Деякі організаційно-тактичні особливості проведення огляду носіїв інформації (комп'ютерної техніки) під час розслідування кримінальних правопорушень проти власності, учинених представниками релігійних організацій

Олександр Кривопуск
доктор філософії, старший викладач кафедри криміналістики та домедичної підготовки, Дніпровський державний університет внутрішніх справ Міністерства внутрішніх справ України, м. Дніпро, Україна,
ORCID: https://orcid.org/0000-0003-4889-5205, e-mail: krivopusk.and@ukr.net

Джерелами цифрових слідів вчиненого кримінального правопорушення є різного роду технічні пристрої, до яких належить і комп'ютерна техніка. Висвітлено особливості проведення огляду носіїв інформації та застосування технічних засобів у провадженнях щодо майнових злочинів. Особливу увагу приділено окремим тактичним особливостям проведення огляду носіїв, які зберігають електронні сліди кримінальних правопорушень.

Ключові слова: *огляд; цифрові сліди; слідова картина; розслідування.*

Some Organizational and Tactical Aspects of Inspecting Data Storage Media (of Computer Equipment) in the Investigation of Property Crimes Committed by Representatives of Religious Organizations

Oleksandr Kryvopusk

Sources of digital traces of a criminal offense are various kinds of technical devices, which include computer equipment. The features of the inspection of information carriers and the use of technical means in the proceedings for property crimes are highlighted. Particular attention is paid to the coverage of certain tactical features of the inspection of media that store electronic traces of criminal offenses.

Keywords: *inspection; digital traces; trace picture; investigation.*

У сучасних умовах під час розслідування кримінальних проваджень проти власності спостерігаємо сталу тенденцію до збільшення частки цифрових (інформаційних) слідів.

Поширення цифрових пристроїв і пов'язаних із ними технологій трансформує механізми вчинення багатьох кримінальних правопорушень у різних сферах людського життя [1, с. 282].

Проведеним аналізом матеріалів кримінальних проваджень досліджуваної категорії з'ясовано, що цифрові сліди як елемент слідової картини характерні для 74 % проваджень.

За результатами проведеного опитування представників правоохоронних органів, які брали безпосередню участь у розслідуванні кримінальних правопорушень проти власності, учинених посадовими особами

релігійних організацій і представниками деструктивних сект, у 53 % проваджень основу доказової бази становили цифрові (інформаційні) сліди.

Хоча зазначений різновид слідів є доволі новим, що пояснює відсутність як наукового визначення цієї дефініції, так і її сталої класифікації, проте їхні кількість та роль для досудового розслідування постійно зростають.

Розкриваючи проблематику питання інформаційних (цифрових) слідів, Є. Є. Демидова зазначає, що цифрові сліди виникають унаслідок застосування цифрових засобів і технологій. Водночас необхідно звернути увагу на те, що застосування таких засобів і технологій може бути як безпосереднім (коли особа фізично їх застосовує, зокрема: за допомогою ноутбуку здійснює пошук в інтернеті певної інформації або завантажує відеофайли в соціальну мережу), так і опосередкованим (коли такі дані утворюються без фактичного втручання особи: утворення метаданих під час фотографування певного об'єкта, фіксування камерами відеоспостереження пересування транспортного засобу тощо). Тобто цифрові сліди можуть утворитися і без підключення до інтернету або активної діяльності в мережі [2, с. 73].

Поміж основних джерел цифрових слідів у провадженнях досліджуваної категорії можна виокремити комп'ютерну техніку, зокрема планшети, ноутбуки, стаціонарні комп'ютери, смартфони тощо.

У процесі документування кримінальних правопорушень проти власності, учинених представниками релігійних організацій, слідчі залежно від ситуації приймають рішення щодо місця проведення огляду носіїв інформації.

Нерідко слідчі у процесі проведення слідчих (розшукових) дій приймають рішення про вилучення носіїв інформації для подальшого їх огляду із залученням спеціалістів, застосовуючи для цього відповідне спеціальне обладнання (з метою подолати системи захисту, відновити раніше видалену інформацію та зняти (скопіювати) інформацію, яка має значення для розслідування фактів протиправної діяльності).

Для надійного збереження слідової інформації варто пам'ятати, що електронні сліди утворюються внаслідок зовнішнього доступу до комп'ютерних систем із 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 умісту файлів, зміна атрибутів файлів, поява нових каталогів і файлів, зміна інформації про час останнього доступу до інформації, результати роботи антивірусних і тестових програм тощо [3, с. 228].

В окремих випадках виникає потреба в оперативному огляді носіїв віртуальних слідів, оскільки існує ризик дистанційного втручання з метою знищення інформації, яка збережена на технічних пристроях.

У разі прийняття слідчим рішення про проведення огляду технічних

засобів на місці проведення слідчих (розшукових) дій для ефективного проведення огляду носія інформаційних слідів і збереження інформації доречним є залучення спеціаліста у сфері комп'ютерних технологій. Його роль полягає у сприянні слідчому у виявленні, належному фіксуванні та вилученні віртуальних (інформаційних) слідів, а також у визначенні напрямів експертних досліджень і формулюванні питань для експертного дослідження.

Із метою не допустити дистанційного знищення інформації та блокування носіїв інформації під час їх огляду, слідчий, окрім недопущення сторонніх осіб, має від'єднати пристрої від інтернету. Окрім цього, перед початком проведення огляду комп'ютерної техніки рекомендовано в налаштуваннях налагодити відповідні параметри, які унеможливлять блокування пристрою через певний проміжок часу.

Якщо до комп'ютерної техніки під'єднані флешнакопичувачі або інші пристрої, необхідно (не вилучаючи їх) зафіксувати ці відомості у протоколі та (за можливості) оглянути вміст накопичувача, не від'єднуючи його від пристрою.

Під час огляду інформації (залежно від учиненого кримінального правопорушення) доречно зафіксувати історію браузера та вміст електронної пошти. Окрім цього, оглядаючи пристрій, доцільно оглянути й зафіксувати відомості, збережені у вкладці «менеджер паролів» відповідних веббраузерів.

У процесі огляду смартфонів у налаштуваннях необхідно передусім налаштувати режим «у літаку» із метою від'єднати пристрій від мереж *WI-FI* та *Bluetooth*.

У процесі вилучення комп'ютерної техніки, смартфонів, зовнішніх жорстких дисків, флешнакопичувачів та інших носіїв інформації (після проведення їх огляду) такі предмети необхідно поміщати у спеціальні екрановані сумки (чохли) — так звані сумки (чохли) Фарадея.

Перелік джерел посилання

1. Братішко Н. Напрями використання цифрової криміналістики в умовах воєнного стану. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2023. Спец. вип. № 2. С. 282—288. DOI: 10.31733/2078-3566-2023-6-282-288 (дата звернення: 28.03.2025).
2. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету.* 2024. Вип. 85. Ч. 4. С. 71—75. DOI: 10.24144/2307-3322.2024.85.4.10 (дата звернення: 28.03.2025).
3. Лазебний А. М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис.* 2023. Вип. 1 (10). С. 226—233. DOI: 10.33244/2617-4154.1(10).2023.226-233 (дата звернення: 28.03.2025).