Однак, чинна редакція ст. 17 Закону України «Про судову експертизу», фактично унеможливлює запровадження нових видів експертиз, оскільки для присвоєння кваліфікації судового експерта з нових питань треба обов'язково мати не менше двох фахівців тієї експертної спеціальності і того класу зі стажем експертної роботи не менше 5 років.

Виходячи з викладеного вважаємо, що державою робляться кроки щодо покращення діяльності судово-експертної системи, але цей процес просувається дещо повільно і реформування потрібно продовжувати, поступово викреслюючи негативні фактори з урахуванням потреб фахівців.

Список використаних джерел

1.Про судову експертизу: Закон України від 25 лютого 1994 року № 4038-XII. URL: http://zakon3.rada.gov.ua/laws/show/4038-12.

2.Інструкція з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України, затверджена наказом МВС України від 17.07.2017 № 591. URL: https://zakon.rada.gov.ua/laws/show/z1024-17

3.Кримінальний процесуальний кодекс України [Електронний ресурс]. –Режим доступу: http: // zakon2.rada.gov.ua/laws/show/4651-17.URL: http://zakon2.rada.gov.ua/laws/show/z1024-17/

Омелян Олексій Сергійович,
аспірант Національної академії Служби безпеки України

ЩОДО ОКРЕМИХ АСПЕКТІВ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ В СУЧАСНИХ УМОВАХ (В КОНТЕКСТІ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ)

В сучасних умовах ефективне розслідування будь якого злочину неможливе або дуже ускладнене без використання спеціальних знань, в тому числі й результатів судової експертизи. Особливо це стосується розкриття таких високотехнологічних злочинів, як кіберзлочини, з яких найбільшу суспільну небезпеку становить кібертероризм.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням [1].

Зміст терміну «кібертероризм», крім того, охоплюється поняттям «технологічний тероризм», під яким в статті 1 Закону України «Про боротьбу з тероризмом» визначено: «злочини, що вчиняються з терористичною метою із застосуванням … засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і

руйнування потенційно небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру» [2].

Слід зазначити, що планування, організація, підготовка терористичних актів, підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об’єктів у терористичних цілях, пропаганда і поширення ідеології тероризму, вербування терористів та інші складові, що входять до поняття «терористична діяльність», можуть здійснюватись із використанням технічних можливостей кіберпростору, особливо з огляду на розповсюдження соціальних мереж, інтернет-месенджерів, електронної пошти та голосових інтернет-сервісів (VoIP).

Разом з цим, аналіз ймовірних способів вчинення терористичного акту в кіберпросторі або з його використанням дозоляє стверджувати, що цей вид злочину дуже близький до передбаченого статтею 361 Кримінального кодексу України, який регламентує кримінальну відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Тобто з технічної точки зору механізм вчинення «кібертеракту» фактично не відрізняється від «несанкціонованого втручання».

Таким чином, на нашу думку, нагальною є потреба визначення у вітчизняному законодавстві поняття кібертеракту, яке, на відміну від визначення кібертероризму в Законі України «Про основні засади забезпечення кібербезпеки України», не буде занадто широким, а включатиме чіткі ознаки злочину, зокрема, характерні особливості технічного характеру, що дозволить використати ці ознаки у тому числі, під час призначення судових експертиз.

Варто зауважити, що обсяг спеціальних знань у сфері інформаційних технологій при розслідуванні кіберзлочинів є значно ширшим за обсяг «звичайних» спеціальних комп’ютерних знань, що використовуються під час досудового розслідування інших злочинів. У даному випадку ефективність пошуку, виявлення, фіксації та вилучення цифрових слідів правопорушення потребує також досконалих знань способів вчинення кіберзлочинів.

Співробітнику кіберполіції чи слідчому, який не володіє спеціальними знаннями, самостійно буде складно відрізнити, наприклад, збій в роботі апаратури або ненавмисну помилку оператора від наслідків цілеспрямованої кібератаки, зокрема, із застосуванням шкідливого програмного забезпечення. Або, наприклад, зрозуміти переповнені технічними термінами пояснення адміністратора атакованої системи. При цьому слід враховувати, що

адміністратор міг бути спільником злочину або міг неналежним чином налаштувати систему, внаслідок чого кібератака стала можливою. Зрозуміло, що в такому випадку він намагатиметься приховати від правоохоронних органів вказані дії. Виявити протиріччя у словах адміністратора слідчому без спеціальних знань за вказаним фахом буде вкрай складно або навіть цілком неможливо.

Таким чином, відсутність у слідчого (оперативного співробітника) спеціальних знань може викликати труднощі при вирішенні основних завдань проведення слідчих (розшукових) дій: виявлення елементів складу кіберзлочину, виходячи зі слідової інформації; встановлення обстановки вчинення кіберзлочину, часу, місця, способу, мотивів і знарядь його вчинення; визначення предмету злочинного посягання; визначення розміру заподіяної шкоди; виокремлення характерних ознак виду кіберзлочину; встановлення інших осіб, причетних до вчинення кіберзлочину, а також способу його приховування.

Крім теоретичних знань у сфері комп'ютерних технологій необхідні й практичні навички роботи з комп'ютерним і телекомунікаційним обладнанням, а також спеціалізованим програмним забезпеченням. Крім того, як вже зазначалося, необхідні знання способів та методів реалізації кібератак. Це дозволить найбільш ефективно застосовувати спеціалізовані криміналістичні програмно-апаратні засоби для пошуку, фіксації, вилучення та подальшого дослідження цифрових слідів кіберзлочину.

До спеціалізованих засобів для виявлення цифрових слідів кіберзлочинів можна віднести:

- експертне програмне забезпечення для криміналістичного дослідження комп'ютерних носіїв інформації, наприклад «Forensic Toolkit», «EnCase Forensic», «X-Ways Forensics»;
- мобільні комплекси, що дозволяють добувати, декодувати та аналізувати цифрову інформацію, отриману з мобільних пристроїв, зокрема «Cellebrite UFED Touch 2», «MSAB XRY Field»;
- програмне забезпечення з відновлення комп'ютерних даних «R-Studio», «UFS Explorer» тощо.

При розслідуванні кіберзлочинів, а особливо кібертерактів, актуальним є залучення спеціаліста (носія спеціальних знань у сфері ІТ) для таких дій:

– на етапі підготовки кожної слідчої дії;

– при пошуку слідів злочину, для виявлення яких потрібне спеціальне апаратне і (або) програмне забезпечення;

– для підбору понятих, які володіють навичками роботи з комп'ютерною технікою та телекомунікаційними мережами і володіють знаннями в сфері комп'ютерних технологій (щоб мати змогу кваліфіковано описати в суді дії правоохоронці та підтвердити дотримання закону);

– для внесення в протоколи слідчих дій додаткових наочних матеріалів (схем топології мережі, скріншотів вікон програм, роздруківок звітів діагностичних утиліт чи лог-файлів тощо);

– для правильного вилучення та упакування комп’ютерної техніки, телекомунікаційного обладнання та інших засобів вчинення злочину;

– на етапі призначення експертизи для правильного формулювання питань та вибору необхідних для проведення експертизи об’єктів тощо.

Підсумовуючи вищенаведене, незважаючи на існуючі наукові напрацювання [3, 4, 5], нагальною залишається потреба у комплексному науковому дослідженні проблемних питань використання спеціальних знань при розслідуванні кіберзлочинів, а також системних змін в українському законодавстві у сфері протидії кібертероризму. Вказані законодавчі зміни повинні торкнутися не лише удосконалення та уніфікації термінологічного апарату, але й розподілу підслідності і визначення нових механізмів взаємодії суб’єктів, задіяних у сфері протидії кібертероризму.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII / база «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.10.2019)

2. Про боротьбу з тероризмом: Закон України від 20 березня 2003 року № 638-IV / база «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 15.10.2019)

3. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

4. Карчевський М. Кібертероризм: поняття та питання кримінально-правової кваліфікації / Протидія терористичній діяльності: міжнародний досвід і його актуальність для України: матеріали міжнародної науково-практичної конференції (30 вересня 2016 року). – К.: Національна академія прокуратури України, 2016. – С. 137-142.

5. Нізовцев Ю. Ю. Судово-експертне дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні: методичні рекомендації / Ю. Ю. Нізовцев. – Київ: Видавничий дім «АртЕк», 2016. – 118 с.