Матеріали Всеукраїнського науково-практичної конференції 23-25 листопада 2016 року, м. Кропивницький. С. 7-8. URL : https://core.ac.uk/download/84825385.pdf.

3. Олена Трофименко, Юлія Прокоп, Наталія Логінова, Олександр Задерейко. Кібербезпека України: Аналіз сучасного стану. Захист інформації, том 21, № 3, липень-вересень 2019, с. 150-158. URL : https://dspace.onua.edu.ua/server/api/core/bitstreams/3acf4b52-6858-4bda-973c-35535be8fcfe/content.

4. Ольга Бакалінська, Олександр Бакалинський. Правове забезпечення кібербезпеки в Україні. 9/2019 Адміністративне право і процес. С. 100-108. URL : http://pgp-journal.kiev.ua/archive/2019/9/18.pdf.

5. Ісланкін С.М. Відсторонення від посади: Міжнародний досвід. Регламентації. Правова позиція № 4 (37) 2022. С. 271-274. URL : https://legalposition.umsf.in.ua/archive/2022/4/51.pdf.

УДК 004.738.5:351.862.4
DOI: 10.31733/15-03-2024/2/357-358

Ярослав ІЖИК
курсант факультету підготовки
фахівців для підрозділів
кримінальної поліції

Олександр ЖУРАВЕЛЬ
старший викладач кафедри
спеціальної фізичної підготовки
Дніпропетровського державного
університету внутрішніх справ,
доктор філософії

ЩОДО ОСНОВНИХ НАПРЯМІВ ТА ОСОБЛИВОСТЕЙ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ В УКРАЇНІ

З 24 лютого 2022 року, з початком повномасштабної агресії з боку росії, український кіберпростір зазнав безпрецедентного натиску. Кібератаки та збої стали зброєю ворога, спрямованою на дестабілізацію роботи державних сайтів, банківських систем, критичної інфраструктури.Під прицілом опинилися сайти Верховної Ради, Кабміну, МЗС, СБУ, Міноборони, Мінреінтеграції, ПриватБанку, Ощадбанку та багатьох інших установ.

Війна в інформаційному просторі несе не меншу загрозу, аніж бойові дії на фронті. Ризик кібератак з боку рф залишається високим як для України, так і для її європейських партнерів. Кібербезпека набуває ключового значення в економічній, політичній, соціальній та військовій сферах.

Сьогодні Україна відстоює не лише свою територіальну цілісність, але й право на незалежність, самостійний розвиток та мирне майбутнє. Перед вітчизняними правоохоронними органами постає все більше завдань з пошуку нових методів та засобів для ефективної протидії кіберзлочинності.

Державна політика України у сфері національної безпеки й оборони має комплексний характер і спрямована на забезпечення стійкості держави перед різними викликами та загрозами й регламентується Законом України «Про національну безпеку України» від 21 червня 2018 р. № 2468-VIII [1].

Стратегія кібербезпеки України (далі – Стратегія) – це документ довгострокового планування, який визначає:

– Загрози кібербезпеці: Стратегія ідентифікує актуальні та потенційні кіберзагрози для життєво важливих інтересів особи, суспільства та держави.

– Пріоритети: Визначає пріоритетні напрямки та концептуальні підходи до забезпечення кібербезпеки.

– Цілі: Створення умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства й держави.

Стратегія кібербезпеки України – це ключовий документ, який визначає курс України на забезпечення стійкості кіберпростору та захисту національних інтересів у цій сфері [2].

Кібербезпека України – це динамічна сфера, що потребує постійного вдосконалення та адаптації до нових викликів. Забезпечення стійкості кіберпростору держави ґрунтується на виваженій політиці, чітко окреслених пріоритетах та комплексних

заходах.

Основні напрямки

1) Створення захищеного національного сегмента кіберпростору:
– Формування стійкої до кібератак інфраструктури.
– Запровадження систем захисту інформаційних ресурсів.
– Підвищення обізнаності користувачів щодо кібергігієни.
2) Запобігання втручанню у внутрішні справи України:
– Протидія кібершпигунству та кібердиверсіям.
– Нейтралізація інформаційних атак та дезінформації.
– Захист критичної інфраструктури.
3) Посилення обороноздатності держави у кіберпросторі:
– Розвиток кібервійськ та підготовка кваліфікованих кадрів.
– Впровадження інноваційних технологій кіберзахисту.
– Співпраця з міжнародними партнерами.
4) Боротьба з кіберзлочинністю та кібертероризмом:
– Удосконалення законодавства та правозастосовної практики.
– Розслідування кіберзлочинів та притягнення винних до відповідальності.
– Підвищення рівня міжнародної співпраці.
5) Зниження рівня уразливості об'єктів кіберзахисту:
– Регулярний аудит та оновлення систем захисту.
– Підвищення кваліфікації фахівців з кібербезпеки.
– Впровадження програм підвищення обізнаності користувачів.
6) Повноправна участь у міжнародних системах кібербезпеки:
– Активна співпраця з міжнародними організаціями.
– Сприяння розвитку глобальних систем кібербезпеки.
– Впровадження міжнародних стандартів та рекомендацій.
7) Дотримання міжнародних зобов'язань:
– Виконання положень Конвенції про кіберзлочинність та інших міжнародних договорів.
– Співпраця з правоохоронними органами інших країн.
– Обмін інформацією та досвідом у сфері боротьби з кіберзлочинністю [3].

Національна стратегія у сферах безпеки та оборони націлено на забезпечення широкого спектру аспектів, таких як військова, зовнішньополітична, економічна, інформаційна, екологічна та кібернетична безпека України. Законодавчі норми, що спрямовані на захист національної кібербезпеки, виступають ключовим елементом в системі права країни, регулюючи відносини у сферах інформаційної безпеки, системи виборів, охорони здоров'я, оборони, транспорту, фінансів та банківської сфери. Ці норми сприяють забезпеченню інформаційного суверенітету України як суб'єкта міжнародного права. Прийняття спеціального законодавчого акта з кібербезпеки сприятиме не лише визначенню спеціалізованої термінології, а й установленню правових та організаційних засад державної політики у цьому напрямку, а також основних принципів та стратегій забезпечення кібербезпеки. Майбутні дослідження у галузі кібербезпеки мають на меті розробку структури цієї правової категорії та її взаємозв'язку з іншими аспектами права, зокрема в інформаційній сфері. Особливу увагу потребує питання використання штучного інтелекту в державному управлінні та судочинстві, яке вимагатиме подальшого правового регулювання, оскільки це не лише сприятиме розвитку, а й несе і значні ризики для національної інформаційної безпеки.

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2468-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text ()

2. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ президента України від 14 вересня 2020 року № 392/2020 URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text

3. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. [Видання друге, перероб. та доп.]. Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.