Носов В.В., доцент, к.т.н., професор кафедри кібербезпеки ХНУВС

ВИКОРИСТАННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Одним із напрямом діяльності Національної поліції України є боротьба із кіберзлочинністю. Терміном кіберзлочин описують кримінальну діяльності, в якій комп'ютери або комп'ютерні мережі є засобом, ціллю або місцем (середовищем) кримінальної діяльності, як окремо так і одночасно у різному поєднанні.

Розслідування кіберзлочинів не можливе без застосування криміналістичних засобів, прийомів і методів збирання, дослідження, оцінки та використання електронних слідів та доказів, джерелом яких є електронні пристрої: комп'ютери та периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери та інші портативні пристрої, в тому числі пристрої для зберігання інформації, а також мережа Інтернет. Інформація з цих джерел не має відокремленої фізичної форми.

Інформаційні технології і електронні пристрої неймовірно швидко змінюються та ускладняються, що відповідним чином вимагає постійного навчання фахівців поліції та розвитку засобів, прийомів і методів збирання, дослідження, оцінки та використання електронних доказів при розслідуванні кіберзлочинів.

Цифрові криміналістичні дослідження широко використовуються і розвиваються в Європейському Союзі та США як державними, та і недержавними інституціями, серед яких:

- Департамент юстиції Сполучених Штатів;
- Національний інститут стандартів та технологій (NIST) Департаменту торгівлі Сполучених Штатів;
- SANS Інститут, США;
- Міжнародна рада консультантів з електронної комерції (EC-Council), США;
- Асоціація з управління і аудиту інформаційної системи (Information System Audit and Control Association, ISACA), США;

- Асоціація керівників органів поліції (The Association of Chief Police Officers, ACPO), Великобританія;
- Європейський центр протидії кіберзлочинності (European Cybercrime Centre, EC3) Європолу, ЄС;
- Octopus спільнота протидії кіберзлочинності (Octopus Cybercrime Community) Ради Європи, ЄС.

Аналіз наявних зарубіжних рекомендацій, настанов і програмних інструментів із проведення цифрових криміналістичних досліджень показав, що існує розрізнена база знань, яку потрібно опрацьовувати і використовувати при розслідуванні кіберзлочинів.

Узагальнений процес отримання електронних доказів згідно [1] можна представити як на рис. 1.

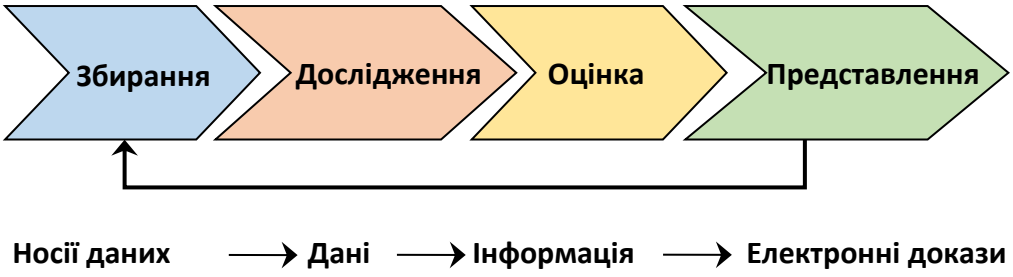

Рис. 1

При *збиранні* електронних доказів на місці події виявляються носії цифрових даних, ці данні фіксуються або вилучаються разом із носієм, забезпечується збереження. При *дослідженні* зібраних даних перевіряється наявність інформації, які є змістом електронних доказів. *Оцінка* інформації, отриманої при дослідженні вилучених даних, встановлює допустимість і відносність доказів, наявність та характер зав'язків між ними, визначає шляхи використання електронних доказів з метою встановлення істини. Далі оцінені докази *представляються* для використання у процесі доказування.

На кожному етапі отримання електронних доказів для різних типів кримінальної діяльності застосовують певні засоби, прийоми та методи. Цифрова криміналістика визначає наступні суттєві для розслідування кіберзлочинів питання:

- поняття, характеристика, прийнятність та принципи роботи з електронними доказами;
- джерела електронних доказів;
- особливості обшуку і вилучення джерел електронних доказів при фізичному та віддаленому доступі;
- пошук доказів в мережі Інтернет;
- окремі аспекти дослідження і оцінки електронних доказів;
- підготовка та представлення електронних доказів.

Розроблені і розвиваються засоби та прийоми криміналістичного дослідження:

- операційних систем Windows, Linux, Mac OS;
- видалених файлів і логічних розділів носіїв даних;
- стеганографічно прихованих та зашифрованих даних;
- журналів протоколювання подій;
- трафіку комп’ютерних мереж;
- бездротових атак;
- атак на веб сервери і застосування;
- електронної пошти;
- мобільних пристроїв.

Таким чином, можна зазначити, що системне опрацювання засобів, прийомів і методів цифрової криміналістики із їх подальшим використанням при розслідуванні кіберзлочинів дозволить якісно змінити ефективність таких розслідувань.

Список використаних джерел.

1. National Institute of Standards and Technology Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response. August 2006. doi:10.6028/NIST.SP.800-86.