хто стріляв (передбачувану або відому), а у разі наскрізного поранення — ще й місце виявлення снаряда чи розташування ушкоджень, спричинених перешкоді після проходження крізь тіло. За необхідності виконують ситуаційне моделювання: візування умовної лінії польоту кулі за допомогою шнура, мотузки та ін., застосування геодезичних і артилерійських приладів (лазер, теодоліт, бусоль та ін.).

Визначаючи напрямок пневмострільного ранового каналу, слід керуватися тільки його розташуванням стосовно основних площин тіла, а не положенням тіла в просторі. Оскільки прямолінійна ділянка ранового каналу на невеликих відстанях пострілу збігається за напрямком із подовжньою віссю каналу ствола зброї (за відсутності попереднього рикошету снаряда), то судово-медичний експерт під час дослідження має можливість визначити положення зброї в мить заподіяння пневмострільного поранення тільки стосовно тіла постраждалого.

Перелік джерел посилання

1. Bligh-Glover W.Z. One-in-a-million shot: A homicidal thoracic air rifle wound, a case report, and a review of the literature. *American Journal of Forensic Medicine and Pathology.* 2012. Vol. 33. Is. 1. Pp. 98—101. DOI: 10.1097/paf.0b013e318221b8a9 (дата звернення: 26.08.2023).
2. Козаченко І. М. Смертельна пневмострільна травма: структурний аналіз та морфологічні особливості ушкоджень. *Судово-медичний експерт*. 2015. № 2. С. 89—93.
3. Grinshteyn E., Hemenway D. Violent death rates: the US compared with other high income OECD countries, 2010. *Am J Med.* 2016. No 129(3). Pp. 266—273. DOI: 10.1016/j.amjmed.2015.10.025 (дата звернення: 26.08.2023).
4. Козаченко І. М. Сучасні термінологія, понятійний апарат і класифікації пневмострільних ушкоджень, пневматичної зброї та снарядів до неї (методичні рекомендації). Київ, 2013. 28 с.

Значення цифрових слідів під час розслідування кримінальних правопорушень

Інна Колеснікова,
канд. юрид. наук, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна, ORCID: https://orcid.org/0000-0002-6138-8569, e-mail: Inna.a.kolesnikova@gmail.com

Висвітлено ключові концепції цифрових слідів, а також їх значення під час розслідування кримінальних правопорушень.

Ключові слова*: цифрова криміналістика; цифрові сліди; розслідування кіберзлочинів.*

The Significance of Digital Traces During the Investigation of Criminal Offenses

Inna Kolesnikova

This paper elucidates the fundamental concepts of digital traces and their significance in criminal investigations.

Keywords*: digital forensics; digital traces; cybercrime investigation.*

Швидкий розвиток цифрових технологій і їх використання у різних сферах життя суспільства призвели до зростання кількості кіберзлочинів та інших правопорушень, пов'язаних із використанням електронно-обчислювальних пристроїв. Розуміння сутності цифрових слідів кримінальних правопорушень є надзвичайно важливим для правоохоронних органів у боротьбі зі злочинністю, що зумовлює можливість обрання належних практико-орієнтованих рекомендацій щодо їх виявлення, збирання, дослідження й використання у кримінальному провадженні. Цифрові сліди, які можуть бути отримані з комп'ютерів, мобільних пристроїв, планшетів, цифрових камер та інших електронних пристроїв, є джерелами доказової та орієнтувальної інформації. Ці дані мають суттєве значення під час пізнання події злочину, установлення винуватців і фактів, доказування. Цифрові сліди можуть містити широкий спектр інформації,

включно з даними про комунікацію, місцезнаходження, активність в інтернеті, файли, повідомлення, електронну пошту, та міститися в інформаційних (автоматизованих) системах, телекомунікаційних системах та інформаційно-телекомунікаційних системах.

Поряд із терміном «цифрові сліди» у юридичній літературі використовують також інші, наприклад: «електронні сліди, електронні докази, [1, с. 148; 2, с. 657] «комп'ютерні сліди», «віртуальні сліди», «інформаційні сліди». Саме дефініцію «цифрові сліди» науковці визначають як невидимі матеріальні сліди, що містять криміналістично значиму інформацію, яку відтворено у цифровій формі на матеріальних носіях, та можуть бути виявлені за допомогою спеціальних криміналістичних знань [3, с. 91].

Вважаємо, що у формуванні поняття цифрового сліду треба 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 із застосуванням комп'ютерних технологій; по-третє, цифрові сліди як інформація містять дані про вчинені кіберзлочини.

Будь-яка взаємодія користувача з цифровою операційною системою, пристроєм або програмним забезпеченням призводить до автоматичного створення та/або зміни файлів, що містять відомості про налаштування та журнали використання [4, с. 1]. Цифрові сліди кримінального правопорушення можуть виникати внаслідок отримання вхідних 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 ін. (*log*-файли, звіти про помилки, тимчасові файли, транзакційні дані тощо). Крім того, ці цифрові сліди можуть міститися на локальних носіях (комп'ютері), які розміщені у межах фізичного доступу уповноважених осіб та можуть бути безпосередньо досліджені, скопійовані або вилучені. В іншому випадку цифрові сліди можуть міститися на носії, розміщеному поза межами фізичної досяжності уповноважених осіб, але доступ до якого може бути отримано віддалено (сервери поштових служб, месенджерів, хмарних сховищ, розташованих на території інших держав; носії, місце розташування яких невідоме, тощо). Досить часто внаслідок роботи одного приладу можуть утворюватися цифрові сліди одночасно на локальних та віддалених носіях [5, с. 208, 209]. Дослідники зазначають, що кіберзлочини дуже часто міжнародні, не підпадають під єдину національну юрисдикцію, а комп'ютери правопорушника та потерпілого можуть бути на територіях різних держав [6, 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, розміщені всередині корпуса комп'ютера та, своєю чергою, бувають від'єднувані (внутрішні жорсткі диски, модулі оперативної пам'яті) та невід'єднувані (флеш-пам'ять мобільних пристроїв, роутери, кеш-пам'ять процесорів та ін.) [5, 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 розміщення, дата, час створення й останнього редагування — це і є цифрові сліди.

Отже, 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 інтернеті (текст статті є електронним доказом, а адреса комп'ютерного пристрою, з якого вона була опублікована, інші метадані є її цифровими слідами); профіль у соціальних мережах (сам профіль, як і листування в ньому, є електронним доказом, дата допиту в профілі, дані про *IP*- адресу, з якої було здійснено вхід на сторінку, логіни та паролі — цифрові сліди); електронні рахунки (наявність рахунку є електронним доказом, а дані про транзакції за такими рахунками є цифровими слідами), бази даних (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 у такій локальній мережі є цифровими слідами); веб-браузер (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 супроводжують).

Отже, цифровими слідами є дані про видозміни електронних документів, що можуть свідчити про їх створення, зміну, переміщення, видалення. Зазвичай первинна інформація доступна для сприйняття людиною, проте в контексті кіберзлочинності такі дані не дають повної картини вчиненого злочину, а тому потребують додаткового криміналістичного вивчення експертом із застосуванням спеціальних засобів, спеціалізованих програм, що можуть декодувати приховану інформацію та відтворити її у версії, доступній для слідчого. Важливо зазначити, що наявність спеціальних знань для вивчення таких доказів є обов'язковою. До спеціалізованих комп'ютерних технологій, необхідних для аналізу цифрових слідів, належать експертне криміналістичне програмне забезпечення, комплекси програм для декодування та аналізу цифрової інформації, створеної на мобільних пристроях, програмне забезпечення для відновлення комп'ютерних даних. Отже, для провадження якісної роботи необхідна висока кваліфікація експерта та знання щодо можливих шляхів учинення кіберзлочинів та видів цифрових слідів, які можуть залишатися внаслідок учинення кримінального правопорушення.

Нині питання електронного доказування в кримінально-процесуальному законодавстві України недостатньо визначене, 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.

Перелік джерел посилання

1. Шевчук В. М. Цифрова криміналістика : формування та роль у забезпеченні безпекового середовища України. *Нова архітектура безпекового середовища України :* зб. тез всеукр. наук.-практ. конф. (Харків, 23.12.2022). Харків, 2022. С. 146—150.
2. 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.
3. 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: 10.09.2023).
4. Horsman G. Raiders of the lost artefacts: Championing the need for digital forensics research. *Forensic Science International: Reports.* 2019. Vol. 1. Pp. 1—5. DOI: 10.1016/j.fsir.2019.100003 (дата звернення: 10.09.2023).
5. Коваленко А. В. Класифікація електронних (цифрових слідів кримінального правопорушення. *Проблеми законності* : зб. наук. праць. 2023. Вип. 161. 304 с. DOI: 10.21564/2414-990X.161.278117 (дата звернення: 10.09.2023).
6. Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. Amazonia Investiga. 2022. Vol. 11. Is. 53. Pp. 259–269. DOI: 10.34069/AI/2022.53.05.26 (дата звернення: 10.09.2023).