УДК 351.95

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

Дар'я Олександрівна СЕЧАНЦИНА,
курсантка 4 курсу факультету № 1
Харківського національного університету внутрішніх справ

ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У СФЕРІ ПОДОЛАННЯ ІНФОРМАЦІЙНИХ ВИКЛИКІВ І КІБЕРЗАГРОЗ У СУСПІЛЬСТВІ

Згідно Закону України «Про національну безпеку України» від 21.06.2018 року № 2469-VIII одним із важливих напрямків державної політики у сфері національної безпеки і оборони є забезпечення кібербезпеки України [1]. Проблема подолання інформаційним загрозам та кіберзлочинності турбує не лише Україну, а й увесь світ. Одним з аспектів тероризму є крадіжка і злом баз даних як закордонних, так і вітчизняних державних органів влади. Під загрозою злому можуть перебувати державні реєстри з персональними даними громадян. Сучасні хакери, використовуючи всі самі передові розробки в області ІТ-технологій, щодня зламують тисячі акаунтів. Зламати можна все: поштову скриньку, акаунт у соціальній мережі, медичну базу, номер банківської карти та кредитної історії тощо. Цікаво, що Україна вже давно асоціюється у світі з місцем, де процвітає кіберзлочинність. Яскравий приклад тому – викрита у серпні 2015 року у Сполучених Штатах Америки злочинна група, в якій були і українські хакери, що зламувала бази даних спеціалізованих біржових видань. Зловмисники завдали шкоди у десятки мільйонів доларів, торгуючи незаконно отриманою інсайдерською інформацією великих міжнародних компаній [2].

Стратегія кібербезпеки України передбачає, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення режимів роботи автоматизованих систем керування технологічними процесами на об'єктах

критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні вебсайти в мережі Інтернет. Після атаки вірусу «Petya» наприкінці 2017-го, від якої постраждали енергетичні компанії, банки, урядові установи, Україна посідає 3 місце світовому рейтингу з ризику зіткнення з вебзагрозами. За оцінками фахівців у сфері загроз інформаційній безпеці характерні такі тенденції: неконтрольовані ризики, пов'язані з «Інтернетом речей» та поширенням мережевих з'єднань; стрімке зростання «кіберзлочинів як сервісу»; зростання правових ризиків у сфері регулювання мережевих комунікацій; хакерські атаки, спрямовані на підрив репутації політичних сил [3, с. 57-58].

Головна роль в подоланні різних видів злочинів, скоєних за допомогою застосування новітніх технологій, належить Національній поліції України.

Створена у рамках реформи системи МВС України кіберполіція здійснює оперативно-розшукову діяльність, а отже, забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, займається захистом персональних даних громадян у віртуальному просторі, в тому числі, боротьбою з піратством, а також поліцейською допомогою онлайн [4]. При цьому на виконання положень Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV [5] та з метою забезпечення міжнародної діяльності кіберполіції у структурі Департаменту кіберполіції діє сектор Національного контактного пункту з реагування на кіберзлочини. Відповідно до Положення про Департамент кіберполіції Національної поліції України, затвердженого наказом Національної поліції України від 10.11.2015 № 85, діяльність підрозділів кіберполіції спрямована на: 1) протидію кіберзлочинності, тобто протиправним діянням, що вчинені з використанням інформаційних технологій або пов'язані з втручанням в роботу комп'ютерів, програмного забезпечення, мереж, несанкціонованою модифікацією даних, а також інші протиправні діяння, вчинені за допомогою пристроїв доступу до інформаційного простору; 2) забезпечення кібербезпеки – стану захищеності прав та інтересів людини, суспільства, держави у кіберпросторі від протиправних посягань; 3) протидія правопорушенням у інформаційній сфері, яка стосується вирішення проблем реалізації інформаційної політики держави, її стратегічних напрямів [6]. Ця діяльність вимагає належної системи правових заходів, спря-

мованих на нейтралізацію, запобігання та припинення кіберзагроз і інформаційних викліків.

Крім того, відповідно до Рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» підтримання належного стану інформаційної безпеки визнано важливою функцією органів поліції щодо захисту прав та свобод людини і громадянина, закріплених Конституцією України [7]. Тому співробітники української кіберполіції борються з кіберзлочинністю і кіберзагрозами, а також здійснюють міжнародне співробітництво щодо знешкодження транснаціональних злочинних угруповань у цій сфері у відповідність з кращими світовими стандартами [4].

Зважаючи на викладене, можна дійти висновку, що удосконалення правових засад діяльності підрозділів Національної поліції в сфері протидії кіберзагрозам і інформаційним викликам, у першу чергу, спрямоване на:

- оптимізацію організаційно-функціональної структури кожного підрозділу поліції, у ході якої особлива увага повинна приділятися аналізу оперативної обстановки, визначенню базових вимог до їх діяльності, на основі чого вже повинні формулюватися конкретні функції;
- обґрунтований розподіл функцій і обов'язків між підрозділами і працівниками поліції, створення належних умов для налагодження якісно нового рівня взаємодії між ними та координації їх діяльності;
- запровадження нових підходів до формування переліку організаційно-правових форм та методів взаємодії усіх суб'єктів протидії правопорушенням в інформаційній сфері, та підвищення контролю за якістю їх реалізації;
- запровадження сучасних механізмів аналітичного і матеріально-технічного забезпечення правоохоронної діяльності, покращення системи заходів, спрямованих на підвищення рівня професіоналізму поліцейських.

Зважаючи на стрімкий розвиток інформаційно-комунікаційних технологій, тенденцію до активізації зусиль щодо розвитку глобального інформаційного суспільства надзвичайно актуальним є вироблення ефективного правового механізму подолання кіберзагрозам за допомогою адміністративних засобів.

Список бібліографічних посилань

1. Про національну безпеку України : Закон України від 21.06.2018 № 2496-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 22.04.2020).
2. США підозрюють українських хакерів у викраденні конфіденційної корпоративної інформації // ZN,UA : сайт. 12.08.2015. URL: https://dt.ua/WORLD/ssha-pidozryuyut-ukrayinskih-hakeriv-u-vikradenni-konfidenciynoyi-korporativnoyi-informaciyi-181425_.html (дата звернення: 17.04.2020).
3. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : АртЕк, 2018. 422 с.
4. Українська кіберполіція: протистояти найнебезпечнішим хакерам світу // Українська правда : сайт. 20.10.2019. URL: http://www.pravda.com.ua/inozmi/deutsche-welle/2019/10/20/7085458 (дата звернення: 11.04.2020).
5. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5–6. Ст. 71.
6. Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Нац. поліції України від 10.11.2015 № 85 // Національна поліція України : офіц. сайт. URL: https://www.npu.gov.ua/uk/publish/article/1816252 (дата звернення: 11.04.2020).
7. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Рішення Ради нац. безпеки і оборони України від 01.05.2014 № 449/2014. *Урядовий кур'єр*. 2014. № 81.

Одержано 05.05.2020