Наступною проблемою взаємодії підрозділів досудового розслідування та оперативних підрозділів, являється те, що слідчий в більшості випадках досить мало, або ж взагалі не знає норм оперативно-розшукового законодавства, не розуміється в нюансах проведення оперативно-розшукової діяльності, оперативно-розшукових заходів. Саме це впливає на швидкість та ефективність їх спільної роботи, бо оперативному працівникові складно довести слідчому про необхідність проведення тої чи іншої негласної слідчої (розшукової) дії під час розслідування кримінального правопорушення.

Отже, можемо дійти висновку, що слідчі та оперативні підрозділи в розкритті та розслідуванні злочинів будуть мати достатній рівень ефективності, тільки в разі спільної взаємодії, яка вимагає детального спільного планування, обговорення думок, участі в проведенні окремих слідчих і розшукових дій, така форма взаємодії додасть спільній діяльності цілеспрямованості і більшої організованості. Вдосконалення системи управління, організації та контролю потребують швидкого вирішення, адже від цього залежить якість, повнота та швидкість розкриття кримінальних правопорушень, що готуються чи були вчинені.

Одержано 19.11.2019

УДК 351.95

Роман Романович РОМАНІВ,
курсант групи Ф4-201 факультету № 4
Харківського національного університету внутрішніх справ

Науковий керівник:
Ірина Дмитрівна КАЗАНЧУК,
доцент кафедри адміністративного права та процесу
факультету № 1 Харківського національного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ОСОБЛИВОСТІ ДІЯЛЬНОСТІ КІБЕРПОЛІЦІЇ ЩОДО ВИЯВЛЕННЯ ТА ПРОФІЛАКТИКИ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

Стрімкий розвиток інформаційних технологій трансформує світ, поступово створюючи інформаційне суспільство. Водночас впровадження в життя людини новітніх інформаційних

технологій викликало появу такого негативного явища як кіберзлочинність. Це явище стало транснаціональним і здатне завдати значної шкоди інтересам кожної людини, суспільства і держави.

Кіберзлочин – це злочин, вчинений у віртуальному просторі (інформаційній мережі Інтернет), створеному за допомогою комп'ютерів, де містяться особисті дані користувачів. До кіберзлочину можна віднести зламану сторінку в соцмережі або «зламаний» телефон, створення та розповсюдження вірусів і шкідливого програмного забезпечення, здійснення незаконного підміну телефонного трафіку (рефайлінг), вкрадені паролі від банківських карт або втручання в роботу системи банків, несанкціонований доступ до інформаційної мережі СБУ та інших правоохоронних органів. При цьому цілі кіберзлочинів можуть бути найрізноманітнішими: вкрасти гроші з банківської карти або, зламавши телефон відомої людини, викласти її селфі-фото в інтернет, викрасти стратегічні документи або «обвалити» фондовий ринок тощо [1]. З'явилася велика кількість шахраїв, які під виглядом добросовісних продавців пропонують у Інтернет-мережі надання неіснуючих послуг та намагаються продати різний товар, якого насправді в них немає. Це може бути як електрообладнання, будівельні матеріали, цифрова, відеотехніка та інше.

З 2015 року в структурі кримінальної поліції Національної поліції України діє Департамент кіберполіції, фахівці якого працюють над виявленням й розкриттям злочинів, скоєних у Інтернет мережі. Створення кіберполіції в Україні в ході реформування та розвитку системи МВС України забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних і слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності [2]. До речі, з вересня 2016 року на базі Харківського національного університету внутрішніх справ працівники Департаменту кіберполіції проходять курси з підвищення кваліфікації, в рамках якого слухачам довелося пройти не лише складний попередній відбір, але і закінчити 760-годинне навчання та витримати 4 місячний курс підготовки. Додатково в Києві були проведені тренінги за участі британських експертів.

Діяльність кіберполіції, як міжрегіонального територіального органу поліції, відповідно до законодавства України, спрямована на: забезпечення реалізації державної політики у сфері боротьби з кіберзлочинністю, організацію і здійснення оперативно-розшукової діяльності, інформування населення про появу нових кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів, реагування на запити зарубіжних партнерів, які надходять по каналах Національної цілодобової мережі контактних пунктів [3].

В ході виконання важливих завдань кіберполіція виконує такі функції:

- визначає, розробляє та забезпечує реалізацію комплексу заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності;
- у межах своїх повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності;
- уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, у тому числі об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень;
- проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті;
- забезпечує формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності;
- організовує виконання, у межах компетенції, доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях та інше.

Кіберполіцейські звертають увагу інтернет-користувачів на той факт, що інколи зловмисники викуповують доменні імена сайтів, які раніше добросовісно надавали послуги покупцям, і намагаються видати новий сайт за ресурс,

який надає такі самі послуги, а інколи навіть може мати такий самий вигляд, як і старий ресурс. У такому випадку користувач навіть може знайти в інтернеті велику кількість позитивних відгуків про цей сайт, однак потрібно звертати увагу на останню дату залишеного коментаря, радять кіберполіцейські [4].

Отже, враховуючи важливу роль кіберполіції, потрібно нарощувати та розширювати її можливості, аби наперед прораховувати кроки злочинців в Інтернет-просторі. Відтак в штат кіберполіції слід ввести додаткові посади, які передбачать новий напрямок роботи, у першу чергу, виконання превентивної функції, спрямованої також на інформування населення про розповсюджені прийоми, які використовують злочинці в Інтернет мережі для того, щоб розпізнавати їх. Це дасть змогу оперативно розкривати кіберзлочини, визначати чинники, які сприяють їх скоєнню, завчасно виявляти протиправний контент (контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства) та зловмисників до того, як вони скоять кіберзлочин, і взагалі – покращать роботу колег з інших підрозділів поліції (карного розшуку та слідчих органів) в рамках кримінальних проваджень у розкритті злочинів, учинених із застосуванням високих інформаційних технологій.

Список бібліографічних посилань

1. Коротка Н. Що таке кіберполіція? *Трибуна*. URL: https://tribuna.pl.ua/news/shho-take-kiberpolitsiya (дата звернення: 10.11.2019).

2. Про Департамент кіберполіції Національної поліції України : наказ МВС України від 10.11.2015 № 85 // Департамент кіберполіції офіц. сайт. URL: https://cyberpolice.gov.ua/police-commission (дата звернення: 10.11.2019).

3. Береза В. В. Принципи діяльності Департаменту кіберполіції Національної поліції. *Форум права*. 2017. № 5. С. 44–48. DOI: http://doi.org/10.5281/zenodo.1189070.

4. Кіберполіція попереджає про сплеск шахрайства в інтернет-магазинах. *Укрінформ.* 18.01.2017. URL: https://www.ukrinform.ua/rubric-society/2158555-kiberpolicia-poperedzae-pro-splesk-sahrajstva-v-internetmagazinah.html (дата звернення: 07.11.2019).

Одержано 19.11.2019