Ронська О.Г

к.е.н, доцент кафедри безпеки та правоохоронної діяльності,

Західноукраїнський національний університет

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ЕВОЛЮЦІЮ МІЖНАРОДНОЇ БЕЗПЕКИ

Стрімкий розвиток інформаційно-комунікаційних технологій суттєво змінив характер міжнародних відносин та підходи до забезпечення безпеки. У сучасному світі кіберпростір став важливим середовищем функціонування держав, міжнародних організацій, бізнесу та громадянського суспільства. Його значення виходить далеко за межі технологічної сфери, оскільки цифрові мережі впливають на політичні процеси, економічний розвиток, обороноздатність країн і стабільність міжнародної системи загалом.

Сьогодні кіберпростір розглядається як один із ключових елементів міжнародної безпеки. Залежність держав від цифрових технологій постійно зростає, а разом із цим збільшується вразливість до кіберзагроз. Інформаційні системи забезпечують функціонування державних органів, фінансового сектору, енергетики, транспорту, зв’язку та інших критично важливих сфер. Порушення їхньої роботи може спричинити значні економічні збитки, соціальну нестабільність і навіть створити ризики для національної безпеки [2].

Особливістю сучасного кіберпростору є його глобальний характер. Інформаційні потоки не обмежуються державними кордонами, що створює нові можливості для міжнародної співпраці, але водночас ускладнює контроль над цифровим середовищем. Кіберпростір став середовищем, у якому реалізуються як конструктивні, так і деструктивні форми взаємодії між державами. Саме тому питання кібербезпеки дедалі частіше

розглядаються як складова міжнародної політики та стратегічного планування.

Однією з головних особливостей сучасних міжнародних відносин є зростання ролі кіберконфліктів. На відміну від традиційних форм протистояння, кібероперації можуть здійснюватися дистанційно, швидко та з відносно невеликими витратами. Водночас наслідки таких дій можуть бути надзвичайно серйозними. Кібератаки здатні порушувати роботу державних установ, фінансових систем, енергетичних об'єктів та інших елементів критичної інфраструктури. Через це кіберпростір дедалі частіше розглядається як окрема сфера стратегічного протиборства.

Сучасні кіберзагрози мають різноманітний характер. До них належать несанкціонований доступ до інформаційних ресурсів, кібершпигунство, поширення шкідливого програмного забезпечення, викрадення конфіденційної інформації, атаки на інформаційні системи та інформаційно-психологічний вплив на населення. Особливу небезпеку становлять атаки на критичну інфраструктуру, оскільки вони можуть призводити до масштабних порушень функціонування держави та суспільства.

Важливою рисою кіберзагроз є складність встановлення джерела їх походження. У багатьох випадках визначити організаторів кібератаки надзвичайно складно через використання посередницьких серверів, анонімних мереж та інших засобів приховування діяльності. Це ускладнює процес міжнародного реагування та притягнення винних до відповідальності [1].

Особливе місце у сучасних конфліктах займають інформаційні операції, які поєднують технологічні та психологічні методи впливу. За допомогою цифрових платформ можуть поширюватися дезінформація, маніпулятивний контент та інші матеріали, спрямовані на формування певних суспільних настроїв або вплив на політичні процеси. У зв'язку з цим

кіберпростір дедалі частіше використовується як інструмент реалізації гібридних загроз.

З метою протидії сучасним викликам держави активно розвивають системи кібербезпеки. У багатьох країнах створені спеціалізовані структури, відповідальні за моніторинг кіберпростору, виявлення загроз та реагування на кіберінциденти. Основними напрямами їх діяльності є захист інформаційних ресурсів, кіберрозвідка, аналіз ризиків та координація заходів із забезпечення безпеки цифрової інфраструктури.

Важливим елементом сучасної безпекової політики є концепція кіберстримування. Її сутність полягає у формуванні таких умов, за яких потенційний противник усвідомлює неминучість відповідних дій у разі здійснення кібератаки. Досягнення цього результату потребує поєднання технічних, правових, організаційних та дипломатичних інструментів. Ефективність кіберстримування значною мірою залежить від рівня розвитку національної системи кіберзахисту та здатності держави співпрацювати з міжнародними партнерами [3]. Забезпечення кіберстійкості неможливе без належного захисту критичної інфраструктури. Для цього впроваджуються сучасні технології моніторингу мереж, системи раннього виявлення загроз, механізми резервування даних та плани реагування на надзвичайні ситуації. Не менш важливим є підвищення рівня цифрової грамотності населення та професійна підготовка фахівців у сфері кібербезпеки. Оскільки кіберзагрози мають транскордонний характер, важливого значення набуває міжнародне співробітництво. Ефективна протидія кіберзлочинності потребує обміну інформацією між державами, координації дій під час реагування на інциденти та вироблення спільних стандартів безпеки. Міжнародні організації та регіональні об’єднання активно працюють над удосконаленням механізмів співпраці у сфері кіберзахисту та створенням єдиних підходів до регулювання цифрового простору.

Значну увагу приділяють також формуванню міжнародних норм поведінки у кіберпросторі. Їхньою метою є зменшення ризику конфліктів, забезпечення відповідального використання цифрових технологій та підвищення рівня довіри між державами. Хоча універсальна система правового регулювання кіберпростору ще перебуває на стадії формування, міжнародна практика свідчить про зростання уваги до цього питання. У сучасних умовах кіберпростір є не лише джерелом потенційних загроз, а й важливим інструментом зміцнення міжнародної безпеки. Використання цифрових технологій дозволяє державам удосконалювати системи управління, підвищувати ефективність обміну інформацією та покращувати координацію дій під час кризових ситуацій. Саме тому розвиток кібербезпеки розглядається як один із пріоритетних напрямів забезпечення стабільності міжнародної системи.

Отже, кіберпростір перетворився на один із визначальних чинників сучасної архітектури міжнародної безпеки. Зростання кількості кіберзагроз, поширення цифрових технологій та підвищення залежності держав від інформаційних систем вимагають постійного вдосконалення механізмів кіберзахисту. Ефективне поєднання національних і міжнародних зусиль, розвиток правового регулювання та підготовка висококваліфікованих фахівців є необхідними умовами забезпечення безпеки та стабільності у цифрову епоху.

ЛІТЕРАТУРА

1. Білоконь М. В., Смаглюк А. А. (2024). Кібербезпека як складова економічної та національної безпеки // Український економічний часопис.

2. Ковальчук П. О. (2023). Кіберпростір у структурі міжнародної безпеки: теоретичний аспект // Науковий вісник міжнародних відносин.

3. Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. Ірпінський юридичний часопис. 2023. № 1(10). С. 180–186.