УДК 343.9

Наталя Іванівна МАЗНИЧЕНКО,
старший викладач кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого;
ORCID: https://orcid.org/0000-0002-2295-2622

ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ СЛІДІВ ПРОТИПРАВНИХ ДІЙ, ЗДІЙСНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Проникнення інформаційних і телекомунікаційних технологій в усі сфери громадського життя є необхідною умовою для переходу до інформаційного суспільства. Проте інформаційні технології дали поштовх не лише розвитку суспільства, але і стимулювали використання їх в протиправних діях.

Сучасний технічний прогрес у сфері розвитку комп'ютерних і інформаційних технологій породжує принципово нові громадські стосунки, які і стають предметом злочинних посягань. Злочинці використовують сучасні досягнення інформаційних технологій для скоєння злочинів новими способами і за допомогою нових знарядь. Навіть таки традиційні злочини, як крадіжка, шахрайство в наше століття здійснюються за допомогою мережі Інтернет. Новими є лише знаряддя здійснення – веб-сайт, електронна пошта, платіжна система. Крім того, з'явилася безліч нових, раніше невідомих способів злочинів у сфері комп'ютерної інформації і високих технологій.

На сьогоднішній день високотехнологічні пристрої (телефони, смартфони, комп’ютери, цифрові фотоапарати, відеокамери, відео регістратори та інші) та інформаційно-комунікаційні мережі все частіше використовують для підготовки, скоєння та приховування злочинів.

За тривалий час існування криміналістика накопичила величезний обсяг знань та досвід. Проте з появою нових способів скоєння злочинів з використанням сучасних комп’ютерних та інформаційно-комунікаційних технологій (далі – кіберзлочинів) цих знань стає недостатньо для виконання основних завдань криміналістики – забезпечення швидкого і повного розкриття зазначених злочинів. За статистикою кількість кіберзлочинів зростає щороку і не тільки в Україні, а і у всьому світі, у зв’язку з чим актуальним для сучасної криміналістики стають задачі розробки нових та вдосконалення існуючих підходів забезпечення розкриття, розслідування та попередження таких злочинів.

Специфічність даного виду злочинів визначає і особливості їх розслідування та розкриття. Слід відзначити, що в зарубіжній літературі виділяють окремий напрямок – forensics (скорочення від «forensic science») – розділ криміналістики, що вивчає цифрові докази.

Процес розслідування злочинів включає виконання слідчих дій, проведення оперативно-розшукових і організаційних заходів, які спрямовані на виявлення, збирання, дослідження, фіксацію, оцінку доказової інформації і встановлення істини у кримінальній справі. Будь-яка діяльність в комп’ютерній системі або в мережі залишає специфічні сліди. Протиправна діяльність з використанням сучасної комп’ютерної та інформаційно-комунікаційної техніки також залишає сліди. Ці сліди в науковій літературі визначають по різному: комп’ютерні, віртуальні, цифрові, електронно-цифрові. На мою думку найбільш вдале визначення надав Вехов В.Б. [1, с. 95] (мовою оригіналу): «Электронно-цифровой след – это любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов». Враховуючі особливість електронно-цифрових слідів до криміналістичного процесу крім стандартних етапів (збирання, дослідження, фіксація, оцінка) можна додати ще один – забезпечення збереження. Таким чином процес збирання доказів при скоєнні кіберзлочинів можна розділити на наступні етапи:

– збереження («заморожування місця злочину») – припинення або попередження будь-яких дій, що можуть нанести шкоду збиранню цифрової інформації. Включає такі операції, як припинення використання комп'ютерів під час збирання, припинення процесів видалення інформації (запобігти видаленню слідів), вибір безпечних способів збору інформації і т.д.

– збирання – знаходження (виявлення) і збір цифрової інформації, що може мати відношення до розслідування. Включає такі операції, як вилучення обладнання, що містить таку інформацію, копіювання інформації на будь-який носій (або друк), запис мережевого трафіка і т.д.

– дослідження – поглиблений систематичний пошук доказів в зібраній цифровій інформації. Доказами можуть бути файли даних, що містять певну інформацію, дані журналів (наприклад, журналу адміністрування), часові мітки і т.д.

– оцінка (аналіз) – зробити висновки на основі зібраних доказів.

– представлення – оформлення результатів дослідження і аналізу в установленій законом формі.

Для здійснення всіх перерахованих дій з електронно-цифровими слідами крім глибоких знань в галузі криміналістики необхідні і спеціальні знання. Дослідник електронно-цифрових слідів повинен вміти збирати та аналізувати дані на всіх пристроях з цифровим сховищем, включаючи комп'ютери, мобільні пристрої та мережі, не зважаючи на те, що інформація про комп'ютерну систему може бути змінена без сліду, масштаб даних, які необхідно проаналізувати, великий, а різноманітність типів даних величезна.

Для роботи з електронно-цифровими слідами слідчі і фахівці повинні застосовувати спеціальні засоби, які включають апаратні засоби та програмне забезпечення. До апаратних засобів можна віднести безпосередньо сам комп'ютер як універсальний інструмент для обробки інформації в електронному вигляді, так і спеціалізовані апаратні криміналістичні пристрої [2, с. 30] для роботи з комп'ютерними системами та мобільними цифровими пристроями. Можна навести наступні приклади сучасних програмно-технічних комплексів, які застосовуються для добування та обробки інформації в електронній формі з різноманітних електронних пристроїв: ImageMASSter Solo-4 Forensic, EPOS DiskMaster Portable, EPOS FlashExtractor, «Мобильный криминалист», «XRY», «MOBILedit», «TARANTULA EDEC», універсальний пристрій для криміналістичного дослідження мобільних пристроїв «UFED» (Universal Forensic Extraction Device) [3].

Щодо програмного забезпечення, то тут можуть бути застосовані як можливості системного програмного забезпечення або програмного забезпечення загального призначення, так і спеціалізоване програмне забезпечення. Наприклад, для отримання потрібної інформації можна звернутись до системного реєстру (з'ясування останніх дій з встановленням, видаленням, налаштуванням програм); дослідити log-файли (протоколи автоматичної реєстрації події, що відбуваються при роботі програмного забезпечення); отримати інформацію з журналів веб-браузерів стосовно діяльності в мережі (які web-сторінки відбудувались). Для отримання більш докладної інформації про мережеві ресурси, домени, їх власників потрібно вже спеціальне програмне забезпечення. Також може бути в нагоді програмне забезпечення для відновлення видаленої, модифікованої, пошкодженої інформації з носіїв інформації (наприклад, R – Studio, EASYUS File Recovery, Ontrack Easy Recovery та ін.). Для змістовного аналізу інформації може бути застосовано програмне забезпечення з можливостями контент-анализу, що сприяє підвищенню ефективності моніторингу мережевих інтернет-ресурсів в місцях мережевого спілкування (соціальні мережі, форуми, блоги та ін.), а також мережевих ресурсів з високою потенційною можливістю розміщення інформації кримінального характеру. Для дослідження вмісту носіїв інформації корисними можуть бути експертні програми: ProDiscover, SMART, Forensic Toolkit, Encase та інші [2, с. 30].

Як бачимо, для роботи з електронно-цифровими слідами необхідно враховувати не лише поглиблені знання в галузі криміналістики, а і в області комп'ютерної техніки, інформаційних технологій, програмного забезпечення і не на рівні звичайного користувача, а на професійному рівні. Також потрібно мати практичні навички, отримані в результаті

професійної діяльності, а також предметну спеціалізацію експерта і фахівця. Ці знання можуть бути використані не лише для грамотного виявлення, збирання, безпечного збереження, дослідження, фіксації електронно-цифрових слідів, але і під час виконання слідчих дій, судових експертиз і оформлення висновків експертиз.

Список бібліографічних посилань: 1. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : моногр. Волгоград : ВА МВД России, 2008. 408 с. **2.** Федотов Н. Н. Форензика – компьютерная криминалистика. М. : Юрид. мир, 2007. 432 с. **3.** Рогова И. А., Бурцева Е. В. Практика применения UFED – универсального устройства для криминалистического исследования мобильных устройств. *Евразийский Союз Ученых.* 2015. № 7 (16), ч. 5. С. 97–100.

Одержано 17.10.2018

УДК 347.9

Аліна Русланівна МАКСЮТА,
студент-магістр юридичного факультету
Харківського національного університету імені В. Н. Каразіна

МІСЦЕ ПРОКУРАТУРИ УКРАЇНИ В СИСТЕМІ ПРАВООХОРОННИХ ОРГАНІВ

На сучасному етапі розвитку української держави на правоохоронні органи покладається низка важливих завдань. Для правильного визначення місця органів прокуратури в системі правоохоронних органів слід детально проаналізувати зазначене поняття. Так, чіткого визначення терміну «правоохоронні органи» в законодавчих актах не закріплено. Слід зауважити, що термін «правоохоронні органи» визначається в ст. 2 Закону України «Про державний захист працівників суду і правоохоронних органів» [1]. До них відносяться органи прокуратури, Національної поліції, служби безпеки, Військової служби правопорядку у Збройних Силах України, Національне антикорупційне бюро України, органи охорони державного кордону, органи доходів і зборів, органи і установи виконання покарань, слідчі ізолятори, органи державного фінансового контролю, рибоохорони, державної лісової охорони, інші органи, які здійснюють правозастосовні або правоохоронні функції.

У науковій літературі інколи вживається термін «органи правопорядку». Вказаний термін є досить дискусійним. Н. Ярмиш стверджує, що термін «органи правопорядку» вчені у своїх працях використовують досить рідко, тож є підстави вважати, що він сформульований саме авторами проекту Закону України «Про внесення змін до Конституції України (щодо правосуддя)» [2, с. 80]. Вищевказаним Законом Конституцію України [3] було доповнено ст. 131-1, у якій зазначено, що в Україні діє прокуратура, яка здійснює організацію і процесуальне керівництво досудовим розслідуванням, вирішення відповідно до закону інших питань під час кримінального провадження, нагляд за негласними та іншими слідчими і розшуковими діями органів правопорядку.

Деякі вчені пропонують власні визначення поняття «правоохоронні органи». Наприклад, на думку В. В. Сухоноса, правоохоронні органи – це державні органи, які реалізують правоохоронну і правозахисну функції держави, вживають заходів щодо виявлення і попередження злочинів та інших правопорушень, а також причин, що їх зумовили, і наділені законом повноваженнями застосовувати у разі необхідності державний примус і притягати винних до юридичної відповідальності. Усі правоохоронні органи доцільно поділяти на дві групи:

1) державні органи, основним завданням яких є попередження, розкриття та розслідування злочинів, застосування юридичних санкцій до правопорушників;

2) державні органи, для яких зазначена діяльність не є основною і визначальною та які переважно виконують управлінські й контрольні функції [4, с. 360–361].