітора термінала мобільного зв'язку» [4, с. 17].

Коли йдеться про електронний слід, здебільшого наголошується не про, власне, слід на матеріальному носієві інформації, а його ідеальне відображення, сформоване електронною схемою комп'ютера. Тобто електронний слід існує у формі електронного відображення.

Оскільки електронні сліди існують виключно в кіберпросторі, який визначено на рівні законодавства як «середовище (віртуальний простір), що надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі «Інтернет» та/або інших глобальних мереж передачі даних» [6].

Саме тому електронні сліди ще називають «віртуальними слідами», хоча з наукової точки зору така назва не є повною мірою коректною.

На думку науковців, це пов'язано з тим, що «...електронний слід не є можливим (тобто таким, що не існує або ж спонтанно зникає). По-перше, він реально існує, як, наприклад, і показання свідка. По-друге, він придатний для відтворення в інформаційно-телекомунікаційній системі в будь-який момент часу. По-третє, його можна зафіксувати (наприклад, у вигляді скриншотів, роздруківок або окремих файлів).

Нематеріальний характер електронних слідів, їхня похідна природа (вони визначаються матеріальними слідами в інформаційно-телекомунікаційній системі), а також незалежність від матеріального носія (здатність до необмеженого копіювання без спотворення змісту) дають підстави віднести їх до категорії ідеальних слідів» [4, с. 17].

Потрібно також звернути увагу на такий момент, як наявність у комп'ютері, терміналі зв'язку чи інформаційно-телекомунікаційній мережі шкідливих комп'ютерних програм (комп'ютерних вірусів), що може позначатися на достовірності електронних відображень як доказів. «Тому, за наявності підстав вважати отримане електронне зображення спотвореним унаслідок впливу комп'ютерних вірусів, слідчий має призначити комп'ютерно-технічну експертизу на предмет відсутності в комп'ютері (сервері, терміналі зв'язку) шкідливих програм» [4, с. 18].

Пошук електронних слідів в окремому (автономному) комп'ютері здійснюють за певними атрибутами, використовуючи, зокрема, опції «Пошук» операційної системи Windows. Також може бути застосовано допоміжні спеціалізовані програми (наприклад, програма автоматичного збору інформації про апаратне і програмне забезпечення комп'ютерного засобу, яка є складовою дистрибутиву Ubuntu 16.04) [5].

Зазначаючи про фіксацію електронних слідів, потрібно наголосити, що це досить складне завдання, яке виконують у визначений спосіб залежно від виду електронних слідів та їх змінюваності в часі, обставин виявлення тощо. Зокрема, фіксацію електронних слідів, які були виявлені в конкретному комп'ютері, можна здійснити шляхом копіювання змісту носіїв інформації за допомогою скриншотів, роздруківки електронних документів, а також використовуючи спеціалізоване програмне забезпечення, тощо.

Коли йдеться про фіксацію електронних слідів в інформаційній мережі, то, як відмічають фахівці, її «здійснювати значно складніше у зв'язку із їх динамічністю (плинністю) і нелокальним характером. У цьому випадку важливо своєчасно зафіксувати певний слід, доки він назавжди не зник з мережі» [5, с. 19].

Потенційна інформація, що міститься в слідах злочину, виявлених в електронних пристроях, телекомунікаційних системах і програмах, актуалізується і перетворюються в доказову інформацію саме шляхом використання спеціальних знань у формі судової експертизи. Адже експертиза є самостійною процесуальною формою одержання нових доказів та уточнення (перевірки) тих, що вже отримані.

Розглядаючи електронні сліди як джерело доказів у кримінальному провадженні, необхідно відмітити, що, відповідно до ст. 84 КПК України, «доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів» [1].

Згідно з ч. 2 ст. 99 КПК України «до документів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (зокрема, комп'ютерні дані).

Матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність», за умови відповідності вимогам цієї статті, є документами та можуть використовуватися в кримінальному провадженні як докази» [1].

Як відмічають науковці, «доказове значення мають електронні зображення, призначені як для передавання відомостей іншим особам (користувачам мережі, абонентам зв'язку), так і для користування самим автором (електронні щоденники, приватні облікові записи тощо). Електронне відображення буде достовірним доказом, якщо його істинність у сенсі відповідності об'єктивній дійсності є встановленою й не викликає розумних сумнівів у чинній парадигмі знань» [8].

Важливими властивостями фактичних даних, які мають значення для кримінального провадження, що надають їм юридичної сили доказів, що можуть використовуватись у кримінальному провадженні, є їх належність та допустимість.

Згідно із ст. 85 КПК України «належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів» [1].

Допустимість доказів – це дозвіл для органу чи посадової особи, яка веде кримінальний процес, внаслідок положень процесуального права використати їх як докази. Допустимість доказу визначається з огляду на обставини його отримання і залучення до справи. Умовами допустимості доказів є: 1) одержання фактичних даних із належного процесуального джерела; 2) одержання фактичних даних належним суб'єктом; 3) одержання фактичних даних у належному процесуальному порядку; 4) належне оформлення джерела фактичних даних [2, с. 132].

Необхідно звернути увагу, що, згідно зі ст. 86 та 87 КПК України, «доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим Кодексом» [1], а недопустимими є «докази, отримані внаслідок істотного порушення прав та свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок істотного порушення прав та свобод людини» [1].

Потрібно також пам'ятати, що електронні докази легше змінити чи підробити, ніж традиційні форми доказів. Саме тому, на думку науковців, до цифрових доказів повинні ставитися більш жорсткі вимоги, оскільки для їх оцінки потрібні спеціальні пристрої, а також особи, які володіють вузькоспеціалізованими науковими знаннями [3, с. 229].

Ю. Ю. Орлов та С. С. Чернявський відмічають, що умови допустимості до «класичного» документа як джерела доказів є такими самими, як і до електронних відображень, що їх сформувала людина: 1) має бути відомим автор документа (установа, організація, підприємство, посадова особа або громадянин); 2) зміст документа має відповідати компетенції і фактичній обізнаності автора. Саме це і дозволяє перевірити доказ. Проте, на їх думку, до тих електронних відображень, що створені інформаційною системою в автоматичному режимі, вимогу про відомість автора як умову допустимості доказу висувати не варто. Водночас у деяких випадках може виявитися потреба у призначенні комп'ютерно-технічної експертизи щодо визначення можливості формування певного електронного

відображення конкретним апаратно-програмним комплексом з метою встановлення належності доказу [8, с. 120].

Д. М. Цехан зауважує, що для забезпечення допустимості «цифрових доказів» необхідно використовувати можливості сучасних судових техніко-криміналістичних експертиз, зокрема: експертизи комп'ютерної техніки і програмних продуктів, інформаційно-комп'ютерної експертизи та комплексної експертизи. Водночас увага експерта має зосереджуватись на виявленні ознак модифікації цифрової інформації, її способів та меж [7, с. 259].

Необхідно звернути увагу на те, що важливим питанням є питання оцінки електронних слідів (відображень) як доказів. Ч. 1 ст. 94 КПК України встановлює, що «слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення» [1].

Враховуючи особливості електронних слідів, зокрема таких як незалежність від матеріального носія, змінюваність у часі, їх оцінка має відбуватися комплексно з іншими доказами у кримінальному провадженні.

Під час оцінки електронних відображень, що містять відомості про факти електронних комунікацій абонентів (користувачів), задля забезпечення достовірності доказів, які не підтверджуються іншими доказами, варто перевірити технічну інформацію, що міститься в електронних пристроях усіх задіяних абонентів, яка має збігатися за своїми параметрами (телефонні номери або IP-адреси абонентів, дата, час, тривалість комунікації).

У процесі оцінки електронних відображень варто з'ясовувати: 1) походження електронного відображення та час його створення (на якому комп'ютері було створено, хто є автором (укладачем), коли було створено і коли вносилися зміни); 2) справжність (автентичність) електронного відображення та його належність до кримінального провадження (чи відповідає задекларована належність електронного відображення юридичній чи фізичній особі фактичній належності, чи відповідає реальна діяльність, що здійснюється шляхом застосування електронного відображення, проголошеній на цьому відображенні, чи має значення електронне відображення до кримінального провадження); 3) джерело обізнаності особи, яка сформувала електронне відображення; 4) дотримання під час створення електронного відображення вимог закону (чи підлягає це відображення офіційній реєстрації та чи зареєстроване воно, чи підлягає ліцензуванню діяльність, що ведеться із застосуванням електронного відображення, і чи видано ліцензію); 5) наявність інших даних, що підтверджують достовірність змісту електронного відображення; 6) відомості про інтернет-провайдера, на серверах якого зберігається електронне відображення [8, с. 122].

Як і за оцінки інших доказів, оцінка електронних слідів (відображень) має бути всебічною, повною та неупередженою.

Висновки. Отже, до електронних слідів як джерела доказів необхідно висувати більш суворі вимоги щодо допустимості, що пов'язано з більш легкими способами їх підробки. Крім того, з точки зору належності вони повинні прямо або опосередковано підтверджувати факти й обставини, які мають значення для кримінального провадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 22.11.2023).

2. Лобойко Л. М. Кримінальний процес : підручник. Київ : Істина, 2014. 432 с. URL : https://www.osce.org/files/f/documents/9/2/358176.pdf (дата звернення: 22.11.2023).

3. Метелев О. П. Проблеми визначення допустимості і належності електронних (цифрових) доказів у кримінальному процесі. Вісник кримінального судочинства. 2019. № 3. С. 224–238. URL : https://vkslaw.knu.ua/ images/verstka/3_2019_METELEV.pdf (дата звернення: 22.11.2023).

4. Орлов Ю. Ю. Електронне відображення як криміналістичний об'єкт. Науковий вісник Національної академії внутрішніх справ. 2019. № 4 (113). С. 15–23. URL : http://elar.naiau.kiev.ua/bitstream/123456789/17509/1/ %D0%9D%D0%92%204%2819%29_p015-023.pdf (дата звернення: 22.11.2023).

5. Особливості використання електронних цифрових доказів у кримінальних провадженнях : метод. рек. / за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 70 с.

6. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL : https://zakon.rada.gov.ua/ laws/show/2163-19#Text (дата звернення: 22.11.2023).

7. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. Науковий вісник Міжнародного гуманітарного університету. Серія: «Юриспруденція». 2013. № 5. С. 256–260. URL : https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc5/56.pdf (дата звернення: 22.11.2023).

8. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. Вісник кримінального судочинства. 2017. № 2. С. 112–124. URL : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=vkc_2017_2_16 (дата звернення: 22.11.2023).

REFERENCES

1. Kryminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine] : Zakon Ukrainy vid 13.04.2012 № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text (data zvernennia: 22.11.2023) [in Ukrainian].

2. Loboiko L. M. (2014). Kryminalnyi protses [Criminal process] : pidruchnyk. Kyiv : Istyna. 432 p. URL : https://www.osce.org/files/f/documents/ 9/2/358176.pdf (data zvernennia: 22.11.2023) [in Ukrainian].

3. Metelev O. P. (2019). Problemy vyznachennia dopustymosti i nalezhnosti elektronnykh (tsyfrovykh) dokaziv u kryminalnomu protsesi [Problems of determining the admissibility and appropriateness of digital (electronic) evidence in criminal proceedings]. Visnyk kryminalnoho sudochynstva. № 3, pp. 224–238. URL : https://vkslaw.knu.ua/images/verstka/3_2019_METELEV.pdf (data zvernennia: 22.11.2023) [in Ukrainian].

4. Orlov Yu. Yu. (2019). Elektronne vidobrazhennia yak kryminalistychnyi obiekt [Electronic Display as a Forensic Object]. Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav. № 4 (113), pp. 15–23. URL : http://elar.naiau.kiev.ua/ bitstream/123456789/17509/1/%D0%9D%D0%92%204%2819%29_p015-023.pdf (data zvernennia: 22.11.2023) [in Ukrainian].

5. Osoblyvosti vykorystannia elektronnykh tsyfrovykh dokaziv u kryminalnykh provadzhenniakh [Features of the use of electronic digital evidence in criminal proceedings] : metod. rek. / za zah. red. M. V. Hrebeniuka. Kyiv : MNDTs pry RNBO Ukrainy, 2017. 70 p.

6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the basic principles of cyber security] : Zakon Ukrainy vid 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia: 22.11.2023) [in Ukrainian].

7. Tsekhan D. M. (2013). Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia [Digital evidence: concepts, characteristics and place in the proof system]. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: «Yurysprudentsiia». № 5, p. 256–260. URL : https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc5/56.pdf (data zvernennia: 22.11.2023) [in Ukrainian].

8. Cherniavskyi S. S., Orlov Yu. Yu. (2017). Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni [Electronic display as a source of evidence in criminal proceedings]. Visnyk kryminalnoho sudochynstva. № 2, pp. 112–124. URL : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64. exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=vkc_2017_2_16 (data zvernennia: 22.11.2023) [in Ukrainian].

M. O. Tymoshenko, O. V. SIRENKO ELECTRONIC TRACES AS A SOURCE OF EVIDENCE

The article is devoted to consideration of electronic traces as a source of evidence. It has been established that the trace left by the criminal in the information and telecommunications system has a number of unique features and exists in the form of an electronic display. The fixation of electronic traces is a rather complex task, which is performed in a certain way depending on the type of electronic traces and their variability over time, the circumstances of detection, etc.

It is emphasized that since electronic evidence is easier to change or falsify than traditional forms of evidence, it should be subject to stricter requirements, as it requires special devices and people with highly specialized scientific knowledge to evaluate it.

In addition, taking into account the peculiarities of electronic traces, in particular, such as independence from a material medium, changeability over time, their evaluation should be carried out in a complex manner with other evidence in criminal proceedings. At the same time, the assessment of electronic traces (images) should be comprehensive, complete and impartial.

Keywords: *electronic traces, evidence, forensic investigation, source of evidence, material traces.*