Список використаних джерел

1. Судебно-почерковедческая экспертиза: общая часть: теор. и метод. основы / под науч. ред. В.Ф. Орловой. 2-е изд. перераб. и доп. Москва: Наука, 2006. 544 с.

2. Томилин В.В. Физиология, патология и судебно-медицинская экспертиза письма. Москва, 1963. 235 с.

Долженко Любов Юріївна,
судовий експерт сектору дослідження звуко- та відеозапису відділу досліджень у сфері інформаційних технологій Харківського НДЕКЦ МВС України

КІБЕРЗЛОЧИННІСТЬ: КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА Й ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ

Розвиток всесвітньої мережі Інтернет спричинив новий вид злочинності – кіберзлочинність, який з кожним роком набирає свої оберти і несе за собою серйозні, а часом, незворотні наслідки.

Дії кіберзлочинців стають більш досконалими, що становить реальну загрозу для суспільства та держави в цілому. Це загострює необхідність боротьби зі злочинами такого роду, як створення комп'ютерних систем і технологій з підвищеним рівнем безпеки в мережі Інтернет, а також законодавчої бази, що дозволить притягнути злочинців до відповідальності.

В українському законодавстві кіберзлочин розуміється як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

Специфіка даного виду злочинності полягає у:

комфортності вчинення злочинів, тобто їх підготовка та скоєння здійснюється, практично, не відходячи від «робочого місця»;

доступності – тому що існує тенденція постійного зниження цін на комп'ютерну техніку. Майже у кожної людини є комп'ютер або мобільний телефон з підключенням до мережі Інтернет;

широкій географії скоєння злочинів, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає більша частина злочинності;

віддаленості об'єкту злочинних посягань – він може знаходитись за тисячі кілометрів від місця скоєння злочину;

складності виявлення, фіксації та вилучення криміналістично-значущої інформації при здійсненні оперативно-розшукових та слідчих (розшукових) дій для використання її як речового доказу.

Слід зауважити, що український законодавець приділяє велику увагу цій проблемі: вперше новий Кримінальний кодекс України передбачив самостійний розділ про ці злочини, а саме розділ XVI

«Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», що свідчить про актуальність цієї проблеми в суспільстві, зокрема статті 361, 361-1, 361-2, 362, 363, 363-1 Кримінального кодексу України [1].

Об'єкт злочину – сукупність діянь, що заподіюють шкоду нормальній роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку [3].

Суб'єкт злочину загальний, тобто суб'єктом є фізична осудна особа, яка вчинила злочин у віці, з якого відповідно Кримінального кодексу України може наставати кримінальна відповідальність, тобто особа, якій до вчинення злочину виповнилося шістнадцять років [1].

Об'єктивна сторона злочину проявляється у формі несанкціонованого втручання у роботу електронно-обчислювальних машин (комп'ютерів), їх систем, комп'ютерних мереж чи мереж електрозв'язку, наслідком якого є: витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації [3].

Суб'єктивна сторона злочину характеризується умисною виною. Злочинні дії можуть бути вчинені лише з прямим умислом, тоді як психічне ставлення винного до наслідків може характеризуватись як умисною (прямим чи непрямим умислом), так і необережною формою вини (злочинною самовпевненістю чи злочинною недбалістю) [3].

Одним з масштабніших злочинів, якій заподіяв багато негативних наслідків є «вірус Petya». Це була масштабна хакерська атака. Хакерські атаки в Україні – це цілеспрямовані масштабні хакерські напади на мережі українських державних підприємств, установ, банків, медіа тощо, які відбулись 27 червня 2017 року. У результаті цих атак була заблокована діяльність наступних підприємств: аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та ряд великих комерційних підприємств. Шахраї вимагали внести визначену грошову суму на їх рахунки для відновлення і подальшої роботи сайтів.

На жаль, Україна зіштовхнулась ще з однією проблемою, такою як COVID-19 (короновірус). Після виявлення цього захворювання, держава повинна була ввести карантинні заходи. Для багатьох людей це велика трагедія, а для шахраїв ще один різновид заробітку. З початку карантину шахраї розсилають СМС-повідомлення або телефонують та повідомляють інформацію про державні компенсації для громадян, такі як: виплата коштів на лікування, придбання тестів для визначення короновірусу, компенсація за втрату місця роботи тощо; розповсюджують фейки з метою поширення паніки та дестабілізації ситуації в країні в умовах карантину; вчиняють певні шахрайські дії з метою заволодіння грошима чи особистими даними

під приводом продажу захисних масок, антисептиків, медичного обладнання тощо.

Розслідування таких злочинів ускладняється їх підвищеною латентністю. У злочинців є можливість змінити, приховати комп'ютерні дані, що можуть бути доказами у досудовому розслідуванні.

Першочерговим завданням слідчого на початковому етапі розслідування кіберзлочинів є аналіз інформаційного середовища вчинення злочину:

визначення типу електронно-обчислювальної машини (носія), де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ, що визначить напрямок всього подальшого розслідування;

встановлення типу операційної системи комп'ютера (сервера), до якого здійснено неправомірний доступ, а також використаного для вчинення злочину програмного забезпечення, що значною мірою допоможе звузити коло можливих підозрюваних;

визначення апаратного та програмного забезпечення, яке піддалося впливу в ході неправомірного доступу, а також інформації про засоби і знаряддя вчинення такого доступу, що дозволить скласти об'єктивну картину слідів злочину [4].

Важливою умовою боротьби з кіберзлочинністю є підготовка фахівців належної кваліфікації для збільшення ефективності розслідування та розкриття злочинів даної специфіки.

В Україні існує Департамент кіберполіції Національної поліції України, завданням якого є забезпечити кібербезпеку країни і запобігти кіберзлочинності. Але немає єдиної бази ключових термінів і понять, не розроблені криміналістичні техніка та тактика, використовуючи які співробітники кіберполіції змогли б ефективніше проводити розслідування кіберзлочинів.

Таким чином, сучасний рівень інформатизації суспільства вимагає від України забезпечити належний та ефективний механізм боротьби із кіберзлочинами як однієї із серйозних загроз національній безпеці держави.

Список використаних джерел

1. Кримінальний кодекс України: Закон України від 05 квітня 2001 р. №2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/print. (Дата звернення 06.10.2020)

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/card/2163-19. (Дата звернення 08.10.2020).

3. Науково-практичний коментар до Кримінального кодексу України / відп. ред. С. С. Яценко. 4-те вид., перероб. та доп. К.: А.С.К., 2005. 848 с. URL: http://ir.nusta.edu.ua/jspui/handle/doc/819. (Дата звернення 07.10.2020).

4. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності. Актуальні питання розслідування кіберзлочинів: матеріали Міжнар. наук.-практ. конф. (м. Харків: 10 груд. 2013 р.). Харків: ХНУВС, 2013. С. 179–181.

Драган Діана Миколаївна,
здобувач ступеня вищої освіти бакалавра
ННІ № 3 Національної академії внутрішніх справ
Науковий керівник: ***Антонюк П. Є.,***
професор кафедри криміналістики
та судової медицини Національної академії
внутрішніх справ, кандидат юридичних наук

СТРУКТУРА КРИМІНАЛІСТИКИ ЯК НАУКИ В ІНОЗЕМНИХ КРАЇНАХ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Одним із напрямів вирішення проблеми підвищення ефективності протидії кримінально протиправній діяльності в Україні є впровадження в роботу правоохоронних органів новітніх техніко-криміналістичних засобів, прийомів, методів збирання, дослідження й використання доказів, розробленням яких займається криміналістика – самостійна наука юридичного циклу.

Запозичуючи досвід зарубіжних країн по боротьбі з кримінально протиправною діяльністю в практику вітчизняних правоохоронних органів, цікавим є, на наш погляд, розуміння, в рамках яких наукових знань відбувається розроблення системи наукових методів, прийомів та засобів протидії кримінально протиправній діяльності в інших країнах світу.

Наприклад, в США та інших країнах англо-саксонської системи права найбільш близькою до криміналістики дисципліною нерідко вважають ForensicScience, яка являє собою застосування будь-яких наукових методів і технік у кримінальному розслідуванні та судовому розгляді. Тобто вітчизняну криміналістику об’єднує з Forensic Science лише криміналістична техніка, яка в Україні входить до складу криміналістичної науки, а в США є частиною Forensic Science. При цьому, Forensic Science за сутністю є сукупністю судових наук. Тому в США немає єдиного підходу до її структури. За одними джерелами до її дисциплін відносяться судова патологія, антропологія, одонтологія, ентомологія, токсикологія, психіатрія, дослідження слідів-предметів, дослідження зброї та слідів її застосування, дослідження документів, дослідження слідів пальців рук, дослідження ДНК, аналіз слідів крові, аналіз слідів-відображень,дослідження комп’ютерних засобів, судові інженерні науки тощо. В інших працях, крім деяких згадуваних, до змісту Forensic Science також включають: хімічні дослідження наркотичних засобів, судову біологію, дослідження мікрооб’єктів, поліграфічний аналіз, дослідження слідів-речовин, криміналістичний