5. Про розвідку : Закон України від 17 вересня 2020 року № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text
6. Про державне бюро розслідувань : Закон України від 12 листопада 2015 року № 794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19#Text
7. Про бюро економічної безпеки України : Закон України 28 січня 2021 року № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20#Text
8. Про внесення змін до деяких законодавчих актів України щодо посилення повноважень Національного атикорупційного бюро України та Спеціалізованої антикорупційної прокуратури : Закон України від 31.07.2025 № 4560- IX URL: https://zakon.rada.gov.ua/laws/show/4560-20#Text
9. Про затвердження Інструкції про порядок проведення психофізіологічного дослідження із застосуванням поліграфа в органах прокуратури України : наказ Генеральної прокуратури України від 27.10.2025 № 341. URL: https://data.gov.ua/dataset/59cef317-2fc6-4f50-9915-fba3264d5783/resource/926e62bc-1e8b-48b2-87eb-0c549f4f62dc (дата звернення: 03.04.2026).
10. Про затвердження Інструкції про порядок використання поліграфів у Національній поліції України : наказ Міністерства внутрішніх справ України від 13.11.2017 № 920. URL: https://zakon.rada.gov.ua/laws/show/z1472-17#Text (дата звернення: 03.04.2026).
11. Про затвердження Інструкції з організації та проведення психофізіологічного дослідження персоналу із застосуванням поліграфа у Міністерстві оборони України та Збройних Силах України : наказ Міністерства оборони України від 14.04.2015 р. № 164. URL: https://zakon.rada.gov.ua/laws/show/z0477-15#Text

УДК 340.1

Ронська О. Г.
к.е.н., доцент кафедри безпеки та правоохоронної діяльності,
Західнроукраїнський національнимй університет

КІБЕРПРОСТІР У СТРУКТУРІ СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

Сучасна система міжнародної безпеки перебуває у стані глибоких трансформацій, що зумовлено активним розвитком цифрових технологій та глобалізацією інформаційного середовища. Кіберпростір поступово інтегрується у всі сфери державного управління та міжнародних відносин, стаючи одним із ключових чинників забезпечення безпеки. Він охоплює політичну, економічну, військову та соціальну сфери, що значно підвищує його стратегічне значення. У наукових дослідженнях наголошується, що цифровізація не лише відкриває нові можливості, але й формує комплекс новітніх ризиків, пов’язаних із кіберзагрозами та інформаційним впливом [2]. Водночас залежність суспільства від цифрових технологій зростає, що підвищує вразливість держав до зовнішніх втручань. Особливо це стосується

країн, які перебувають у стані політичної або військової нестабільності.

У сучасних геополітичних умовах домінування в кіберпросторі розглядається як важливий показник державної спроможності. Кібероперації активно застосовуються як інструмент досягнення стратегічних цілей, зокрема через вплив на інформаційно-комунікаційні системи управління. Вони дозволяють здійснювати прихований вплив без прямого застосування військової сили. Особливе значення має кіберрозвідка як складова національної безпеки та механізм попередження загроз [1]. Крім того, кіберрозвідка забезпечує своєчасне виявлення потенційних атак і сприяє формуванню ефективної системи реагування. У цьому контексті важливим є розвиток аналітичних центрів та обмін інформацією між союзниками.

Кіберпростір сформувався як самостійна сфера протиборства, що доповнює традиційні домени ведення війни. Його специфіка полягає у відсутності чітких механізмів стримування та залученні широкого кола акторів, включаючи недержавні структури. Це ускладнює питання відповідальності та регулювання у сфері міжнародної безпеки [4, с. 67]. Водночас анонімність у кіберпросторі створює додаткові труднощі для ідентифікації джерел загроз. Через це держави змушені розробляти нові підходи до міжнародно-правового регулювання кібердіяльності. Значну роль відіграє формування норм поведінки держав у цифровому середовищі.

Суттєвою особливістю кіберконфліктів є їхня доступність та відносно низькі витрати на реалізацію. Водночас наслідки кібератак можуть бути масштабними та критичними для держави. Зокрема, атаки можуть призводити до порушення функціонування енергетичних систем, транспорту або фінансових установ. Значного поширення набувають інструменти інформаційного впливу, кібершпигунства та використання шкідливого програмного забезпечення [2]. Крім того, інформаційні операції можуть суттєво впливати на політичні процеси та громадську думку. Це створює додаткові виклики для демократичних суспільств.

Держави у відповідь на зростання кіберзагроз формують комплексні системи кіберзахисту, які включають технічні, організаційні та правові компоненти. Особлива увага приділяється захисту критичної інфраструктури, яка є основною ціллю кібератак. Дослідники підкреслюють, що сучасні загрози мають системний характер і здатні впливати на ключові сфери функціонування суспільства. Важливим напрямом є створення центрів реагування на кіберінциденти та впровадження систем раннього попередження. Також значну роль відіграє співпраця держави з приватним сектором у сфері кібербезпеки. Така взаємодія дозволяє підвищити ефективність захисту інформаційних ресурсів.

Кіберзагрози характеризуються складністю, багатовекторністю та транснаціональним характером. Вони охоплюють несанкціонований доступ до інформаційних систем, поширення шкідливого програмного забезпечення, інформаційно-психологічні операції та маніпуляції громадською думкою. У сучасних умовах кіберзагрози часто поєднуються з іншими формами гібридного впливу. Це значно ускладнює процеси їх виявлення та нейтралізації. Крім того, швидкість поширення інформації в цифровому середовищі значно підсилює ефект таких загроз. Це вимагає від держав оперативності та гнучкості у прийнятті рішень.

Важливим інструментом протидії є концепція кіберстримування, яка передбачає формування здатності держави до ефективної відповіді на загрози. Її реалізація потребує розвитку кадрового потенціалу, міжнародної співпраці та впровадження сучасних підходів до кіберзахисту [2, с. 183]. Важливим аспектом є також підвищення рівня кіберграмотності населення. Це дозволяє зменшити вплив інформаційних атак та маніпуляцій. Крім того, держави активно впроваджують стратегії кібербезпеки на національному рівні.

Отже, кіберпростір є важливим елементом сучасної архітектури міжнародної безпеки, що визначає нові принципи взаємодії держав. Його значення постійно зростає, що потребує вдосконалення механізмів захисту та координації міжнародної діяльності у сфері кібербезпеки. У перспективі роль кіберпростору лише посилюватиметься, що робить необхідним подальший розвиток міжнародного співробітництва. Ефективна кібербезпекова політика стає важливою умовою забезпечення стабільності світового порядку.

ЛІТЕРАТУРА:

1. Козій А., Марченко Т., Шевченко В. Актуальні проблеми протидії кіберзлочинності в Україні. *Theoretical foundations of state and law*. 2022. P. 59–65.

2. 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.

3. Онищенко С., Глушко А. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. Національний університет ім. Юрія Кондратюка. 2022. № 1 (84). С. 13–20.

4. Пелих А. О. Кіберпростір як новий вимір міжнародної безпеки // *Гілея: науковий вісник*. Київ, 2023. Вип. 182. С. 65–70.

УДК 351:004

Голда М.
аспірат Західноукраїнського національного університету

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним із наріжних каменів системи управління на всіх рівнях функціонування суб’єктів організованої діяльності – від підприємницьких структур, господарських організацій і бюджетних установ до органів та інституцій регіональної й загальнодержавної законодавчої та виконавчої влади – є належне інформаційне забезпечення. Без відповідної інформації не може бути прийняте жодне управлінське рішення. Роль інформаційного забезпечення невпинно зростає в умовах інформаційного суспільства та розвитку інформаційних технологій.

У сучасних умовах ефективність державного управління, функціонування господарського комплексу країни, діяльність підприємств, установ і організацій значною мірою залежать від рівня та досконалості інформаційного