

Рец В. В., слухач магістратури
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Мирошниченко В. О.,
професор кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
(Дніпропетровський державний
університет внутрішніх справ)

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СТРАТЕГІЧНЕ ЗАВДАННЯ СВІТОВОЇ СПІЛЬНОТИ: ПРОБЛЕМАТИКА

У сфері забезпечення інформаційної безпеки на міжнародному рівні важливе значення має міжнародне співробітництво усіх суб'єктів міжнародного права, які диференційовано між собою взаємодіють. Інформаційна безпека є запорукою стабільності у світі. Саме тому держави, зокрема Україна, повинні здійснювати пошук спільних рішень в межах міжнародних організацій або в межах переговорів укладанням договорів або меморандумів, які стосуються напрямів протидії інформаційним та кіберзагрозам, кібервійнам, інформаційному тероризму та інформаційної злочинності. Треба зауважити, що світові проблеми, пов'язані з інформаційними загрозами, стосуються безпосередньо окремої держави, впливаючи на її суспільно-політичну, економічну, ідеологічну та багато інших сфер діяльності [1].

Міжнародне співтовариство створило нормативно-правову базу для реагування на кіберзлочини та кібертероризм і закликає держави до активної боротьби зі злочинними загрозами інформаційній безпеці. Однак проблематика полягає у відсутності ефективних механізмів, які б могли реалізувати матеріальні норми та рекомендації щодо попередження кіберзлочинів або притягнення осіб, що їх вчинили, до певного виду юридичної відповідальності. Боротьба з такими серйозними проблемами, як кіберзлочини та кібертероризм здійснюється державами через механізми міжнародного співробітництва в галузі права та безпеки. Державами контролюється використання технологій, комунікацій та ресурсів з тим, щоб вони не були використані для вчинення міжнародних злочинів та злочинів міжнародного характеру. Інформаційно-телекомунікаційні мережі – це платформа, на якій зібрано значний моноліт інформації, саме тому вони є інструментом поширення екстремістських позицій, а також відомостей, які становлять загрозу для національної безпеки окремої держави. Міжнародне співтовариство, базуючись на існуючій та функціонуючій нормативно-правовій базі, робить кроки до формування дієвих та ефективних механізмів попередження інформаційних загроз із диференційованих джерел. На сьогодні досягнуто певного успіху в цій царині, адже у розробці норм

двостороннього і багатостороннього співробітництва для запобігання вчинення правопорушень у сфері користування Інтернетом та іншими інформаційними та телекомунікаційними базами даних або банками інформації досягнуто неабиякого прогресу [2].

Необхідно наголосити, що світова спільнота має чимало напрацювань у сфері забезпечення інформаційної безпеки, значна кількість яких робить акцент на необхідності чіткого розуміння і виокремлення факторів, що зумовлюють загострення загроз інформаційній безпеці. Детермінанти загроз інформаційної безпеки є системними та створюють перешкоди для реалізації прав і свобод людини та громадянина кожної окремої держави. М. Т. Гаврильців зазначає, що аналіз викликів – це завжди суб'єктивний процес сприйняття суб'єктом певних факторів через призму власних інтересів і професійності [3, с. 201].

У теорії інформаційної безпеки розглядається механізм загрози безпековому компоненту в межах гібридної війни. Зокрема, посягання на інформаційну безпеку держави під час гібридної війни здійснюється за такою моделлю: агресор втручається в інформаційно-комунікаційний простір країни з метою придушення опору та формування ідеологічної позиції і переконань, які відповідають інтересам агресора. Це здійснюється з використанням різноманітних інструментів маніпулювання, починаючи від впливу і маніпуляції громадською думкою через засоби масової інформації і аж до вчинення кіберзлочинів [4, с. 18]. Саме тому на сьогодні світова спільнота вважає, що запобігання загрозам інформаційній безпеці як важливому елементу національної безпеки є одним із стратегічних завдань і формує низку відповідних концепцій.

Отже, міжнародна інформаційна безпека сьогодні є стратегічним завданням всього світового співтовариства, зусиллями якого створено значну нормативно-правову базу із запобігання кіберзагрозам. Однак проблематика полягає у відсутності ефективних механізмів, які б могли реалізувати матеріальні норми та рекомендації щодо попередження кіберзлочинців або притягнення їх до певного виду юридичної відповідальності. Боротьба із такими серйозними проблемами, як кіберзлочини та кібертероризм здійснюється державами через механізми міжнародного співробітництва в галузі права та безпеки.

Бібліографічні посилання

1. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. Актуальні проблеми міжнародних відносин. 2011. Вип. 102 (Ч. I).
2. Report on World Internet Development 2016 of World Internet Conference «Innovation-driven Internet Development for the Benefit of All – Building a Community of Common Future in Cyberspace». URL: http://www.wuzhenwic.org/2016-11/18/c_61834.htm (дата звернення: 08.10.2021).
3. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200–203.
4. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 4. С. 16–26.