З метою ефективного збирання цифрових даних під час протидії злочинності поліції часто доводиться залучати відповідних спеціалістів. Так, наприклад, представники Експертної служби МВС України у 2014 році взяли участь у 13656 оперативно-розшукових заходах, у 2015 році таких випадків було 9380. У 2016 році працівники експертної служби 190 раз брали участь у здійсненні негласних слідчих (розшукових) дій.

Вказана ситуація свідчить на користь збільшення ролі цифрових даних, зібраних під час негласної роботи, для вирішення завдань ефективної протидії злочинності. Водночас брак фахівців з комп'ютерно-технічної експертизи викликає нагальну потребу у підвищенні рівня знань та вмінь у сфері збирання та використання цифрових даних саме пересічних оперативних працівників та слідчих. Наразі в Україні підвищення кваліфікації щодо застосування високих технологій у протидії злочинності переважно ведеться у кіберполіції, при цьому інші підрозділи нерідко залишаються поза увагою науковців та інших фахівців під час розробки відповідних рекомендацій та надання практичної допомоги. Вказане зумовлює необхідність опрацювання теоретичних та практичних особливостей негласної діяльності підрозділів національної поліції щодо пошуку та використання цифрових доказів.

Одержано 14.10.2017

УДК 343.98

Яна Анатоліївна СОКОЛОВА-ВИСОЧИНА,
кандидат юридичних наук, доцент, старший викладач відділу підготовки прокурорів з нагляду за додержанням законів органами, які проводять оперативно-розшукову діяльність, дізнання та досудове слідство Національної академії прокуратури України

АКТУАЛЬНІ ПИТАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Розвиток та впровадження сучасних інформаційних технологій у всі сфери суспільного життя та економіки в Україні дає можливість використовувати їх, зокрема, й з корисливих та інших мотивів. Інформаційні технології також надають нові можливості для злочинної діяльності, комп'ютер «забезпечує» і нові види злочинів, і нові способи вчинення вже звичних протиправних діянь. Протидія злочинам, вчиненим із застосуванням інформаційних технологій, є новим викликом для правоохоронних органів [1, с. 6, 143].

Підвищений інтерес злочинців до Інтернету не випадковий. Унікальність глобальної мережі полягає в тому, що вона не перебуває у віданні конкретної фізичної особи, приватної компанії, державної або громадської організації чи навіть окремої держави. Використання телекомунікаційних мереж дає можливість вчинити злочин, не виходячи з дому, офісу, не покидаючи межі своєї країни, або одночасно з території декількох держав. Відсутні будь-які форми контролю за інформацією, що відкриває необмежені можливості для доступу до неї та її використання злочинцями. Зазначене обумовлює транснаціональний, організований, груповий характер багатьох кіберзлочинів [2, с. 15].

Кіберзлочинність є явищем міжнародного значення, рівень якого перебуває у прямій залежності від рівня розвитку та впровадження сучасних інформаційних технологій. Відбувається консолідація ІТ-злочинців у групи з подальшим їх укрупненням до злочинних угруповань, злочинних організацій, що діють на постійній основі – «професійна кіберзлочинність». Також має місце швидке налагодження та зміцнення зв'язків між злочинними угрупованнями, що дає змогу забезпечити оперативний обмін інформацією, здійснення обміну прийомами та способами вчинення злочинів, способами переведення електронних коштів у готівку тощо [3, с. 93].

У науковій літературі зазначається, що з'явився новий напрям науково-практичної діяльності – інформаційні технології процесуального доказування, що виник в умовах інформаційного суспільства на стику правових та природничо-технічних наук. Він покликаний забезпечити ефективність правосуддя шляхом включення у процедуру його здійснення найбільш ефективних сучасних інформаційних технологій. Не лише злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, але й багато «традиційних» суспільно небезпечних діянь залишають після себе електронні сліди у комп'ютерних мережах, на магнітних чи оптичних носіях, екранах моніторів. У зв'язку з цим виникає практична проблема використання зазначених слідів під час досудового розслідування [4, с. 313].

Розслідування кіберзлочинів також ускладнене певними особливостями: латентністю; можливістю знищення або зміни комп'ютерної інформації, що є доказом вчинення злочину; виникненням проблеми під час огляду комп'ютерних систем, ви-

лучення та дослідження слідів, які зберігаються в пам'яті технічних пристроїв, в електромагнітному полі, на машинних носіях комп'ютерної інформації; короткочасністю зберігання інформації, здатної виступити як доказ на серверах компаній – операторів телекомунікаційних мереж тощо [5, с. 180].

Саме тому викликом сучасності, що постав перед криміналістичною теорією і практикою, є необхідність вивчення електронних слідів як явища об'єктивної дійсності й розроблення криміналістичних рекомендацій щодо найбільш ефективного їх виявлення, дослідження, фіксації, вилучення й використання у діяльності з розслідування й попередження злочинів. Адже потенціал використання електронних слідів у діяльності органів кримінальної юстиції з розшуку та ідентифікації осіб, запобігання правопорушенням тощо, залишається на неприпустимо низькому рівні [6, с. 426].

Список використаних джерел:

1. Болгов В. М., Гадіон Н. М., Гладун О. З. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посібник. Київ: НАПУ, 2015. 202 с.
2. Гусаров С. М. Розслідування кіберзлочинів органами внутрішніх справ України: наукове та кадрове забезпечення // Актуальні питання розслідування кіберзлочинів : матеріали міжнародної науково-практичної конференції, м. Харків, 10 грудня 2013 року. Харків: ХНУВС, 2013. С. 14-18.
3. Шапочка С. В. До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет. Правова інформатика. 2014. № 3(43). С. 89–95..
4. Мурадов В. В. Електронні докази: криміналістичний аспект використання. Порівняльно-аналітичне право. 2013. № 3-2. С. 313–315.
5. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності // Актуальні питання розслідування кіберзлочинів: матеріали міжнародної науково-практичної конференції, м. Харків, 10 грудня 2013 року. Харків: ХНУВС, 2013. С. 179–182.
6. Білоус В.В. Електронні сліди як актуальний напрямок криміналістичних досліджень // Правове життя сучасної України : матеріали міжнародної наукової конференції, м. Одеса, 20–21 квітня 2012 р. Т. 2. Одеса: Фенікс, 2012. С. 425–427.

Одержано 01.11.2017