ОКРЕМІ ПИТАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В КОМП'ЮТЕРНО-ТЕХНІЧНІЙ ЕКСПЕРТИЗІ

Олена Володимирівна НЕНЯ,

кандидат юридичних наук,
начальник 1-го відділу науково-дослідної
лабораторії криміналістичної та спеціальної
техніки Державного науково-дослідного
інституту МВС України
https://orcid.org/0000-0001-9721-5718

Станіслав Миколайович КОРНІЙКО,

науковий співробітник 1-го відділу науково-
дослідної лабораторії криміналістичної та
спеціальної техніки Державного науково-
дослідного інституту МВС України
https://orcid.org/0000-0003-1266-8166

Андрій Володимирович ГУЛЯЄВ,

кандидат технічних наук,
старший науковий співробітник, завідувач
науково-дослідної лабораторії криміналістичної
та спеціальної техніки Державного науково-
дослідного інституту МВС України
https://orcid.org/0000-0002-4965-8677

Наталія Михайлівна БЕРЕЗНЕНКО,

кандидат технічних наук, доцент,
провідний науковий співробітник 2-го відділу
науково-дослідної лабораторії криміналістичної
та спеціальної техніки Державного науково-
дослідного інституту МВС України
https://orcid.org/0000-0003-4589-3829

Широке впровадження комп'ютерної техніки та комп'ютерних технологій у суспільне життя супроводжується поширенням кола злочинів з їх використанням.

У зв'язку з цим необхідність трансформації спеціальних знань з області комп'ютерної інформації в область криміналістичну набуває все більшої актуальності та необхідності. А ефективність роботи експертів, саме з напряму комп'ютерно-технічних досліджень, знаходиться у прямій залежності від використання найновітніших розробок у галузі апаратно-програмного забезпечення та інформаційних технологій.

До інформаційних технологій належать процеси, де «вихідним матеріалом» і «продукцією» є інформація. Зрозуміло, що інформація, яка переробляється, зв'язана з визначеними матеріальними носіями.

Під інформаційними технологіями розуміється переробка інформації на базі комп'ютерних обчислювальних систем.

Комп'ютерно-технічна експертиза – одна з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка та (або) комп'ютерні носії інформації, а метою – пошук і закріплення доказів [1-3].

Слід зазначити, що цілий ряд злочинів можуть містити інформацію в електронному вигляді, і сюди входять не лише кіберзлочини, а й підробка та виготовлення документів і грошових банкнот, вимагання хабарів та погрози, надіслані засобами електронної пошти або через месенджери за допомогою як комп'ютерної техніки, так і смартфонів, переписка про наміри вчинити той чи інший злочин тощо. Тому об'єктами комп'ютерно-технічної експертизи можуть бути як апаратні засоби (системні блоки комп'ютерів та їх комплектуючі, сервери, ноутбуки, жорсткі диски, флеш-накопичувачі, модеми, маршрутизатори тощо), так і програмні продукти (комп'ютерні програми, бази даних тощо).

З огляду на те, що комп'ютерно-технічна експертиза знаходиться у процесі постійного розвитку і перелік питань, на які вона може дати відповідь постійно розширюється та зазнає змін, наслідком цього є величезна кількість об'єктів, що підлягають огляду та вилученню (фіксації) під час здійснення заходів забезпечення досудового розслідування за цим напрямом. При цьому, їх види та типи також складають дуже широкий спектр. Наслідком цього є й специфічний підхід до відбору вилученню (фіксації) об'єктів досліджень (ст. 159 КПК), що потребує обов'язкової участі спеціаліста (ст. 71 КПК) в галузі комп'ютерної техніки» [4].

Тому перед спеціалістом (ст.71 КПК), який залучений до досудового розслідування, постає завдання вилучення надвеликої кількості об'єктів з місця проведення огляду, які у подальшому мають бути досліджені експертом, що вимагає значних обсягів часу. При цьому значна кількість таких об'єктів може не містити інформації, яка стосується даного правопорушення.

Тому, актуальним питанням для підвищення якості та ефективності комп'ютерно-технічної експертизи є розгляд аспекту оптимізації кількості об'єктів, що підлягають вилученню (фіксації) під час здійснення заходів забезпечення досудового розслідування, шляхом ефективного використання спеціальних пристроїв для запобігання умисного втручання або випадкового редагування інформації на вилучених оригінальних носіях інформації та пристроїв для виготовлення побітових копій з таких носіїв.

Виконання судових експертиз та багато інших напрямків діяльності, пов'язані з комп'ютерною криміналістикою, вимагають максимально можливого збереження цілісності досліджуваних даних. Для цього використовуються програми або пристрої, що не дозволяють записати будь-яку інформацію на досліджуваний накопичувач.

Як у світовій практиці, так й у практиці українських криміналістів, відповідно до вимог ДСТУ iso/iec 17025:2017 [5] у сфері комп'ютерно-технічних досліджень, загальноприйнятим є певний порядок проведення

таких досліджень з використанням спеціальних пристроїв для запобігання умисного втручання або випадкового редагування інформації на вилучених оригінальних носіях інформації (далі – блокувач), наприклад, Digital Intelligence UltraBlock (США), WiebeTech Forensic UltraDock (США), EPOS WriteProtector (Україна), а також пристроїв для виготовлення побітових копій з оригінальних носіїв (далі – дублікатор), наприклад, Tableau Forensic Duplicator TD3 (США), IM Solo-4 Forensic (США), ICS Image MASSter 4000 Pro (США), EPOS DiskMaster Portable (Україна).

Для обробки та аналізу побітових копій з оригінальних носіїв ще десять років тому вітчизняними експертами використовувався цілий набір різноманітних програм, який с кожним роком все активніше замінюється спеціальними програмно-апаратними комплексами, що дає змогу індексувати скопійовану інформацію за її видами (текстова, графічна, відео, тощо), відновлюючи при цьому видалені раніше файли, якщо їх залишки будуть виявлені під час індексації. Також зазначені програмно-апаратні комплекси дають змогу проводити дуже швидкий пошук за контекстом серед проіндексованого масиву інформації, перегляд та пошук необхідної графічної інформації та відеоконтенту за визначеними замовником критеріями.

Так як вітчизняними експертами активно переймається зарубіжний досвід, то змінюється й алгоритм досліджень, який передбачає наявність наступних кроків.

1. Виготовлення побітової копії носія електронної інформації з використанням блокувачів. Така копія зазвичай називається «файл-образом» або «образом диска». Часто таких файлів може бути багато.

Образ диска (англ. термін «Image») – файл, що містить у собі повну копію вмісту та структури файлової системи та даних, що містяться на диску (наприклад, на компакт-диску, дискеті чи розділі жорсткого диска) [6]. Термін описує будь-який файл, незалежно від того, чи був образ отриманий із реального фізичного диска, чи ні. Таким чином, образ диска містить всю інформацію, необхідну для дублювання структури, розташування та вмісту даних будь-якого пристрою для зберігання інформації.

2. Проведення індексації скопійованої інформації (сортування інформації за певними критеріями, наприклад поділ файлів відповідно до їх формату: txt, doc, xls, ppt, mdb, jpg, bmp, avi, mov тощо) з використанням спеціального програмного забезпечення та потужних комп'ютерів, що призначені для даних завдань.

3. Пошук заданої інформації відповідно до встановлених замовником критеріїв та оформлення висновків експерта.

Перші два пункти реалізуються за допомогою саме спеціального програмно-апаратного забезпечення, а саме блокувачів та дублікаторів.

Аналіз технічних характеристик та можливостей застосування таких зразків сучасного спеціального програмно-апаратного забезпечення, а також деяких аспектів його функціонування, як зарубіжного так і вітчизняного виробництва, демонструє їх високу надійність з урахуванням валідаційних процедур і доводить доцільність їх активного використання саме під час здійснення заходів забезпечення кримінального провадження безпосередньо на місці скоєння правопорушення, з огляду на те, що вони дають змогу копіювати інформацію в незмінному вигляді, запобігаючи її по-

шкодженню або редагуванню, а також апаратне прискорення дешифрації даних під час криміналістичного копіювання інформації з електронних носіїв.

Проте дослідження окремих науковців [7, 8] висвітлюють наявність деяких проблем під час використання цих пристроїв. Так, іноді можуть виникати ймовірні стани файлової системи (наприклад, викликані нестандартною роботою користувачів з носіями інформації), які можуть призвести до спотворення інформації, що вилучається (фіксується).

Отже, на нашу думку, для оптимізації (зменшення) кількості об'єктів дослідження, які у подальшому спрямовуватимуться на комп'ютерно-технічну експертизу, вбачається доцільним попередній перегляд слідчим разом зі спеціалістом за цим напрямом інформаційного наповнення виявлених електронних носіїв для відбору тих, що містять кримінально значиму інформацію.

Список використаних джерел:

1. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень. Наказ Міністерства юстиції України від 08.10.1998 № 53/5. Відомості Верховної Ради (ВВР). 1998. № 27-28. Ст.181.

2. Перелік видів судової експертизи та експертних спеціальностей, за якими присвоюється кваліфікація судового експерта працівникам Експертної служби МВС: Додаток 2 до Положення про Експертно-кваліфікаційну комісію МВС та атестацію судових експертів Експертної служби МВС (пункт 15), затвердженого наказом Міністерства внутрішніх справ України від 08.02.2017 № 102, зареєстровано в Міністерстві юстиції України 01.03.2017 р. за № 275/30143. URL: https://zakon.rada.gov.ua/laws/show/z0275-17 (дата звернення 17.05.2021).

3. Комп'ютерно-технічна експертиза. URL: https://uk.wikipedia.org/wiki//Комп%27ютерно-технічна_експертиза (дата звернення 13.05.2021).

4. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст. 88.

5. Акредитація підрозділів експертної служби МВС. URL: https://dndekc.mvs.gov.ua/акредитація-підрозділів-експертної/ (дата звернення: 03.12.2020).

6. Образ диска. URL: https://uk.wikipedia.org/wiki/Образ_диска (дата звернення 18.05.2021).

7. 1496_508_Test Report_NIST_Disk Imaging_Paladin v6.09_October_14_ 2016.pdf. URL: https://www.dhs.gov/sites/default/files/publications/ (дата звернення 20.05.2021).

8. 1495_508_Test Report_NIST_Disk Imaging_Paladin v6.09_October_14_ 2016.pdf. URL: https://www.dhs.gov/sites/default/files/publications/ (дата звернення: 19.05.2021).