Волков Олександр Олександрович,
начальник сектору аналітичної роботи Головного слідчого управління Національної поліції України

ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ЗЛОЧИНАХ, ПОВ'ЯЗАНИХ ЗІ СТВОРЕННЯМ, ВИКОРИСТАННЯМ І РОЗПОВСЮДЖЕННЯМ ШКІДЛИВИХ ПРОГРАМНИХ ЗАСОБІВ

Поняття «електронні докази» уперше згадується в сімдесятих роках минулого сторіччя при появі комп'ютерів, та виготовлення за їх допомогою перших електронних документів. Світовою практикою використовується термін data message, який роз'яснюється ст. 2 Типового Закону про електронну торгівлю 1997 року, який рекомендовано Генеральною Асамблеєю ООН [1], як інформація, що підготовлена, відправлена, отримана або збережена за допомогою оптичних, електронних, електромагнітних або аналогічних засобів, включаючи електронний обмін даними, електронну пошту, тощо.

У злочинах пов'язаних зі створенням, використанням та поширенням шкідливих програмних засобів (далі – ШПЗ) подекуди наявність вини у діях особи, а в деяких випадках взагалі і складу злочину залежить від процесуальних джерел доказів у вигляді показів, речових доказів, документів, а також висновків експертів.

Слідчим під час проведення досудового розслідування рішення приймаються за наявності або відсутності доказів про обставини, які підлягають доказуванню у кримінальному провадженні визначеними у статті 91 КПК України [2].

Законодавцем визначено лише загальне правило допустимості доказів, а саме отримання їх у порядку, встановленому Кримінальним процесуальним кодексом. Що стосується комп'ютерних злочинів, такі докази класифікуються за трьома основними категорії, згідно зі стандартами SWGDE / IOCE: цифровий доказ, це інформація збережена або передана в електронній або магнітної формі; матеріальні предмети, це інформація в цифровому вигляді збережена або передана через її фізичні носії; об'єкти даних, де інформація пов'язана з фізичними матеріальними предметами [3].

У загальному розумінні електронними доказами є будь-яка інформація представлена в електронному (цифровому) вигляді, що представляє собою інформацію про обставини, що мають значення у кримінальному провадженні. Електронні докази можуть міститися у

вигляді текстових, графічних, фото, відео, аудіо файлах. Крім цього, в більш специфічному вигляді міститься технічна інформація (метабази, технічний опис процесу, стану операційної системи, програмного засобу тощо).

Така інформація може знаходитися в директоріях операційної системи, електронних носіях інформації, серверах, хмарних середовищах їх збереження. Місця збереження інформації з плином часу можуть змінюватися, однак основне правило того, що електронна інформація не може існувати без електронного середовища, залишається незмінним.

Зважаючи на це можна зазначити ознаки, що характерні електронним доказам, а саме:

– електронні докази існують виключно в електронному середовищі;

– оригінал електронного доказу може бути в декількох місцях електронного середовища одночасно;

– для сприйняття електронної інформації необхідні як технічні так і електронні програмні засоби;

– створення дублікату електронної інформації здійснюється без втрати характеристик оригіналу.

У кримінальних провадженнях, пов'язаних зі злочинами у сфері створення, використання та поширення шкідливих програмних засобів, виявлення місця значущої для слідства інформації подекуди є недостатнім. Як правило, у таких випадках необхідні спеціальні знання, визначення залежностей між несанкціонованим втручанням в роботу ЕОТ, наявністю ШПЗ та негативними наслідками необхідні спеціальні знання, проведення судових експертиз.

Метою експертизи комп'ютерної техніки і програмних продуктів є збір, збереження, вилучення, аналіз і представлення комп'ютерних доказів. Для проведення експертизи судовий експерт використовує спеціалізоване програмне забезпечення, зазвичай недоступне широкому загалу. Експертиза дозволяє виявляти дані, які знаходяться в комп'ютерній системі, або відновлювати видалену / стерту, зашифровану або пошкоджену ШПЗ інформацію в файлах, а також відновлювати паролі, що забезпечують доступ до інформації.

Таким чином, ці докази можуть бути видимими, якщо вони були збережені в файлах на дисках, або невидимими, коли для їх виявлення потрібне спеціальне програмне забезпечення. Вся інформація, виявлена в процесі експертизи, може бути використана під час досудового розслідування в кримінальному провадженні.

Підводячи висновок слід зазначити, що електронні докази не можуть існувати без електронного середовища, або його носія, їх копіювання здійснюється без будь-яких змін оригіналу та утворення дублікату оригінала документу в іншому місці електронного середовища. Однак, на електронні докази як і на інші докази у кримінальному провадженні поширюється критерії допустимості, передбачені Кримінальним процесуальним законодавством.

Список використаних джерел

1. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market («Directive on electroniccommerce»). URL: http://eurlex.europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

2. Кримінальний процесуальний кодекс України. Київ : Паливода, 2017. 402 с.

3. Forensic science communications. URL: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.