час здійснення оперативно-розшукових заходів чи негласних слідчих (розшукових) дій. У суді може бути оскаржено правові підстави використання оперативно-технічних засобів чи спеціальної техніки, які знаходились та застосовувались за допомогою БпЛА [3].

До того ж, відсутність відповідної освіти та допуску в особи, яка забезпечує польоти безпілотника, а також нездійснення сертифікації БпЛА може призвести до прийняття на озброєння відповідних підрозділів Національної поліції України безпілотників, які не відповідають вимогам безпеки. Експлуатація таких БпЛА може створити небезпеку для життя людей, спричинити настання інших тяжких наслідків, або ж може чинити загрозу безпеці повітряних польотів, що утворює склад злочину, передбаченого ст. 281 «Порушення правил повітряних польотів» або ст. 282 «Порушення правил використання повітряного простору» КК України [3].

Отже для забезпечення належної ефективності протидії злочинності правоохоронними органами (а, зокрема, їх оперативними підрозділами) нагальною потребою є правове урегулювання використання досягнень сучасної науки й техніки в розкритті злочинів. При цьому врегульовувати такі передові засоби діяльності правоохоронних органів потрібно на законодавчому рівні, аби було дотримано принципу встановленого ч. 2 ст. 19 Конституції України.

Список використаних джерел

1. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : методичні матеріали для працівників підрозділів поліції / [уклад. В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов та ін.]. ХНУВС. Харків, 2020. 44 с.

2. Апетик А. Безпека чи відповідальність? Коментуємо проект «Білої книги для штучного інтелекту». Експертний центр з прав людини. URL: https://ecpl.com.ua/news/bila-knyha-dlia-shtuchnoho-intelektu/.

3. Кузьменко Є.В. проблеми правового регулювання застосування безпілотних літальних апаратів у правоохоронній діяльності Національної поліції України. Науковий вісник Національної академії внутрішніх справ. 2016. № 4 (1). С. 82–88.

Аброськін В'ячеслав Васильович,
ректор Одеського державного університету
внутрішніх справ, кандидат юридичних наук

«OPEN SOURCE INTELLIGENCE» ЯК СКЛАДОВА КІБЕРРОЗВІДКИ В ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ

Як стверджують науковці, будь-який розвиток і прогрес, який приносив людству цивілізаційні блага й нові можливості, завжди супроводжувався і негативними явищами. На сьогодні стрімкий розвиток інформаційних технологій невблаганно супроводжується

динамічним поширенням злочинів у цій сфері. З абсолютною впевненістю можна сказати, що саме кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, адже з кожним роком вони стають дедалі поширеними й небезпечнішими.

Дійсно, сучасне суспільство являє собою суспільство інформаційних технологій, яке використовує кожен день у повсякденному житті комп'ютерну техніку, мережі зв'язку, мобільні засоби комунікації та інші технічні засоби [2, с. 84]. Збільшення користувачів світовою мережею зумовило значне зростання кількості злочинів, які вчиняються в кіберпросторі, тому збільшуються ризики зловживання інформаційними та комунікаційними технологіями в злочинних або інших цілях [4].

Слід зазначити, що кіберпростір характеризується трьома основними ознаками: інформаційний простір; комунікативне середовище; утворюється за допомогою технічних систем [2, с. 85]. Сьогодні вже скоєння злочину не потребує попереднього особистого контакту з потенційною жертвою. Кіберпростір став місцем та безпосередньо інструментом злочину. Саме тому, враховуючи особливості сучасної злочинності, важливе значення для результативності їх оперативного документування має взаємодія оперативних підрозділів Національної поліції на всіх рівнях, у тому числі із представниками правоохоронних органів інших країн [3; 6, с. 102].

Останнім часом набуває популярності провадження правоохоронними органами зарубіжних країн кіберрозвідки, яка є більш вдосконаленою методикою попередження та прогнозування злочинності. Завдяки саме такій діяльності накопичується розвідувальна інформація, необхідна для протидії кримінальним правопорушенням, та вживаються заходи превентивного характеру [5, с. 258].

Для України важливим та ефективним кроком на шляху запровадження використання кіберрозвідки у протидії кримінальним правопорушенням була ратифікація Конвенції про кіберзлочинність, яка спочатку розроблялася для держав Європейського союзу, проте з ростом суспільної небезпеки кіберзлочинності була визнана й іншими країнами, які до неї приєдналися: її підписали 46 країн, включаючи 4 країни, які не є членами Ради Європи, і 23 з них вже ратифікували її. Реформи по боротьбі зі злочинністю в Інтернет мережі, які базуються на керівних принципах Конвенції, здійснюються також в Аргентині, Бразилії, Єгипті, Індії, Нігерії, Пакистані й Філіппінах [2, с. 85].

На сьогодні, у правоохоронних органах зарубіжних держав існують спеціальні підрозділи, що здійснюють кіберрозвідку на основі відкритих джерел інформації (Open Source Intelligence – OSINT). Наприклад, таку діяльність здійснюють: Scotland Yard OSINT, Royal Canadian Mounted Police OSINT, OSINT unit of New York Police Department, OSINT unit of the Los Angeles County Sheriff's Department, британська BBC Monitoring, ізраїльський Хатсав, австралійське Управління національних оцінок) [1, с. 11; 7].

Слід зазначити, що для з'ясування дефініції «кіберрозвідка» необхідно більш детально проаналізувати поняття «кримінальна розвідка», «розвідувальна інформація» та «розвідка з відкритих джерел».

Як слушно вказують науковці, кримінальна розвідка – це форма внутрішньої розвідки, вид діяльності державних органів, спеціально створених для боротьби зі злочинністю, яка здійснюється шляхом використання системи розвідувальних, пошукових, інформаційно-аналітичних заходів, у т.ч. із застосуванням оперативних та оперативно-технічних засобів, спрямованих на своєчасне запобігання, виявлення і нейтралізацію реальних та потенційних загроз національним інтересам України від організованої злочинності, поширення корупції в органах державної влади, зрощення бізнесу і політики [1, с. 11]. Метою кримінальної розвідки є своєчасне запобігання, виявлення й нейтралізація реальних та потенційних загроз національним інтересам України від організованої злочинності, поширення корупції в органах державної влади, зрощення бізнесу та політики [3].

Взагалі, у наукових колах існує наступне визначення розвідувальної інформації (розвідувальні відомості) – це оброблена, проаналізована та/або поширена інформація, яка використовується з метою прогнозування, попередження або спостереження за кримінальною активністю [6, с. 107]. Отже, за своєю сутністю розвідувальна інформація є дуже подібної до терміну «оперативно-розшукова інформація».

У свою чергу, відповідно до Інструкції з організації роботи з відкритих джерел інформації в розвідувальних цілях (США), остання являє собою одну з видів воєнної розвідки, яка призначена для пошуку, збору та аналізу інформації з загальнодоступних джерел [7]. Закон США «National Defense Authorization Act for Fiscal Year 2006» визначає кіберрозвідку з відкритих джерел як розвідку, що здійснюється шляхом збору, обробки та передачі цільовому адресату інформації з загальнодоступних відкритих джерел з метою вирішення конкретних завдань розвідки [8].

Науковці наголошують, що кіберрозвідка відкритих джерел – це завжди специфічна інформація, зібрана й структурована особливим чином для відповіді на конкретні запитання [5, с. 258]. У спрощеному варіанті, даний термін стосується інформації, що не має грифу «таємно». Розвідувальне співтовариство США (Intelligence Community) визначає таку інформацію як загальнодоступний матеріал, що може отримати кожен законним шляхом через запит, купівлю чи спостереження [8].

За нашим переконанням, використовуючи кіберрозвідку у протидії кримінальним правопорушенням, предметом пошуку виступають дані про особу, які містяться у відомчих базах даних, відкритих державних реєстрах, соціальних мережах та інших ресурсах мережі Інтернет з відкритим доступом. При цьому, завдання інформаційного пошуку стосується пошуку інформації в документах,

пошуку самих документів, вилучення метаданих з документів, пошуку тексту, фото-, відеоматеріалів, аналізу інформації з гіпертекстових баз даних. При цьому, джерелами отримання інформації кіберрозвідки можуть бути: ЗМІ: друковані газети, журнали, радіо та телебачення з різних країн; Інтернет: онлайн-публікації, блоги, дискусійні групи, медіа громадян (наприклад, відео з мобільних телефонів, вміст, створений користувачами), YouTube та інші відео-хостинги, вікі-довідники та інші веб-сайти соціальних медіа (наприклад, Facebook, Twitter, Instagram та ін.). Ці джерела також випереджають безліч інших джерел через своєчасність і легкість доступу; Державні дані, публічні урядові звіти, бюджети, слухання, телефонні довідники, прес-конференції, веб-сайти та виступи; Професійні та академічні публікації, інформація, отримана з журналів, конференцій, симпозіумів, наукових праць, дисертацій та тез; комерційні дані, комерційні зображення, фінансові та промислові оцінки, бази даних тощо.

Таким чином, стрімке зростання ролі та цінності інформації, розвиток інформаційних технологій, програмних та апаратних засобів, доступність мережі Інтернет, збільшення інформаційного потоку відкритої інформації з одного боку та запровадження методик «Open source intelligence», як складової кіберрозвідки серед правоохоронних органів з іншого боку ставить збір та аналіз інформації з відкритих джерел одним із дієвих сучасних засобів протидії кримінальним правопорушенням.

Список використаних джерел

1. Албул С.В. До питання концептуалізації напрямів вдосконалення інформаційно-аналітичного забезпечення негласної роботи суб'єктів оперативно-розшукової діяльності в Україні. Правові та організаційно-тактичні засади оперативно-розшукової діяльності Національної поліції України: Матеріали Всеукраїнської науково-практичної інтернет-конференції (м. Одеса, 30 жовтня 2020 р.). Одеса: ОДУВС, 2020. С. 9–12.

2. Ісмайлов К.Ю. Кримінальна розвідка з відкритих джерел як інструмент збирання оперативної інформації. Кримінальна розвідка: методологія, законодавство, зарубіжний досвід: матеріали Міжнародної науково-практичної конференції (29 квітня 2016 р., м. Одеса). Одеса: ОДУВС, 2016. С. 84–86.

3. Кримінальна розвідка: методологія, законодавство, зарубіжний досвід: матеріали Міжнародної науково-практичної конференції (29 квітня 2016 р., м. Одеса). Одеса: ОДУВС, 2016. 184 с.

4. Основи кримінального аналізу: посібник з елементами тренінгу / Користін О.Є., Албул С.В., Заєць О.М., Ісмайлов К.Ю., Тетерятник Г.К., Горбаньов І.М. Одеса: ОДУВС, 2016. 112 с.

5. Ржевська Н.Ф. Розвідка відкритих джерел (open source intelligence) / Н.Ф. Ржевська, О.О. Кожушко. Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців: всеукраїнська наукова

конференція, Львів, 27 травня 2011 р. / Міністерство освіти і науки, молоді та спорту України, Національний університет «Львівська політехніка». Львів: Видавництво Національного університету «Львівська політехніка», 2011. С. 257–261.

6. Albul S. Intelligence-Led Policing – theoretical Problems. Scientific Achievements of modern Society. Abstracts of the 4th International scientific and practical conference (4-6 December 2019). Cognum Publishing House. Liverpool, United Kingdom. 2019. Pp. 101–110.

7. Criminal intelligence [Електронний ресурс]. URL: http://en.wikipedia.org/wiki/Criminal_intelligence.

8. Open source intelligence. Fmi 2-22.9. December 2006 [електронний ресурс]. Federation of american scientists. Url: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf.

Кузнєцов Михайло Валентинович,
начальник Департаменту оперативно-технічних заходів Національної поліції України;
Василинчук Віктор Іванович,
професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, доктор юридичних наук, професор

ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ МЕТОДІВ КРИМІНАЛЬНОГО АНАЛІЗУ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ПІД ЧАС ТИМЧАСОВОГО ДОСТУПУ ДО ІНФОРМАЦІЇ ПРО ЗВ'ЯЗОК

У межах наданих повноважень підрозділи кримінальної поліції здобувають достатній масив інформації про злочинну діяльність, у тому числі про представників організованої злочинності. У зв'язку із зазначеним, надважливим завданням є застосування інструментів, які б надали можливість опрацьовувати велику кількість наявних даних.

Одним із таких інструментів в діяльності оперативних підрозділів Національної поліції України є кримінальний аналіз, який є специфічним видом інформаційно-аналітичної діяльності і полягає в ідентифікації та якомога більш точному визначенні внутрішніх зв'язків між інформацією (відомостями, даними), що стосуються злочину, і будь-якими іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, їх аналітичної підтримки.

У країнах Європейського Союзу та США використання можливостей кримінального аналізу є обов'язковим для всіх правоохоронних органів. Його зміст, правила та процедури чітко визначено та врегульовано у правовому відношенні [1, с. 30–32].