УДК 343.985

В. А. Поліщук
Тернопільський науково-дослідний експертно-криміналістичний центр МВС України, Україна

РОЛЬ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ В РОЗКРИТТІ ТА РОЗСЛІДУВАНІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

V.A. Polischuk

THE ROLE OF COMPUTER-TECHNICAL EXPERTISE IN REVEALING AND INVESTIGATING CRIMINAL OFFENSES

Сучасний світ характеризується стрімким розвитком інформаційних технологій, створенням і розвитком нових методів та засобів передавання зберігання і обробки інформації, суцільної комп'ютеризації суспільства. Злочинний світ також не відстає від загальних тенденцій і активно використовує сучасні технології в своїй протиправній діяльності. Відповідно, для ефективного розкриття та розслідування злочинів правоохоронним органам необхідно йти в ногу з часом та впроваджувати новітні технології. Як показує практика, кількість комп'ютерної техніки, що використовується при здійснені кримінальних правопорушень постійно зростає, при цьому змінюється характер використання даної техніки. Якщо раніше основними об'єктами дослідження виступали персональні комп'ютери, вилучені в процесі розслідування злочинів у сфері інформаційних технологій, то на даний час все більше доказів вдається отримати із засобів комунікацій, мобільних телефонів, смартфонів які вилучаються у зловмисників при вчинені широкого кола правопорушень.

Одним з основних методів використання сучасних інформаційних технологій в правоохоронній діяльності є проведення судових комп'ютерно-технічних експертиз. Даний напрям досліджень є досить молодим і активно розвивається, постійно розробляються і впроваджуються нові методи і засоби проведення досліджень, програмно-апаратні комплекси, тощо.

Комп'ютерно-технічна експертиза в системі МВС проводиться працівниками державних спеціалізованих установ (науково-дослідних експертно-криміналістичних центрів) – атестованими судовими експертами, які мають вищу технічну освіту за напрямком інформаційних технологій, пройшли відповідну підготовку та отримали кваліфікацію за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів».

Основними завданнями даного виду експертиз є:

- пошук та аналіз інформації на цифрових носіях (персональних комп'ютерах, серверах, мобільних пристроях, тощо);
- відновлення видалених даних, пошук прихованої інформації;
- встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;
- встановлення Інтернет активності користувача, кола спілкування, історії використання засобів зв'язку;
- дослідження технічного стану, характеристик, конструктивних особливостей комп'ютерної техніки та мобільних засобів.

З метою розширення кола вирішуваних питань комп'ютерно-технічна експертиза досить часто проводиться в комплексі з іншими видами судових експертиз, такими як: експертиза об'єктів інтелектуальної власності, експертиза матеріалів та засобів відеозвукозапису, технічна експертиза документів, інженерно-транспортна експертиза, мистецтвознавча експертиза.

З постійним розвитком інформаційних технологій збільшуються об'єми даних які обробляються в інформаційних системах, ускладняються алгоритми обробки, передачі та збереження даних, що в свою чергу ускладнює процес проведення комп'ютерно-технічної експертизи. Основні проблемні питання які виникають в процесі проведення дослідження:

- використання засобів шифрування даних користувача (системи BitLocker, FileVault, cryptfs);
- наявність механізмів захисту доступу до носія даних в мобільних пристроях (смартфони Apple iPhone, Samsung Galaxy);
- використання віртуалізації, «хмарних» технологій збереження даних;
- необхідність постійного оновлення апаратних та програмних засобів проведення дослідження;
- відсутність універсальних засобів, необхідність використання при проведені дослідження комплексу різних інструментів.

Набір криміналістичних програмних засобів, які використовуються при проведені експертиз досить широкий, кожен з них має свої переваги і недоліки. Є як безкоштовні утиліти з відкритим кодом, так і професійні програмно-апаратні комплекси ціною від 20000 дол. США. Найбільш поширенішими засобами для проведення криміналістичного аналізу інформації є:

- LiveCD CAINE 3.0 (Computer Aided INvestigative Environment) – спеціалізований завантажувальний дистрибутив, призначений для пошуку прихованих і видалених даних на дисках і виявлення слідів злому інформаційної системи. Дистрибутив створений на основі Ubuntu Linux, розповсюджується вільно;
- AccessData Forensic Toolkit – містить потужний інструмент текстового пошуку, розпізнавання графічного тексту, відновлення видалених файлів, створення гнучких фільтрів і звітів, проводить повне дослідження комп'ютера в рамках судової експертизи;
- X-Ways Forensics - інтегрований комплекс, що дозволяє оперативно вирішувати практично весь спектр завдань комп'ютерної експертизи і розслідування IT інцидентів, від знімання даних до складання звітів.
- EnCase® Forensic комплекс зі зрозумілим графічним інтерфейсом, чудовою аналітикою, поліпшеною email/Internet підтримкою і потужною мовою сценаріїв, оптимізований до проведення масштабних і складних досліджень. Працює на різних платформах - Windows, Linux, AIX, OS X, Solaris і т.д.;
- UFED 4PC - універсальний апаратно-програмний комплекс для криміналістичних досліджень, що дає можливість отримувати, декодувати і аналізувати цифрові дані, отримані з мобільних пристроїв. Комплекс поставляється з набором додатків UFED, периферійними пристроями та аксесуарами, потрібними для успішного проведення досліджень.

Результати проведення комп'ютерно-технічних експертиз досить часто дозволяють встановити обставини, виявити приховані факти, необхідні для розкриття та розслідування правопорушень, підтвердити причетність підозрюваних до вчинення злочинів, створити надійну доказову базу для притягнення злочинців до відповідальності.

Література

1. Закон України «Про судову експертизу», Редакція від 11.10.2017 [Електронний ресурс] / Верховна Рада України – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/main/4038-12 – Дата звернення: 08.11.2017.

2. Россинская Е.Р. Судебная компьютерно-техническая экспертиза : монография / Е.Р. Россинская, А.И. Усов. — М. : Юристъ, 2005. — 625 с.