Список використаних джерел:

1. Письмо Постоянного представителя Соединенного Королевства Великобритании и Северной Ирландии при Организации Объединенных Наций от 7 марта 2017 года на имя Генерального секретаря: «Концептуальная записка для открытых прений Совета Безопасности на уровне министров по теме «Торговля людьми в условиях конфликта: принудительный труд, рабство и другая аналогичная практика», которые состояться 14 марта 2017 года» // Совет безопасности Организации объединенных наций URL: http://undocs.org/ru/S/2017/198 (дата звернення: 24.10.2017).
2. В МИД рассказали о многочисленных случаях торговли людьми и рабства на оккупированных территориях Донбасса // Інформаційне агентство «УНІАН». URL: https://www.unian.net/society/1825467-v-mid-rasskazali-o-mnogochislennyih-sluchayah-torgovli-lyudmi-i-rabstva-na-okkupirovannyih-territoriyah-donbassa.html (дата звернення: 24.10.2017).
3. Наконечна І. М. Поняття кваліфікуючих (особливо кваліфікуючих) ознак складу злочину. *Часопис Київського університету права*. 2013. № 4. С. 313-317.

Одержано 25.10.2017

УДК 351.74 (477)

Ольга Ігорівна БЕЗПАЛОВА,
доктор юридичних наук, професор, завідувач кафедри адміністративної діяльності поліції факультету № 3 Харківського національного університету внутрішніх справ

ВЗАЄМОДІЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ З ІНШИМИ ПРАВООХОРОННИМИ ОРГАНАМИ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ ЯК ОДИН ІЗ НАПРЯМКІВ ЗАБЕЗПЕЧЕННЯ СКЛАДОВИХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Реальні прояви кібератак мало прогнозовані, а їх результатом є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим, існуючі загрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. Варто наголосити на тому, що питання забезпечення кібербезпеки є надзвичайно актуальними для України. В той же час, у нашій державі заходи з протидії викликам і загрозам у зазначеній

сфері знаходяться на початковому етапі та ще не мають комплексного характеру.

У рішенні Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» звертається увага, що серед основних напрямків досягнення необхідних оперативних та інших спроможностей складових сектору безпеки і оборони виокремлюється удосконалення державного управління та керівництва сектором безпеки і оборони, у тому числі систем забезпечення інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів, посилення боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері. У зв'язку із зазначеним необхідно розглянути питання взаємодії Національної поліції, як одного із суб'єктів сектору безпеки і оборони, з іншими правоохоронними органами у сфері боротьби з кіберзлочинністю.

У результаті аналізу нормативно-правових актів, які регламентують діяльність Національної поліції та враховуючи особливості правопорушень у сфері інформаційно-комунікаційних технологій, що передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидію забороненим видам господарської діяльності у цій сфері; надання телекомунікаційних послуг, а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище діянь, то важливе значення має взаємодія на наступних рівнях: 1) внутрішньовідомчому; 2) внутрішньодержавному (з органами і підрозділами Служби безпеки України, органами місцевого самоврядування, підприємствами, установами і організаціями різних форм власності у сфері боротьби з кіберзлочинністю); 3) міжнародному (з правоохоронними органами інших країн).

Враховуючи виокремленні вище рівні взаємодії Національної поліції з іншими правоохоронним органами, варто вказати на їх форми реалізації на внутрішньовідомчому та внутрішньодержавному рівні. До зазначених форм варто віднести такі: 1) організація вивчення матеріалів, що утворюються під час здійснення поліцейськими оперативно-розшукової діяль-

ності, у їх числі справ оперативного обліку, матеріалів виконання письмових доручень слідчого, ухвал суду; 2) створення та застосування автоматизованих інформаційних систем (формування й поповнення інформаційних масивів даних) відповідно до потреб оперативно-службової діяльності; 3) організація виконання доручень слідчого щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях, які відносяться до компетенції поліції; 4) організація проведення комплексних і цільових оперативно-профілактичних заходів, у тому числі за участю правоохоронних органів інших країн; 5) внесення в установленому порядку пропозицій щодо вдосконалення законодавчої бази у сфері боротьби з кіберзлочинністю, а також участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері; 6) забезпечення своєчасного розгляду звернень та запитів громадян, підприємств, установ, організацій з питань, віднесених до компетенції поліції, контролю за належним дотриманням порядку їх прийняття, реєстрації, обліку і розгляду; 7) участь в організації та проведенні навчальних та науково-практичних заходів з питань, що відносяться до сфери боротьби з кіберзлочинністю (тренінгів, конференцій, семінарів) тощо.

Говорячи про міжнародний рівень взаємодії, варто зазначити, що ефективна боротьба проти кіберзлочинності вимагає тісного, швидкого та ефективного, функціонального міжнародного співробітництва всіх державних структур, а що найперше – правоохоронних органів, у розслідуванні такого роду правопорушень. Перші серйозні кроки в налагодженні міжнародного співробітництва у протидії кіберзлочинності Україна зробила на початку XXI століття, коли 23 листопада 2001 р. в Будапешті Україна разом із 30-ма іншими державами підписала Європейську конвенцію «Про кіберзлочинність». Наступним важливим кроком України щодо налагодження міждержавної співпраці розглядуваній сфері є ратифікація 7 вересня 2005 р. зазначеної Конвенції, що передбачає надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях, укладення домовленостей щодо дієвого міжнародного співробітництва. Національна поліція уповноважена здійснювати співробітництво з правоохоронними органами іноземних держав в рамках функціонування цілодобової контактної мережі для надання

невідкладної допомоги при провадженні щодо кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, які підозрюються або обвинувачуються у їх вчиненні, а також збирання доказів в електронній формі.

Взаємодію Національної поліції з іншими правоохоронними органами щодо протидії правопорушенням у сфері кіберзлочинності умовно слід поділити на внутрішню (в рамках органів та підрозділів поліції) та зовнішню. В залежності від напрямків діяльності Національної поліції слід виокремити такі види взаємодії: 1) взаємодія щодо протидії правопорушенням у сфері телекомунікацій; 2) взаємодія щодо протидії правопорушенням у сфері електронної комерції; 3) взаємодія щодо протидії правопорушенням у сфері шахрайства та легалізації (відмиванню) доходів, одержаних злочинним шляхом тощо.

Одержано 25.10.2017

УДК 343.1 : 65.012.8 + 004

Олег Валерійович БОГІНСЬКИЙ,
аспірант Харківського національного університету внутрішніх справ

МЕТОДИ МЕРЕЖНОГО АНАЛІЗУ ТА КАРТОГРАФУВАННЯ В СИСТЕМІ КРИМІНАЛЬНОЇ РОЗВІДКИ

Для стримування злочинності можуть застосовуватися різні моделі. Найбільшої популярності сьогодні набули такі з них: нульової толерантності; проблемно-орієнтована; небезпечних зон; на основі розвідувальних даних; прогностична. Кримінальна розвідка є елементом описаних проактивних стратегій стримування злочинності.

Центральним елементом кримінальної розвідки як процесу є аналіз, без проведення якого сама ця діяльність втрачає сенс, а накопичення даних буде у більшості випадків марним витрачанням часу. Під час аналізу можуть бути застосовані різні методи та використовуватися конкретні моделі роботи з даними.

Практика показує, що переважна кількість аналітичних висновків містить елементи мережного аналізу. Цей метод є особливо актуальним в умовах дослідження великих злочинних груп та організацій, адже зі збільшенням мережі, яка підлягає аналізу, зростає ймовірність виявити у ній слабкі місця