УДК 343.1
DOI 10.33244/2617-4154.1(10).2023.226-233

А. М. Лазебний,
канд. юрид. наук, доцент,
Державний податковий університет
e-mail: a_lazebna15@ukr.net
ORCID ID 0000-0001-9812-6151

СУТНІСТЬ ТА ЗНАЧЕННЯ ЕЛЕКТРОННИХ СЛІДІВ У КРИМІНАЛІСТИЦІ

Стаття присвячена дослідженню сутності електронних слідів у криміналістиці, визначено поняття цього терміна. Розгляд питання стає закономірним наслідком розвитку інформаційних технологій, глобального впровадження в усі аспекти життєдіяльності людини. Людина більшою чи меншою мірою існує одночасно в двох просторах – реальному і віртуальному. У зв'язку з цим актуальним завданням сучасної криміналістики стають питання електронних слідів та виконання діагностичних завдань, які стоять як перед кожним криміналістом окремо в процесі розслідування злочинів, так і перед криміналістикою як наукою в цілому.

Новітні інформаційні технології викликали появу і подальший стрімкий розвиток нових форм злочинності, а саме злочинів, що вчиняються шляхом використання таких технологій, завдяки чому вони отримали назву кіберзлочинів.

Електронні сліди є новим об'єктом криміналістичного дослідження, а електронна техніка надає цій інформації значення джерела доказів. При цьому комп'ютерна техніка, інформаційні технології та окремі програмні продукти можуть слугувати як засобом вчинення злочинів, так і предметом злочинного посягання. Характер слідової картини кіберзлочинів залежить від способів їх вчинення та характеристик електронних засобів, за допомогою яких здійснюються злочинні посягання. Електронний слід має певну систему ознак у вигляді окремих інформаційних елементів, які можуть бути записані як на одному, так і на декількох носіях цифрової інформації. Носії електронних слідів можуть бути одночасно підключені до декількох цифрових пристроїв, об'єднаних, наприклад, у телекомунікаційну мережу.

На сайтах соціальних мереж (наприклад, Facebook, Twitter, LinkedIn, Instagram) можна виявити електронні сліди у вигляді повідомлень і коментарів осіб, що перевіряються, їх персональних даних (наприклад, електронну адресу), фотознімків і відеозаписів, історію пошукових запитів та ін. Ці сліди містять інформацію про час відвідування сайтів, деякі персональні дані користувача (наприклад, електронну адресу), за якими можна здійснити пошук його номера телефону, дати народження, місця роботи та проживання, визначити коло спілкування та інтереси. Останні 2–3 роки спостерігається стрімке зростання правопорушень у системах дистанційного банківського обслуговування (ДБО). ДБО – це комплекс сервісів віддаленого доступу

клієнтів до банківських послуг, в основному за допомогою комп'ютерних або телефонних мереж. При цьому клієнт віддалено (без візиту в банк) передає необхідні розпорядження, використовуючи інформаційні технології.

Ключові слова: *електронні сліди, цифрові сліди, кіберзлочини.*

Постановка проблеми. Закономірним наслідком розвитку інформаційних технологій стає їх глобальне впровадження в усі аспекти життєдіяльності людини. Людина більшою чи меншою мірою існує одночасно в двох просторах – реальному і віртуальному. Якщо перший був предметом вивчення криміналістики впродовж усього часу її існування, то другий все ще перебуває на стадії усвідомлення необхідності його дослідження та поступового освоєння.

Будучи частиною суспільного життя, віртуальний простір стає частиною злочинного світу, де накопичені криміналістикою знання є недостатніми для виконання завдань кримінального провадження. У зв'язку з цим актуальним завданням сучасної криміналістики стають питання електронних слідів та виконання діагностичних завдань, які стоять як перед кожним криміналістом окремо в процесі розслідування злочинів, так і перед криміналістикою як наукою в цілому.

Новітні інформаційні технології викликали появу і подальший стрімкий розвиток нових форм злочинності, а саме злочинів, що вчиняються шляхом використання таких технологій, завдяки чому вони отримали назву кіберзлочинів [2, с. 10]. Останнім часом збільшилася кількість кібератак на енергетичні та транспортні структури, банки, окремі державні та приватні установи.

Мета статті. Дослідити сутність електронних слідів як новий вид слідів у криміналістиці та формування визначення терміна «цифровий електронний слід».

Науковці активно дискутують не лише щодо сутності слідів злочинів у сфері використання інформаційних технологій, а й щодо їх найменування.

Запропоновано такі найменування слідів цієї категорії: комп'ютерні сліди, віртуальні сліди, електронно-цифрові, інформаційні, комп'ютерно-технічні тощо. Найбільш вдалим та таким, що адекватно віддзеркалює сутність слідів злочинів такої категорії є найменування «електронні сліди», запропоноване низкою російських та вітчизняних вчених [3, с. 242].

Виклад основного матеріалу. Електронні сліди є новим об'єктом криміналістичного дослідження, а електронна техніка надає цій інформації значення джерела доказів. При цьому комп'ютерна техніка, інформаційні технології та окремі програмні продукти можуть слугувати як засобом вчинення злочинів, так і предметом злочинного посягання. Характер слідової картини кіберзлочинів залежить від способів їх вчинення та характеристик електронних засобів, за допомогою яких здійснюються злочинні посягання. Електронний слід має певну систему ознак у вигляді окремих інформаційних елементів, які можуть бути записані як на одному, так і на декількох носіях цифрової інформації. Носії електронних слідів можуть бути одночасно підключені до декількох цифрових пристроїв, об'єднаних, наприклад, у телекомунікаційну мережу.

Основою механізму утворення електронних слідів слугують електромагнітні взаємодії двох і більше матеріальних об'єктів, кожен з яких є сукупністю електронного цифрового пристрою (комплексу пристроїв) і системи управління ним (набору програмних продуктів). Об'єкти, які утворюють і сприймають електронні сліди, мають об'єктивну форму існування. Сліди впливу однієї об'єктивної форми існування цифрової інформації на іншу можуть бути виявлені, зафіксовані і вивчені лише за допомогою певних цифрових електронних пристроїв.

За аналогією, об'єктивну форму існування слідів впливу високої температури на лезо ножа можливо вивчати лише за допомогою спеціальних металографічних мікроскопів [1, с. 172].

Основними об'єктами, які утворюють і сприймають електронні цифрові сліди, є такі: машинні носії цифрової інформації, інтегральні мікросхеми, мікроконтролери, ЕОМ і їх системи, обладнання телекомунікаційних мереж, цифрові фотокамери та диктофони, пристрої для зчитування інформації з пластикових банківських карт, мобільні телефони, планшети тощо. Крім того, що в них зафіксовані електронні цифрові сліди, пов'язані з подією злочину, окремі електронні модулі цих засобів дозволяють зафіксувати місце і час перебування пристрою у кожний конкретний момент. Зокрема, за допомогою системи геолокації в режимі реального часу можна визначити точне місцезнаходження конкретного комп'ютера, планшета або мобільного телефону і, відповідно, його власника. Дані геолокації також можуть бути використані для встановлення факту одночасної присутності двох і більше осіб в одному місці, а неодноразове повторення таких фактів свідчить про їх взаємодію.

Електронні сліди також утворюються внаслідок зовнішнього доступу до комп'ютерних систем з метою знищення або копіювання інформації, модифікації баз даних, блокування роботи системи. Такими слідами є видалення з каталогів імен файлів, видалення або додавання окремих записів, фізичне руйнування або розмагнічування носіїв, перейменування каталогів і файлів, зміна розмірів вмісту файлів, зміна атрибутів файлів, поява нових каталогів і файлів, зміна інформації про час останнього доступу до інформації, результати роботи антивірусних і тестових програм тощо. Вони можуть бути виявлені під час експертного дослідження комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду та ін.

Час роботи користувача в інтернеті можна встановити за спеціальним log-файлом (журналом). Додаткові відомості про вид, порядок і час підключень користувача до мережі і збіг цих даних з log-файлом провайдера може слугувати вагомим доказом несанкціонованого доступу до певної комп'ютерної системи.

Сліди неправомірного доступу до інформації містяться в журналах операційних систем і окремих програмних продуктів, які створюють резервні копії файлів і файли-звіти, зберігають інформацію про останні проведені операції та виконані програми, а також містять іншу інформацію, що має значення для розслідування злочину [1, с. 174]. Важливу криміналістично-значущу інформацію можна отримати під час вивчення даних електронного листування і сервісів обміну смс-повідомленнями. В атрибутах

файлів електронних листів міститься дата і час відправлення, електронна адреса відправника, найменування та адреса інтернет-провайдера та інша інформація. Телефонні дзвінки з мобільного телефону і тексти смс-повідомлень автоматично фіксуються і накопичуються на сервері оператора мобільного зв'язку. У багатьох випадках саме ці сліди дозволяють встановити організаційні злочинні схеми.

На сайтах соціальних мереж (наприклад, Facebook, Twitter, LinkedIn, Instagram та ін.) можна виявити електронні сліди у вигляді повідомлень і коментарів осіб, які перевіряються, їх персональних даних (наприклад, електронну адресу), фотознімків і відеозаписів, історію пошукових запитів тощо. Ці сліди містять інформацію про час відвідування сайті, в деякі персональні дані користувача (наприклад, електронну адресу), за якими можна здійснити пошук його номера телефону, дати народження, місця роботи та проживання, визначити коло спілкування та інтереси.

Останні 2–3 роки спостерігається стрімке зростання правопорушень у системах дистанційного банківського обслуговування (ДБО). ДБО – це комплекс сервісів віддаленого доступу клієнтів до банківських послуг, в основному за допомогою комп'ютерних або телефонних мереж. При цьому клієнт віддалено (без візиту в банк) передає необхідні розпорядження, використовуючи інформаційні технології [1, с. 175]. Системи ДБО в Україні розподіляються на такі види: система «Клієнт-банк» (PC-banking, remote banking, direct banking, home banking); інтернетбанкинг; мобільний банкинг. Шахрайська схема розкрадання грошових коштів складається з трьох основних етапів: отримання конфіденційної інформації для здійснення неправомірного доступу в систему ДБО, проведення шахрайської операції від імені користувача з використанням його авторизаційних даних і ключів електронних засобів захисту, отримання грошових коштів. Для розкрадання персональних (авторизаційних) даних користувача системи ДБО (логіна, пароля і ключів підпису) правопорушники часто використовують спеціальне шкідливе програмне забезпечення. Найчастіше це – модифікації добре відомих троянських програм з додатковими функціями, що дозволяють після певних неправомірних дій повністю «самоліквідуватися» без можливості відновлення.

На сьогодні активно здійснюється побудова міжнародної системи боротьби з такими видами злочинів, об'єднуються необхідні кадри, розробляються методики розслідування злочинів цієї категорії, уточнюються процедури взаємодії з міжнародними структурами і правоохоронними органами різних країн (наприклад, за допомогою телекомунікаційних засобів і систем).

Зазначимо, що електронні сліди залишаються в різних інформаційних базах даних, наприклад у базах операторів мобільного зв'язку; під час використання кредитних, дисконтних карт, проїзних документів, персональних комп'ютерів, засобів стільникового зв'язку та інших пристроїв, асортимент яких стрімко розширюється. У зв'язку з цим сучасний правоохоронець просто зобов'язаний грамотно використовувати цифрові сліди в інтересах установлення обставин кримінального правопорушення. Виявлення, фіксація, розшифровка таких слідів сприяє розкриттю і розслідуванню кримінальних правопорушень. У криміналістичній науці і практиці віртуальні сліди розглядаються двояко, з огляду на їх специфічність їх не можна віднести ні до

матеріальних, ні до ідеальних. На нашу думку, електронні сліди являють собою сукупність інформації про діяльність користувача інформаційно-телекомунікаційного середовища під час перебування в електронно-віртуальному просторі.

Цифровий слід можна розглядати як діяльність особи у віртуальному просторі [5, с. 67]. Очевидно, що виявлення, фіксація і вилучення електронних слідів кримінального правопорушення потребує використання спеціальних знань і технологій, розробка та вдосконалення яких упродовж останніх кількох років представляє виключно актуальний напрям криміналістики.

Доцільно зазначити про існування самостійного підрозділу криміналістичної техніки – криміналістичного дослідження електронних носіїв інформації та цифрових слідів [7, с. 81]. Цей розділ повинен забезпечити однаковість у роботі відповідних посадових осіб, які стикаються з указаною категорією об'єктів.

На думку О. О. Двойнікова, у разі виявлення факту розміщення забороненої інформації в глобальній мережі правоохоронними органами, під час фіксування готуються такі документи, що підтверджують факт знаходження протиправного контенту на сайті: 1) рапорт (лист) працівника органів внутрішніх справ про виявлення та встановлення наявності знаходження протиправної інформації на сайті; 2) протокол зі скріншотами (копії сторінки сайту з екрана), що підтверджує наявність протиправної інформації на сайті; 3) документ (файл) для перегляду сторінки сайту в режимі онлайн; 4) додається посилання на сторінку сайту у каталозі обраного в Microsoft Internet Explorer; 5) створюється копія сторінки сайту на жорсткому диску за допомогою спеціальної утиліти; 6) готується інформаційна довідка про ідентифікаційні дані сайту (IP-адреса, URL), інтернет-провайдера (електронна адреса, номери телефонів) тощо [9, с. 221].

Під час огляду вебсайту у разі відсутності в слідчого спеціальних знань слідчий повинен залучати до огляду відповідного спеціаліста.

У протоколі огляду варто зазначати серійний номер службового комп'ютера, назву та версію операційної системи, яка встановлена на даному комп'ютері, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі «Інтернет» [10, с. 187].

Електронним слідам варто відвести окреме місце у переліку всіх слідів, які вивчаються у криміналістиці, а також визначитись з єдиною загальновизнаною класифікацією віртуальних слідів.

Наука криміналістика як першорядна основа протидії злочинності орієнтована на вивчення механізму вчинення того чи іншого виду кримінального правопорушення у сфері інформаційно-телекомунікаційної спрямованості, пошук доказової бази і відображення відповідних об'єктів у матеріальних слідах. У зв'язку з розвитком інноваційних технологій необхідним стає розвиток нового напряму криміналістичної ідентифікації, пов'язаного з ідентифікацією технічних засобів за залишеними цифровими слідами [6, с. 249].

Кінцева мета такої ідентифікації – встановлення даних про особу, яка використала відповідний технічний засіб. Крім того, визначити відповідність інформації, що міститься на різних електронних носіях, або наявність на носії інформації із заданими

характеристиками не є можливим за допомогою традиційних видів криміналістичної ідентифікації.

Отже, розслідування злочину за електронними слідами є новим та актуальним напрямом криміналістики. Найголовнішим та найскладнішим завданням, яке стоїть перед слідчим у процесі розслідування злочину, є ідентифікація особистості злочинця за електронними слідами.

Основними перешкодами у цьому є відсутність комплексних наукових досліджень у такому напрямі, недостатність спеціальних знань у слідчих та працівників оперативних підрозділів, а також дії самих злочинців, які приховують такі сліди.

Тому в процесі встановлення особистості злочинця слідчий повинен використовувати облікові дані, які особа залишила за собою в мережі. Пошукові системи, відкриті бази даних, соціальні мережі стають одним із головних джерел криміналістичної інформації, на підставі якої встановлюється особистість злочинця, його психофізіологічні риси, соціальний статус, місцезнаходження тощо. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою інформаційних та телекомунікаційних технологій.

Об’єктами кіберзлочинів є персональні дані, банківські рахунки, паролі та інша інформація не лише окремих фізичних і юридичних осіб, а й державних структур: енергетичних об’єктів, транспортних та банківських установ. Тому дослідження сутності поняття «електронний слід» та визначення терміна «цифровий електронний слід» є досить важливим для визначення їх ознак та шляхів пошуку.

Електронний слід – це ідеальне електронне відображення (статичне чи динамічне) на моніторі обчислювального пристрою (комп’ютера, термінала, мобільного зв’язку тощо) матеріального сліду в інформаційно-телекомунікаційній системі. Сліди в елементарних носіях інформаційно не мають індивідуальних криміналістичних ознак. Проте їхня інтегральна (комбінаторна) природа дає підстави стверджувати, що матеріальні сліди в інформаційно-телекомунікаційній системі та створювані ними електронні сліди набувають цих ознак і можуть бути придатними для криміналістичної ідентифікації. Виявлення та фіксацію електронних слідів здійснюють за спеціальними методиками шляхом застосування програмного забезпечення загального та спеціального призначення. Наявні проблеми щодо виявлення та фіксації електронних слідів потребують законодавчого врегулювання. Електронні відображення мають загальні й окремі ідентифікуючі ознаки. Водночас ідентичні електронні сліди можуть мати відмінності в окремих ознаках через їх динамічну природу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдеева Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2017. № 1(77). С. 169–176.

2. Шило О. Г. Проблемні питання досудового розслідування злочинів, учинених із застосуванням комп’ютерних технологій та/або використанням мережі «Інтернет». *Міжнародні стандарти з кібербезпеки та їх застосування в Україні:* матеріали круглого столу, м. Харків, 19 квіт. 2016 р. Х.: Право, 2016. С. 10–13.

3. Веліканов С. В. До поняття електронного сліду в криміналістиці. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення:* матеріали постійно діючого науково-практичного семінару. Х.: Право, 2015. Вип. 7. С. 241–244.

4. Орлов Ю. Ю. Електронне відображення як криміналістичний об'єкт. *Науковий вісник Національної академії внутрішніх справ*. 2019. Випуск 4 (ИЗ). С. 15–23.

5. Використання електронних (цифрових) доказів у кримінальному провадженні: методич. рекомен. / Гребенюк М. В., Гавловський В. Д., Гуцалюк М. В., Хахановський В. Г. та ін. Київ: МНДЦ при РНБО України, 2017. С. 61–75.

6. Алєксєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247–253.

7. Заєць І. С. Перспективи криміналістики в умовах інформатизації суспільства. *Матеріали ОРД круглого столу*. С. 77–84.

8. Гринько Л. П. Електронні сліди як актуальний напрямок криміналістичних досліджень / МЦНД. Чернівці, 2020. С. 51–53.

9. Двойніков О. О. Кримінально-процесуальні особливості встановлення особи, яка вчинила злочин за допомогою інтернет-сайту. *Актуальні питання розслідування кіберзлочинів:* матеріали Міжнародної науково-практичної конференції. 2013. С. 218–222.

10. Коваленко А. М. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України*. 2017. № 1. С. 182–191.

REFERENCES

1. Avdeeva G. K., Storozhenko S. V. Electronic traces: concepts and types. *Bulletin of LDUVS named after E. O. Didorenko.* 2017. No 1 (77). Pp. 169–176.

2. Shilo O. G. Problematic issues of pre-trial investigation of crimes committed with the use of computer technology and/or the Internet. *International cybersecurity standards and their application in Ukraine*: proceedings of the round table in Kharkiv, April 19. 2016. X.: Law, 2016. Pp. 10–13.

3. Velikanov S. V. To the concept of electronic footprint in criminology. *Pre-trial investigation: current problems and ways to solve them*: proceedings of the permanent scientific-practical seminar. X.: Law, 2015. Vip. 7. Pp. 241–244.

4. Orlov Yu. Yu. Electronic mapping as a forensic object. *Scientific Bulletin of the National Academy of Internal Affairs*. 2019. Issue 4 (FROM). Pp. 15–23.

5. The use of electronic (digital) evidence in criminal proceedings: methodical. recommend / Grebenyuk M. V., Gavlovsky V. D., Gutsalyuk M. V., Khakhanovsky V. G. etc. Kyiv: MNDC at the National Security and Defense Council of Ukraine, 2017. P. 61–75.

6. Alekseeva-Protsyuk D. O., Briskovskaya O. M. Electronic evidence in criminal proceedings: concepts, features and problematic aspects of application. *Scientific Bulletin of Public and Private Law*. 2018. Vip. 2. Pp. 247–253.

7. Hare I. S. Perspectives of criminology in the conditions of informatization of society. *ORD materials of the round table*. Pp. 77–84.

8. Grinko L. P. Electronic traces as a topical area of forensic research / ICND. Chernivtsi, 2020. S. 51–53.

9. Dvoinikov O. O. Criminal-procedural features of identification of the person who committed the crime with the help of the Internet site. *Current issues of cybercrime investigation:* proceedings of the international scientific-practical conference. 2013. Pp. 218–222.

10. Kovalenko A. M. Features of tactics of reviewing electronic documents during the pre-trial investigation of encroachments on the life and health of a journalist. *Bulletin of the National Academy of Legal Sciences of Ukraine*. 2017. № 1. Pp. 182–184.

A. Lazebny. The Essence and Significance of Electronic Traces in Criminology

Consideration of the issue becomes a natural consequence of the development of information technology, global implementation in all aspects of human life. Man to a greater or lesser extent exists simultaneously in two spaces - real and virtual. before criminology as a science in general.

The latest information technologies have caused the emergence and further rapid development of new forms of crime, namely crimes committed through the use of such technologies, which is why they are called cybercrime.

Electronic traces are a new object of forensic research, and electronic technology gives this information the value of a source of evidence. At the same time, computer technology, information technology and certain software products can serve as a means of committing crimes and the subject of criminal encroachment. The nature of the trace picture of cybercrime depends on the methods of their commission and the characteristics of electronic means by which criminal encroachments are carried out. The electronic footprint has a certain system of features in the form of separate information elements that can be recorded on one or more digital media. Electronic footprints can be connected to multiple digital devices connected to, for example, a telecommunications network.

On social networking sites (for example, Facebook, Twitter, LinkedIn, Instagram) you can find electronic traces in the form of messages and comments of persons being checked, their personal data (eg email address), photos and videos, search history, etc. These traces contain information about the time of visiting the site, some personal data of the user (for example, e-mail address), which can be used to search for his phone number, date of birth, place of work and residence, identify communication and interests. The last 2-3 years there has been a rapid increase in offenses in remote banking (DBO) systems. DBO is a set of services for remote access of clients to banking services, mainly through computer or telephone networks. At the same time, the client remotely (without visiting the bank) transmits the necessary instructions using information technology.

Key words: *electronic traces, digital traces, cybercrimes.*

Стаття надійшла до редколегії 9 січня 2023 року