УДК 351:349.6

І. Д. КАЗАНЧУК,
кандидат юридичних наук, доцент,
професор кафедри адміністративної діяльності поліції факультету підготовки фахівців для підрозділів міліції громадської безпеки та кримінальної міліції у справах дітей
Харківського національного університету внутрішніх справ
ORCID: http://orcid.org/0000-0003-4269-2749

ЩОДО УДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Автором розглянуто сучасний стан та правові засади діяльності Національної поліції в сфері забезпечення інформаційної безпеки в Україні. Проаналізовано передовий закордонний досвід діяльності правоохоронних органів в сфері протидії кіберзлочинності та надані шляхи удосконалення діяльності кіберполіції України в сучасних умовах.

Ключові слова: *Україна, Національна поліція, інформаційна безпека, протидія кіберзлочинності, IT-технології, міжнародний досвід.*

У всьому світі, і Україна – не виключення, стрімкий розвиток інформатизації суспільства призвів до появи такого негативного явища як кіберзлочинність. Під загрозою перебувають державні і регіональні реєстри з персональними даними громадян. Повна приватність фактично залишилася в минулому. Сучасні хакери, використовуючи передові розробки в області IT-технологій, щодня зламують тисячі акаунтів, баз даних як закордонних, так і вітчизняних державних структур [1, с. 48]. За великим рахунком, будь-яка секретна інформація щодо особистого життя людини чи державного органу може опинитися у вільному доступі, що загрожує інформаційній безпеці країни.

Питання забезпечення інформаційної безпеки – як основи національної безпеки, захисту інформаційного простору держави знаходяться у центрі уваги правоохоронних структур багатьох країн, а також органів й інституцій Організації Об'єднаних Націй: Генеральної Асамблеї (A/RES 63/195), Комісії з попередження злочинності і кримінального правосуддя (док. E/ CN.15/2009/15) [2, с. 195].

Задля забезпечення інформаційної безпеки, боротьби з кіберзлочинністю в таких країнах світу як Австралія, Великобританія, Данія, Естонія, Канада, Малайзія, Нідерланди, Німеччина, Норвегія, Польща, США, Швейцарія, Швеція і інших створені спеціальні підрозділи поліції. Серед основних функцій цих спецпідрозділів є: здійснення оперативно-розшукових, розвідувальних заходів з метою фіксування протиправних дій

кіберзлочинців, моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення; розслідування кіберзлочинів, надання методичної і практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції; профілактика кіберзлочинів за допомогою ЗМІ і населення; навчання працівників поліції [3, с. 110]. Деякі з підрозділів поліції щодо протидії злочинам з використанням інформаційних технологій виконують додаткові функції: профілактика і нагляд за телекомунікаційними послугами; експертне дослідження доказів на електронних носіях; створення відповідної бази даних щодо злочинів у сфері кіберпростору та постійного її оновлення; надання послуг банкам щодо захисту персональної інформації клієнтів тощо.

Україна не стоїть в осторонь від протидії кіберзлочинності [4]. Протягом останніх років терористичні та кримінальні структури вдосконалили способи використання інформаційних технологій і засобів, щоб отримати можливість здійснення деструктивних інформаційних впливів на інформаційні ресурси, інформаційно-телекомунікаційних систем, Інтернет мереж державних і недержавних організацій. Таке застосування інформаційних технологій надало їм властивості так званої інформаційної зброї. Як результат, з'явилися нові правопорушення, які були раніше не відомі нашій правоохоронній системі, і які безпосередньо пов'язані з інформаційною безпекою людини, регіонів, держави.

Міністр внутрішніх справ України Арсен Аваков у своїй доповіді вказав на цілий ряд правопорушень, з якими боротися новостворена кіберполіція [5]. Це: скімінг (незаконне копіювання чіпів банківських карток); кеш-трепінг (викрадення готівки з банкомату, коли на нього встановлюють спеціальну накладку); онлайн-шахрайство; кардінг (використання грошей з банківської картки); фішинг (виманювання у користувачів інтернету їхніх логінів та паролів до електронних гаманців, сервісів, онлайн-аукціонів), тощо.

Слід зазначити, що Україна у світовому значенні асоціюється з місцем, де процвітає кіберзлочинність. У 2012 році Україна була визнана міжнародними експертами як країна що є «раєм для хакерів» і яскравий приклад тому – заарештовані у 2010 році українські «чорні» хакери, яких звинуватили у крадіжці 72 мільйонів доларів з банківських рахунків у США за допомогою вірусу «Conficker» [6]. Найсвіжіша з резонансних справ – це викрита у США у 2015 року злочинна група, до якої входили й «кіберфахівці» з України, яка зламувала бази даних спеціалізованих біржових видань. Внаслідок торгів незаконною інсайдерською інформацією великих міжнародних компаній було завдано збитків країні у десятки мільйонів доларів [7].

Саме тому діяльність кіберполіції, як міжрегіонального територіального органу Національної поліції України, спрямована на реалізацію державної політики у сфері протидії кіберзлочинності, інформаційно-аналітичне забезпечення поліції України та органів державної влади відповідно до законодавства України [8]. Структурні підрозділи кіберполіції мають поділ на Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське і Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному і східному регіонах. Крім того у структурі кіберполіції створено сектор Національного контактного пункту з реагування на кіберзлочини у регіонах, який за своїми технічними і професійними можливостями має змогу миттєво реагувати на кіберзагрози, а також, у відповідності до кращих європейських стандартів забезпечити захист персональних даних

громадян у віртуальному просторі, проводити міжнародну співпрацю по знешкодженню транснаціональних злочинних утруповань у інформаційній сфері. Зазначимо, що у створенні кіберполіції використано найкращий світовий досвід, а також пропозиції міжнародних організацій з метою забезпечення міжнародної кібердіяльності та вимог Закону України «Про ратифікацію Конвенції про кіберзлочинність» [9].

Крім того, між Україною і Європейським Союзом підписана Угода про процедури безпеки, що стосуються обміну інформацією з обмеженим доступом. Ця Угода закріпила основні положення обміну, зберігання, охорони та доступу до такої інформації [10]. Однак неврегульованими залишаються питання, що пов'язані з використанням інформаційних ресурсів, застосуванням усіх засобів системи забезпечення інформаційної безпеки при впровадженні заходів активного характеру, визначенням інформаційних загроз як на державному, так і регіональному рівнях, виробленням механізму протидії ним. Все це потребує прийняття відповідного законодавчого нормативно-правового акту України.

Також в контексті оптимізації правового регулювання діяльності кіберполіції у сфері інформаційної безпеки в Україні слід звернути увагу на позитивний досвід діяльності правоохоронних органів інших країн, зокрема, Канади. Так, одним із важливих напрямів діяльності поліції Канади є боротьба з комп'ютерними і телекомунікаційними порушеннями, розслідуванням яких займається підрозділ Королівської канадської кінної поліції (федеральної поліції) з боротьби з комп'ютерною злочинністю, який діє, спираючись на дані канадського поліцейського інформаційного центру та співпрацюючи з іншими країнами. У свою чергу, сектор захисту інформаційних технологій забезпечує зміст федеральних державних комп'ютерних центрів, приватного сектора, дає консультації, готує персонал для роботи щодо здійснення комп'ютерного захисту. Враховуючи те, що інформаційна система дозволяє передавати повідомлення від одного пункту до іншого майже миттєво, у Канади діє близько 2500 точок доступу, до яких входить близько 1205 федеральних і провінційних поліцейських відділень. Цей напрямок діяльності поліції є важливим, оскільки економічні втрати вже досягли міжнародних масштабів. Слід визнати, що канадське законодавство щодо інформаційної безпеки не є досконалим з урахуванням того, що завдання, які стоять перед підрозділами поліції з боротьби з комп'ютерною злочинністю, носять міжнародний характер і не є специфічними для Канади. Тому вони активно розвивають міжнародну співпрацю з іншими країнами та Інтерполом [11, с. 101-107].

Крім того у різних регіонах світу було застосовано низку нових підходів і методів протидії тероризму, вірусам, порнографії, екстремізму, що поширюються в мережі Інтернет [3]. Європейським Союзом докладено багато сил з узгодження законодавства щодо забезпечення безпеки інформаційного простору, яке діє на території держав-членів ЄС. Зокрема прийняті:

- директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, таких, як електронна торгівля на внутрішньому ринку;
- рамкове рішення Ради Європейського Союзу 204/68/ЛНА про боротьбу із сексуальною експлуатацією;
- рамкове рішення Ради Європейського Союзу 2000/41/ЛНА про боротьбу з шахрайством і фальсифікацією безготівкових платіжних засобів [10].

У 2002 році Співдружністю націй був розроблений типовий закон про комп'ютери та

пов'язані з комп'ютерами злочинами, метою якого є удосконалення законодавчих норм у інформаційній сфері, поглиблення міжнародної співпраці. Оскільки цей закон має регіональний характер, то його положення стосуються лише держав членів Співдружності.

Безперечним є факт, що найбільш вразливою для інформаційних впливів є суспільна свідомість, а основними суб'єктами впливу на суспільну свідомість та формування громадської думки виступають засоби масової інформації: мережа Інтернет, медіа та радіомовлення, реклама. Виходячи з цього, на підставі світової практики забезпечення та захисту національних інтересів в інформаційному просторі слід систему інформаційної безпеки в Україні поділити на дві основні підсистеми: 1) інформаційно-технічну (комп'ютерні пристрої, інформаційні мережі, програми); 2) інформаційно-психологічну (засоби масової інформації, громадські організації) [4, с. 107-108].

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. *Максименко Ю. С. Боротьба з тероризмом в умовах інформатизації: Правові проблеми сучасності. К.: Вид. Ліпкан О.С., 2013. С.48-50.*
2. *Сироїд Т. Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. С. 194-196.*
3. *Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. Право і Безпека. 2015. № 2 (57). С. 107-113.*
4. *Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. [О. С. Користін, В. М. Бутузов, В. В. Василевич та ін.]. Київ : Скіф, 2012. 728 с.*
5. *Аваков А. Кіберполіція (крок реформи) – наш захист у віртуальному просторі // Українська правда. 11.10.2015. URL: http://blogs.pravda.com.ua/authors/avakov/561a92c183c27 (дата звернення: 10.01.2016).*
6. *США підозрюють українських хакерів у викраденні конфіденційної корпоративної інформації // «ZN'UA». 12.08.2015. URL: http://dt.ua/WORLD/ssha-pidozryuyut-ukrayinskih-hakeriv-u-vikradenni-konfidencynoyi-korporativnoyi-informaciyi-181425 (дата звернення: 20.08.2016).*
7. *Українська кіберполіція: протистояти найнебезпечнішим хакерам світу // Українська правда. 20.10.2015. URL: http://www.pravda.com.ua/inozmi/deutsche-welle/2015/10/20/7085458 (дата звернення: 10.05.2016)*
8. *Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10.11.2015 № 85. / База даних «Законодавство України». URL: https://www.npu.gov.ua/uk/publish/article/1816252 (дата звернення: 26.11.2016)*
9. *Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV / Відомості Верховної Ради України. 2006. № 5-6. ст. 71.*
10. *Украина – Европейский Союз: Собрание международных договоров и других документов (1991-2010). К. : ЮСТИНИАН, 2010. 608 с.*
11. *Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні: дис. канд. юрид. наук : 12.00.07. Дніпропетровськ, 2012. 203 с.*

Надійшла до редколегії 25.01.2017