УДК 343.98
DOI https://doi.org/10.32782/2524-0374/2023-10/114

ЦИФРОВІ СЛІДИ: ПОНЯТТЯ ТА ЇХ ЗНАЧЕННЯ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

DIGITAL TRACES: CONCEPTS AND THEIR MEANING IN THE INVESTIGATION OF CRIMINAL OFFENSES

Колеснікова І.А., к.ю.н.,
асистентка кафедри криміналістики
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена дослідженню концепції цифрових слідів та їх значення у розслідуванні кримінальних правопорушень. Звернуто увагу, що цифрові сліди являють собою сліди вчинення будь-яких дій в інформаційному просторі комп'ютерних та інших цифрових пристроїв, їх систем та мереж. Визначено види цифрових слідів, наголошено на відмінностях цифрових слідів від електронних доказів. Акцентовано увагу на важливості визнання електронних доказів окремим джерелом доказування у кримінальному провадженні, а їх метаданих як супутніх доказів, що можуть бути виявлені, зібрані, досліджені й використані, як цифрові сліди.

Проведено аналіз методології та техніки, яка використовується для виявлення, збирання, дослідження й використання цифрових слідів. Звернуто увагу на сучасні можливості судової експертизи у дослідженнях цифрових доказів, включаючи судове програмне забезпечення, методи відновлення даних та аналізу шифрування. Досліджено питання допустимості цифрових доказів у суді, проблеми приватності та етичності, які виникають у роботі з особистою інформацією. Звернуто увагу на правові межі та принципи, яким має відповідати діяльність щодо виявлення, збирання, дослідження й використання цифрових доказів у кримінальних провадженнях. Акцентовано увагу на практичному значенні розуміння сутності цифрових слідів для правоохоронних органів у боротьбі зі злочинністю під час пізнання події злочину, установлення винуватців і фактів доказування.

Запропонована стаття надає всебічне уявлення про сутність та види цифрових слідів, їх ознак, особливості виявлення, збирання, дослідження та використання їх під час розслідування та розкриття кримінальних правопорушень.

Ключові слова: цифрова криміналістика, цифрові сліди, розслідування кіберзлочинів, інформаційно-телекомунікаційні технології, спеціальні знання, судова експертиза.

The article is dedicated to investigating the concept of digital traces and their significance in investigating criminal offenses. It is emphasized that digital traces are the trail of any actions taken in the information space of computers and other digital devices, their systems, and networks. The types of digital traces are defined, and the differences between digital traces and electronic evidence are highlighted. The importance of recognizing electronic evidence as a separate source of proof in criminal proceedings is emphasized, and their metadata is recognized as accompanying evidence that can be discovered, collected, researched, and used as digital traces.

An analysis of the methodology and techniques used to discover, collect, research, and utilize digital traces is conducted. Attention is drawn to the modern capabilities of forensic expertise in investigating digital evidence, including forensic software, data recovery methods, and encryption analysis. The admissibility of digital evidence in court, privacy issues, and ethical considerations that arise when dealing with personal information are examined. The legal limits and principles governing the activities of discovering, collecting, researching, and utilizing digital evidence in criminal investigations are emphasized. The practical significance of understanding the essence of digital traces for law enforcement agencies in combating crime and determining the perpetrators and facts of evidence is highlighted.

The proposed article provides a comprehensive understanding of the essence and types of digital traces, their characteristics, and the specifics of discovering, collecting, researching, and utilizing them in the investigation and disclosure of criminal offenses.

Key words: digital forensics, digital traces, cybercrime investigation, information and telecommunications technologies, specialized knowledge, forensic examination.

Важливим інноваційним напрямком у розвитку криміналістики та судової експертизи є дослідження концепції цифрових слідів та їх значення під час розслідування кримінальних правопорушень. Практично безмежні можливості глобальної мережі Інтернет у сфері передачі та обробки інформації, з одного боку, зробили мережу Інтернет найсприятливішим середовищем для розвитку суспільних відносин, з іншого боку, призвели до зростання кількості кіберзлочинів та інших правопорушень, пов'язаних з використанням електронно-обчислювальних пристроїв. Розуміння сутності цифрових слідів кримінальних правопорушень зумовлює можливість подальшої розробки практичних рекомендацій щодо їх виявлення, збирання, дослідження й використання у кримінальному провадженні.

Цифрові сліди кримінальних правопорушень, що можуть бути отримані з персональних комп'ютерів фізичних та юридичних осіб; мобільних пристроїв, планшетів, фотоапаратів та відеокамер, вилучених в учасників кримінального провадження; із серверів та інших накопичувачів інформації в організаціях та установах; з мережевих сервісів, що встановлюють голосовий та відеозв'язок між комп'ютерами через інтернет, такі як ICQ, Skype, WhatsApp, Viber, Telegram та інші; з банківських систем на відповідних цифрових носіях (SD-диски, флеш-картки та ін.); з камер відеоспостереження різних комерційних та державних структур та інших електронно-обчислювальних пристроїв є джерелами доказової та орієнтуючої інформації. Ці дані мають суттєве значення під час пізнання події злочину, установлення винуватців і фактів доказування. Цифрові сліди можуть містити широкий спектр інформації, включаючи дані про комунікацію, місцезнаходження, активності в Інтернеті, файли, повідомлення, електронну пошту та міститися в інформаційних (автоматизованих) системах, телекомунікаційних системах та інформаційно-телекомунікаційних системах. Дослідження цифрових слідів слідчим, прокурором, слідчим суддею і судом при здійсненні відповідно розслідування або судового провадження дозволяє встановити обставини вчиненого кримінального правопорушення та осіб, які його вчинили. Тому на сьогодні проблеми використання цифрових слідів у досудовому розслідуванні набувають вкрай важливого значення для правоохоронних органів у боротьбі зі злочинністю.

Проблемам пізнання сутності цифрових слідів присвячували свої праці такі науковці, як Г. К. Авдєєва, В. Д. Басай, Я. Найдьон, Ю. Ю. Нізовцев, І. О. Крицька, О. А. Парфило, Є. С. Хижняк, Д. М. Цехан, В. М. Шевчук, В. Ю. Шепітько та інші.

Поряд із терміном «цифрові сліди» у юридичній літературі використовують також інші, наприклад: «віртуальні

сліди», [1; 2; 3], «електронні сліди, електронні докази, [4, с. 148; 5, с. 657; 6] тощо.

Так, Є.С. Хижняк використовує термін «віртуальні сліди» та розуміє під ними будь-які зміни комп'ютерної інформації, пов'язані з подією злочину, зафіксовані на матеріальних носіях комп'ютерної техніки [1; с. 423]. З нашої точки зору, термін «віртуальні сліди» є не досить вдалим з точки зору семантики слова «віртуальний». Відповідно до тлумачних словників, віртуальний (від лат. *virtualis* – можливий) – це умовний, уявний, реально не існуючий [7]. Отже, сліди, які є уявними та які реально не існують не можуть бути досліджені слідчим, прокурором, слідчим суддею та судом при здійсненні відповідного розслідування або судового провадження та, тим більше, не можуть бути визнані доказом, оскільки суперечать вимогам ст. 84 КПК України.

Інші науковці використовують термін «електронні сліди». Дійсно, у більшості випадках інформація зберігається, обробляється та передається саме в електронному вигляді. Але не завжди, наприклад, в оптоволоконних телекомунікаційних системах для зберігання та, відповідно, передавання інформації використовуються властивості світлового потоку. Тому, зважаючи на зазначене, найбільш вдалим є термін «цифрові сліди» .

Саме дефініцію «цифрові сліди» науковці визначають як невидимі матеріальні сліди, що містять у собі криміналістично-значущу інформацію, що відтворюється у цифровій формі на матеріальних носіях та можуть бути виявлені за допомогою спеціальних криміналістичних знань [8, с. 91]. Тому цифрові сліди являють собою сліди вчинення будь-яких дій в інформаційному просторі комп'ютерних та інших цифрових пристроїв, їх систем та мереж.

Вважаємо, що при формуванні поняття цифрового сліду слід виходити з таких характеристик цього явища: по-перше, цифрові сліди – це інформація, що міститься на матеріальних цифрових пристроях; по-друге, для аналізу цієї інформації необхідні спеціальні криміналістичні знання з застосуванням комп'ютерних технологій; по-третє, цифрові сліди як інформація містять дані про вчинені кримінальні правопорушення.

До основних властивостей цифрових слідів належить відсутність нерозривного зв'язку з матеріальним носієм, динамічність – можливість перенесення в просторі, можливість моментального знищення таких слідів та можливість створювати ідентичні копії таких слідів.

У теорії криміналістики є різні думки про те, на які види варто поділяти цифрові сліди. Так, Mary Madden, Susannah Fox, Aaron Smith, Jessica Vitak класифікують цифрові сліди на пасивні та активні [9]. Пасивні сліди відображують активності користувача в Інтернеті та інформацію, що зберіглася у вигляді файлів cookie після відвідування вебсайтів, дій щодо пошуку, онлайн-покупок тощо. Активні сліди є результатом публікацій або зміни інформації користувачем на веб-сайтах, створення дописів у соціальних мережах, публікації повідомлень, завантаження відео або зображень у групах WhatsApp, Viber, Telegram тощо.

Інші науковці цифрові сліди класифікують за такими критеріями: відповідно до їх походження: комп'ютерна електронна інформація (файли оновлення), електронна інформація, створена людиною (кодовані файли), похідна електронна інформація – така, що створюється комп'ютером на основі даних, які згенеровані комп'ютерною системою (метадані); відповідно до форми подання цифрові сліди поділяють на ті, що підлягають зчитуванню людиною та ті, які можуть бути зчитані лише за допомогою комп'ютерного пристрою (із застосуванням певного комп'ютерного коду); відповідно до місця зберігання цифрових слідів – ті, що зберігаються на першоджерелі – комп'ютерному пристрої, на якому така інформація була створена, цифрові сліди, які зберігаються на вторинному комп'ютерному пристрої (направлені, скопійовані до нього), цифрові сліди, що скопійовані або переміщені на електронні носії – накопичувачі, паперові цифрові копії; відповідно до форми: вихідні дані, програмне забезпечення, коди шифрування, комп'ютерні системи, бази даних [10, с. 171].

Крім того цифрові сліди кримінального правопорушення можуть виникати в наслідок отримання ввідних даних і команд від користувача та утворені внаслідок виконання електронно-обчислювальною технікою заздалегідь закладених алгоритмів або утворюватися в автоматичному режимі відповідно до заздалегідь запрограмованих алгоритмів та зберігати дані про стан та роботу системи, її користувачів, виконані алгоритми, помилки, що виникли під час їх виконання та інше (log-файли, звіти про помилки, тимчасові файли, транзакційні дані тощо). Такі цифрові сліди можуть міститися на локальних носіях (комп'ютера), які перебувають у межах фізичного доступу уповноважених осіб та можуть бути безпосередньо досліджені, скопійовані чи вилучені у натурі. У іншому випадку цифрові сліди можуть міститися на носії, що розміщений поза межами фізичної досяжності уповноважених осіб, але доступ до якого може бути отримано віддалено (сервери поштових служб, месенджерів, хмарних сховищ, що розміщені на території інших держав; носії, місце розташування яких невідоме). Досить часто унаслідок роботи одного приладу можуть утворюватися цифрові сліди одночасно на локальних та віддалених носіях [11, с. 208, 209]. Дослідники зазначають, що кіберзлочини дуже часто є міжнародними, не підпадають під єдину національну юрисдикцію, а комп'ютери правопорушника та потерпілого можуть знаходитися на територіях різних держав [12, с. 268]. Також цифрові сліди можуть міститися на внутрішніх та зовнішніх носіях. Зовнішні носії призначені для зберігання даних поза межами електронно-обчислювального приладу та використовуються для переміщення інформації між такими приладами (CD, DVD-диски, USB флеш-диски, флеш-карти пам'яті, зовнішні жорсткі диски тощо). Внутрішні носії призначені для зберігання даних у межах електронно-обчислювального приладу й забезпечення його роботи, розміщуються всередині корпуса комп'ютера та, у свою чергу, поділяються на від'єднувані (внутрішні жорсткі диски, модулі оперативної пам'яті) та невід'єднувані (флеш-пам'ять мобільних пристроїв, роутери, кеш-пам'ять процесорів та ін.) [11, с. 210].

Загалом варто відрізняти цифрові сліди від електронних доказів. Електронні докази – це інформація, зафіксована в електронній формі на будь-якому електронному носії. А цифрові сліди – це метадані – це інформація, яка супроводжує електронну інформацію – це дата та час її створення, місце створення, інформація про внесені зміни, про її переміщення. До прикладу, електронний документ – це електронний доказ, а дані, які йому присвоює комп'ютерний пристрій – розмір файлу, назва, розширення назви, каталог розташування, дата, час створення й останнього редагування – це і є цифровими слідами.

Таким чином, до цифрових слідів належать електронні поштові скриньки (сам лист і його текст є електронним доказом, а час, дата його відправлення є цифровими слідами); сторінка в мережі Інтернет (текст статті є електронним доказом, а адресу комп'ютерного пристрою, з якого вона була опублікована, інші метадані є її цифровими слідами); профіль в соціальних мережах (сам профіль як і листування в ньому є електронним доказом, в той час, дата допиту у профілі, дані про IP- адресу, з якої було здійснено вхід до сторінки, логіни та паролі свідчать про наявні цифрові сліди), електронні рахунки (наявність рахунку є електронним доказом, а дані про транзакції по таких рахунках є цифровими слідами), бази даних (наприклад інформація з бази даних про абонентів операторів зв'язку є електронним доказом, а інформація щодо

вхідних, вихідних дзвінків, переміщення мобільних пристроїв є цифровими слідами); локальна мережа (її наявність є електронним доказом, проте можливість доступу через неї до інших комп'ютерних пристроїв, історія дій в такій локальній мережі є цифровими слідами); веббраузер (його наявність може бути електронним доказом, а історія пошуку та IP- адреса, з якої були вчинені певні дії виступають цифровими слідами); комп'ютер (виступає матеріальним носієм інформації – як електронних доказів так і метаданих, що їх супроводжує).

Отже, цифровими слідами є дані про видозміни електронних документів, що можуть свідчити про їх створення, зміну, переміщення, видалення. Як правило, первинна інформація доступна для сприйняття людиною, проте такі дані не дають повної картини про вчинений злочин, а тому потребують додаткового криміналістичного вивчення експертом із застосування спеціальних засобів, спеціалізованих програм, що можуть декодувати приховану інформацію і відтворити її у версії доступній для слідчого. При цьому участь одного й того ж спеціаліста у всіх відповідних слідчих (розшукових) діях одного кримінального провадження має суттєві переваги. Це дозволить йому всебічно дослідити виявлені цифрові сліди, а слідчому – у найкоротші строки пізнати подію злочину, установити винуватців і факти доказування.

Перед пошуком цифрових слідів спеціалісту рекомендується створити криміналістичну копію (образ) носія (наприклад, жорсткого диска), з яким він працюватиме. Це дозволить забезпечити збереження та незмінність цифрових слідів на основному носії. Після цього фахівець може відновити резервні копії системи, логфайли, дампи оперативної пам'яті, дампи мережевих трафіків, інші файли або їх частини (у разі пошкодження), як наявні, так і видалені, а також службову інформацію про ці файли тощо. Потім фахівець аналізує сукупність знайдених цифрових слідів і вибудовує таймлайн діяльності користувача ЕОМ щодо операцій, які здійснювалися з певними файлами і програмами (встановлення, видалення, зміна), про роботу в локальній мережі або мережі Інтернет.

Будь-яка діяльність щодо пошуку, виявлення, фіксації та вилучення цифрових слідів кримінальних правопорушень має відповідати міжнародним стандартам ідентифікації, збору, отримання та збереження цифрових доказів [13]. Проте на сьогодні цифрова криміналістика має деякі проблеми щодо етичності, так технологічності. Слідчим, прокурором та слідчим суддею при здійсненні відповідно розслідування має бути збережена конфіденційна приватна інформація користувача глобальної мережі Інтернет. Особливо це питання є нагальним під час розслідування кібератак, бо часто для відтворення та визначення місця кібератаки викривається конфіденційність користувачів, особливо, коли з цією метою використовуються хмарні обчислення. Також доступність гігабітних класових посилань і багатого мультимедійного вмісту пояснює відповідне суттєве збільшення обсягу даних, які потрібно зберігати й обробляти під час розслідування та розкриття кримінальних правопорушень. Це має суттєве значення під час аналізу цифрових слідів у мережі Інтернет, експерт може не мати змоги охопити та зберегти весь необхідний трафік. Також цифрові сліди можуть бути розпорошені між різними фізичними або віртуальними місцями, такими як онлайн-соціальними мережами, криптовалютними гаманцями, механізмом CaaS, хмарними ресурсами та певним електронно-обчислювальним пристроєм, підключеним до персональної мережі. Тому ефективність пошуку, виявлення, фіксації та вилучення цифрових слідів кримінальних правопорушень потребує досконалого знання й практичних навичок роботи з комп'ютерним і телекомунікаційним обладнанням, а також спеціалізованим програмним забезпеченням, що забезпечить найбільш ефективне його застосування під час пошуку, фіксації, вилучення та подальшого дослідження і зберігання цифрових слідів.

Так, до спеціалізованих засобів виявлення та аналізу цифрових слідів кримінальних правопорушень можна віднести: 1) експертне програмне забезпечення для криміналістичного дослідження комп'ютерних носіїв інформації, наприклад «X-Ways Forensics», «EnCase Forensic», «Belkasoft Evidence Center», «Forensic Toolkit»; 2) мобільні комплекси, що дозволяють добувати, декодувати та аналізувати цифрову інформацію, отриману з мобільних пристроїв, зокрема «MSAB XRY Field», «MOBILedit Forensic Express Pro», «Cellebrite UFED Touch 2»; 3) програмне забезпечення з відновлення комп'ютерних даних «UFS Explorer», «RStudio» тощо [14, с. 462].

Таким чином, на сьогодні виявлення, розслідування та розкриття значної кількості кримінальних правопорушень потребує виявлення, збирання, дослідження та використання цифрових слідів. Проте наразі питання електронного доказування в кримінально-процесуальному законодавстві України є недостатньою мірою визначеним, а тому потребує особливої уваги з боку законодавця, що, перш за все, має полягати у визнанні електронних доказів, як окремих джерел доказування в кримінальному провадженні, а їх метаданих як супутніх доказів, що можуть бути виявлені, зібрані, досліджені й використані у кримінальному провадженні, як цифрові сліди.

На сьогодні цифрова криміналістика є необхідним інструментом для провадження якісного судочинства щодо кримінальних правопорушень, скоєних у віртуальному просторі, оскільки показники злочинності, що вчинена за допомогою мережі Інтернет невпинно зростає. Цифрові сліди варто відокремлювати від електронних доказів, зважаючи на те, що цифрові сліди є метаданими, тобто фактично інформацією про інформацію. Саме вони супроводжують документи, що виступають доказовою базою, проте такі дані містять якнайповнішу інформацію про автора такої інформації, дату, час створення, зміни, переміщення та її видалення. Дослідження цифрових слідів потребує не лише додаткових експертиних знань, а й спеціального програмного забезпечення. Крім того, важливим аспектом є також законодавче забезпечення дослідження та використання електронних доказів та цифрових слідів в криміналістиці та кримінальному процесі. Необхідно враховувати специфічні властивості цифрової інформації та з урахуванням цього залучати експертів-криміналістів до проведення слідчих (розшукових) дій, під час яких можуть бути виявлені цифрові сліди, оскільки через неправильне їх вилучення вони можуть бути пошкоджені (знищені), а також враховувати, що деякі цифрові сліди можуть бути недоступними для дослідження їх під час судового розгляду, тому вони потребують розшифрування та відтворення у звичній графічній, текстовій або звуковій формі у висновку експерта.

ЛІТЕРАТУРА

1. Хижняк Є. С. Віртуальні сліди: поняття та ознаки. *Правове життя сучасної України* : у 2 т. : матер. Міжнар. наук.-практ. конф., 17 трав. 2019 р. Одеса : ВД «Гельветика», 2019. Т. 2. С. 422–425.

2. Басай В. Д., Томин С. В. Дослідження віртуальних слідів – перспективний напрямок кримінального слідознавства. *Актуальні проблеми держави і права.* 2008. Вип. 44. С. 220–223.

3. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304–307.

4. Шевчук В. М. Цифрова криміналістика: формування та роль у забезпеченні безпекового середовища України. *Нова архітектура безпекового середовища України* : зб. тез всеукр. наук.-практ. конф., 23 грудня 2022 р. Харків: Юрайт, 2022. С. 146–150.

5. Журавель В. А., Шепітько В. Ю. Розвиток криміналістики та судової експертизи в Україні: наближення до єдиного європейського простору / Правова наука України: сучасний стан, виклики та перспективи розвитку: монографія. Харків, 2021. 786 с.

6. Авдєєва Г., Стороженко С. Електронні сліди: поняття та види. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 1. С. 169–176.

7. Віртуальний / Великий тлумачний словник сучасної мови. URL: https://slovnyk.me/dict/vts/%D0%B2%D1%96%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9 (дата звернення: 09.10.2023).

8. Авдєєва Г. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики*. 2018. С. 90–93. URL: https://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf (дата звернення: 06.10.2023).

9. Digital Footprints. Pew Research Center: Internet, Science & Tech. URL: https://www.pewresearch.org/internet/2007/12/16/digital-footprints/ (дата звернення: 09.10.2023).

10. Joshua I James. Challenges with Automation in Digital Forensic Investigations. *Digital Forensic Investigation Research Group University College Dublin Belfield*. Dublin. URL: https://www.researchgate.net/publication/258817785_Challenges_with_Automation_in_Digital_Forensic_Investigations (дата звернення: 09.10.2023).

11. Коваленко А. В. Класифікація електронних (цифрових слідів кримінального правопорушення. *Проблеми законності.* 2023. Вип. 161. С. 202–214.

12. Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. *Amazonia Investigaю.* 2022. Vol. 11, issue 53. P. 259–269. URL: https://doi.org/10.34069/AI/2022.53.05 (дата звернення: 09.10.2023).

13. ISO/IEC 27037:2012. ISO. Guidelines for identification, collection, acquisition and preservation of digital evidence. 2018. URL: https://www.iso.org/ru/standard/44381.html (дата звернення: 09.10.2023).

14. Омельян О. С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 457–466. URL: https://digest.kndise.gov.ua/wp-content/uploads/2020/06/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%96%D1%81%D1%82%D0%B8%D0%BA%D0%B0_65_%D0%B4%D1%80%D1%83%D0%BA_%D0%BD%D0%BE%D0%B2%D0%B8%D0%B9-457-466.pdf (дата звернення: 12.10.2023).