Лагуна Альона Володимирівна,
здобувач ступеня вищої освіти магістра навчально-наукового інституту заочного та дистанційного навчання Національної академії внутрішніх справ
Науковий керівник: **Корольчук Віктор Володимирович,** провідний науковий співробітник відділу організації наукової діяльності та захисту прав інтелектуальної власності Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ДІЯЛЬНОСТІ КІБЕРПОЛІЦІЇ УКРАЇНИ, США ТА ФРАНЦІЇ

Важливу роль у формуванні та безперервному функціонуванні правової, демократичної, незалежної та міцної держави відграє налагоджена система правоохоронних органів. З огляду на сучасні тенденції та розвиток інформаційних технологій відслідковується стрімке зростання кількості кримінальних правопорушень, пов'язаних з використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. На думку А. В. Вінакова, вияви кіберзлочинності у вигляді хакерських атак на комп'ютерні системи банківських та інших фінансових установ, крадіжок електронних коштів, широкого використання мережі Інтернет для наркоторгівлі, торгівлі людьми, інших протиправних дій стають реальною загрозою національній безпеці [1, с. 34].

У зв'язку з вищенаведеним постає необхідність достатньої реалізації державної політики у сфері забезпечення кібербезпеки держави задля забезпечення прав людини й громадянина на просторах віртуальної мережі Internet.

Відповідно до статті 3 Закону України «Про основні засади забезпечення кібербезпеки України» правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України [2]. Відповідно чинне нормативно-правове регулювання у даній сфері сьогодні потребує свого удосконалення.

Вагоме місце в системі органів державної влади як суб'єктів реалізації інформаційної функції держави відіграє Національна поліція України, в межах якої створений такий територіальний орган, як Департамент кіберполіції Національної поліції України. Головними завданнями Департаменту кіберполіції Національної поліції України є забезпечення реалізації державної політики у галузі протидії кіберзлочинності, інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції, формування та забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку тощо [3].

Проте для створення відповідної дієвої системи кіберзахисту, формування її та функціонування у відповідності до міжнародних нормам та стандартів слід звернути увагу та спробувати перейняти позитивний досвід інших країн. Повсякденно в політиці провідних європейських держав розроблюються новітні заходи протидії шахрайству та іншим загрозам, такі як удосконалення кримінального законодавства, здійснення заходів для співпраці з іншими органами, які допоможуть у викритті кіберзлочинів та вдосконалення методів кібербезпеки.

Сполучені Штати Америки одні з перших, хто визначив на національному рівні та прийняв низку законів та нормативно-правових актів у сфері протидії кіберзлочинності та забезпечення кібербезпеки держави. США відсутнє єдине поліцейське управління, оскільки у кожному штаті діють свої закони та функціонують органи, діяльність яких може відрізнятися від функціонування аналогічних органів інших штатів. Так, Департамент кіберполіції Нью-Йорку, що створений у 1845 році, є одним із найбільших підрозділів муніципальної поліції США. Структурно Департамент поліції штату Нью-Йорк складається із бюро та офісів. Окрему увагу слід приділити функціонуванню Бюро по боротьбі з тероризмом, оскільки його діяльність спрямована на захист штату від внутрішніх та міжнародних (зовнішніх) загроз терористичного характеру, у тому числі кіберзагроз. На території штату діє так звана «Команда критичного реагування», яка одна із перших здійснює оперативне реагування та захисту від терористичних атак та кіберзагроз. Також, у США при ФБР спільно з іншими державними органами створено ряд бюро та робочих груп з питань протидії кіберзлочинності з різними категоріями громадян та відповідно до їх соціального статусу. Одним із напрямів діяльності є врегулювання питання забезпечення кібербезпеки дітей у Інтернет-просторі та протидія кібербулінгу [4].

У правоохоронній системі Франції діє відповідний суб'єкт по боротьбі з кіберзлочинністю такі як: відділ кіберзлочинів технічного обслуговування судових досліджень та документації (STRJD), комп'ютерний і електронний відділ Інституту кримінального розслідування Національної жандармерії (IRCGN) та Національне агентство безпеки інформаційних систем (ANSII). Французької національної стратегія цифрової безпеки від 16.10.2015 активно впроваджується ANSSI. Основними пріоритетами в діяльності ANSSI: захист та безпека державних інформаційних систем та критично важливих інфраструктур, важливих операторів економіки та суспільства; цифрова довіра, конфіденційність, особисті дані, кібернасильство; підвищення обізнаності, початкове навчання, безперервна освіта; навколишнє середовище бізнесу цифрових технологій, промислова політика, експорт та інтернаціоналізація; цифрова стратегічна автономія, стійкість кіберпростору [5].

Отже, з огляду на позитивний зарубіжний досвід США та Франції щодо ефективної діяльності суб'єктів, яка пов'язана з протидією кіберзлочинності та забезпечення кібербезпеки держави виникає необхідність перегляду чинного нормативно-правового законодавства України, особливо при кваліфікації даних злочинів. Важливо урахувати наразі існуючі та потенційні кіберзагрози, створити спільний міжнародний підрозділ по розслідуванню таких злочинів, а також розширити повноваження кіберполіції у сфері співпраці з іншими органами.

Список використаних джерел

1. Вінаков А. В. Зміст підготовки фахівців для підрозділів боротьби з кіберзлочинністю в в сучасних умовах. Використання інноваційних технологій у попередженні злочинів : матеріали наук.-практ. семінару (м. Харків, 6 груд. 2012 р.) / МВС України ; Харк. нац. ун-т внутр. справ. Харків, 2012. С. 34–36.

2. Закон України Про основні засади забезпечення кібербезпеки України № 2163-VIII від 5 жовтня 2017 року [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/216319#Text.

3. Офіційний сайт кіберполіції України [Електронний ресурс]. Режим доступу: https://cyberpolice.gov.ua/contacts/.

4. Білоброва Т.В Міжнародний досвід протидії кіберзлочинності органами кіберполіції [Електронний ресурс]. ежим доступу: https://revolution.allbest.ru/law/01270465_0.html.

5. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності [Електронний ресурс]. Режим доступу: https://otherreferats.allbest.ru/ programming/01239024_0.html.