Шпак І.М.
студентка;
Грекова Л.Ю.
завідувач навчально-наукової криміналістичної лабораторії,
Юридичний факультет
Національного авіаційного університету

ОСОБЛИВОСТІ ВИЛУЧЕННЯ ЦИФРОВИХ СЛІДІВ

Актуальним та одним із найбільш обговорюваних серед науковців на сучасному етапі розвитку нашої держави та суспільства в умовах так званої «діджиталізації» є питання про цифрову інформацію та її доказове значення у кримінальному провадженні. Однозначно те, що на сьогоднішній день правоохоронні структури зацікавлені в розробці концепцій щодо впровадження ефективних методів, засобів, методик, спрямованих на виявлення, розслідування, розкриття кримінальних правопорушень інформаційної спрямованості.

Отож, насамперед, потрібно з'ясувати правовий зміст поняття «цифровий слід». Стосовно цього варто вказати на існування плюралізму підходів навіть до самого словосполучення, що вживається у науці кримінального процесу та криміналістики на позначення вказаного правового явища. Так, аналіз різних наукових публікацій у цьому ракурсі засвідчує те, що найчастіше вчені оперують такими поняттями, як

«віртуальний слід» (В. А. Мещеряков, А. Б. Смушкін, Л. Б. Краснова, В. Ю. Агібалов та інші), «бінарний слід» (В. А. Мілашев), «електронний слід» (В. Б. Вехов), «цифровий слід» (О. Р. Россинська, І. А. Рядовський, А. І. Семікаленова тощо). Проте більш вдалим видається використання у цьому контексті словоконструкції «цифровий слід», оскільки вона дає можливість максимально охопити різноманітні прояви цього явища та відображає його реальну технічну природу утворення [1, с. 93].

Таким чином злочинці можуть залишати електронні сліди в різних інформаційних базах даних, наприклад у базах операторів мобільного зв'язку; при використанні кредитних, дисконтних карт, проїзних документів тощо. Важливим джерелом доказів є комп'ютерна система, яка складається з корпусу, де розміщені мікропроцесор, плати, накопичувачі інформації та порти для зовнішніх пристроїв, монітора, периферійних пристроїв (принтер, сканер тощо), програмного забезпечення [2, с. 79].

Існують також зовнішні та внутрішні накопичувачі інформації, а також змінні носії (CD, DVD-диски) та різноманітні USB-накопичувачі. У цифрових камерах та мобільних телефонах широко використовуються невеликі за розмірами карти пам'яті, які також в свою чергу можуть містити значний обсяг даних.

Надзвичайно багато різноманітної інформації містять сучасні мобільні пристрої – смартфони, планшети, а також плеєра.

Крім того, системи відеоспостереження можуть містити інформацію про факти та обставини, що мають значення для кримінального провадження.

Варто також зважати на те, що сьогодні значний обсяг інформації зберігається у «хмарних технологіях», тобто поза місцезнаходженням фізичної чи юридичної особи.

У зв'язку з цим сучасний правоохоронець просто зобов'язаний грамотно використовувати цифрові сліди в інтересах встановлення обставин кримінального правопорушення. Виявлення, фіксація, розшифровка таких слідів сприяє розкриттю і розслідуванню кримінальних правопорушень, у тому числі вчинюваних в Інтернет-просторі. Однозначно можна сказати, що збирання доказів в електронній формі є достатньо нелегким та клопітким процесом. І, правду кажучи, не кожен слідчий володіє відповідними знаннями у сфері сучасних інформаційно-комунікаційних технологій у достатній мірі, аби успішно організувати розслідування. Саме тому у такій справі бажана допомога

висококваліфікованого фахівця, який є достатньо обізнаним у цій сфері та має досвід, адже навіть незначна помилка у дії з доказами в електронній формі може спричинити незворотну втрату потрібної інформації.

Важливо наголосити і на тому, що під час роботи з електронними доказами слід дотримуватися таких принципів:

1. Законність. Працівники та підрозділи, що провадять розслідування і досліджують докази в електронній формі, зобов'язані дотримуватися чинного законодавства, загальних процесуальних та криміналістичних принципів.

2. Цілісність даних. Дії фахівця не повинні призводити до матеріальних змін даних, електронних пристроїв чи носіїв інформації, які можуть використовуватись як докази.

3. Документування процесу. Документують будь-які дії, виконувані стосовно електронних доказів, і зберігають ці документи на випадок перевірки, щоб незалежна третя сторона могла повторити ці дії та отримати аналогічний результат.

4. Експертна підтримка. Якщо передбачається, що при огляді (обшуку) можуть бути виявлені електронні докази, отримують підтримку фахівців (спеціалістів), забезпечивши, за можливості, їх присутність на місці події.

5. Відповідна фахова підготовка. Якщо при огляді (обшуку) відсутні фахівці з електронних доказів, першочергові дії на місці події здійснюють особи, які мають необхідні знання та навички для виявлення і збирання доказів.

6. Розумна обережність. Уникають будь-яких навмисних або ненавмисних дій, які можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі [3, с. 9].

До прикладу, правоохоронці не повинні мати доступ до цифрових пристроїв, якщо їм бракує компетентності і вони не обізнані з відповідними процесами. Зокрема, якщо фізичний обсяг цифрового пристрою занадто великий, приміром, сервер в інформаційному центрі, чи це критично для безпеки цифрового пристрою, зупинка якого загрожуватиме життю людей, або коли необхідно зафіксувати спосіб роботи підозрюваного під час зловживання системою.

Отож, для того аби вилучити електронні докази потрібно не лише запросити висококваліфікованого спеціаліста, але й мати відповідні інструменти та обладнання, які він може використовувати в залежності від конкретної ситуації:

1. Носії інформації, на які безпосередньо копіюватимуться дані: жорсткі диски (вінчестери); змінні носії (CD-DVD-диски); зовнішні пристрої з накопичувачами та для роботи з оптичними носіями інформації тощо.

2. Інструменти для демонтажу обладнання: викрутки (плоскі та фігурні); кусачки; плоскогубці; пінцет тощо.

3. Інструменти для документування процесу: фото- та відеокамера; бирки для нумерації доказів.

4. Матеріали для упаковки та транспортування вилучених об'єктів: антистатичні пакети; кабельна стяжка; коробки для DVD-дисків; коробки різноманітних розмірів для інших вилучених об'єктів.

5. Інші засоби та матеріали: транспорт для перевезення слідчо-оперативної групи, інструментів та вилучених матеріалів; папір для друку; роздруковані тексти із правами та обов'язками учасників слідчих дій; ноутбук зі стандартним програмним забезпеченням; спеціалізовані програмно-апаратні пристрої цифрової криміналістики (форензіки), криміналістичні загрузочні диски тощо [3, с. 13].

Отже, виявлення, фіксація і вилучення цифрових слідів кримінального правопорушення потребує використання спеціальних знань і технологій, розробка та вдосконалення яких протягом останніх кількох років представляє виключно актуальний напрямок криміналістики. Вважаю, що саме цифровим (віртуальним) слідам варто відвести окреме місце у переліку всіх слідів, які вивчаються в криміналістиці, а також визначитись з єдиною загальновизнаною кваліфікацією самих віртуальних слідів. Саме завдяки розвитку інноваційних технологій необхідним стає розвиток нового напрямку криміналістичної ідентифікації, пов'язаного з ідентифікацією технічних засобів за залишеними цифровими слідами, адже визначити відповідність інформації, що міститься на різних електронних носіях, або наявність на носії інформації із заданими характеристиками не представляється можливим за допомогою традиційних видів криміналістичної ідентифікації.

Список використаних джерел:

1. Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні / Цифрові трансформації України 2020: виклики та реалії : зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу, 18 вересня 2020 р. Харків : НДІ ПЗІР НАПрН України, 2020. С. 93.

2. Заєць І. С. Перспективи криміналістики в умовах інформатизації суспільства // Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід : матеріали Міжнар. наук.-практ. круглого столу, 19 лютого 2020 р. Київ : Нац. акад. внутр. справ, 2020. С. 79.

3. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. С. 9–13.