МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут міжнародних відносин
імені Б. Д. Гаврилишина
Кафедра політології та філософії імені Сергія Коновала

ДИПЛОМНА РОБОТА

бакалавра

на тему:

«Кібербезпека та політика: роль інформаційних технологій у сучасних міжнародних відносинах»

Виконавець:
Студент 4 курсу групи Пол-41
Золотогурський Денис

Науковий керівник:
кандидат історичних наук,
доцент Руслан Чигур

Тернопіль–2025

З М І С Т

ВСТУП

Актуальність теми дослідження. Кібербезпека в умовах сучасного глобалізованого світу стала однією з основних складових міжнародної безпеки. Розвиток інформаційних технологій значно змінив характер міжнародних відносин, вивівши на перший план нові загрози, пов'язані з кіберпростором. Кібернапади, хакерські атаки, кібершпигунство та кібертероризм стали не лише технічними проблемами, але й серйозними політичними та економічними викликами для держав і міжнародних організацій.

Оскільки кіберпростір не має чітких географічних кордонів, держави все більше стикаються з необхідністю адаптації своїх політичних і правових систем до нових реалій. Саме тому важливість вивчення кібербезпеки та її впливу на міжнародні відносини зростає з кожним роком.

Ступінь вивчення проблеми. Дослідження проблеми кібербезпеки має багаторічну історію, однак інтерес до цієї теми значно зріс після масових кібератак на ключові інфраструктури держав та міжнародних організацій. Останніми роками з'явилася значна кількість наукових робіт, присвячених кібербезпеці як частині міжнародної політики, а також правовим аспектам кіберзагроз.

Водночас питання інтеграції інформаційних технологій у міжнародні відносини та розробки ефективних політик кібербезпеки ще залишаються недостатньо дослідженими в контексті глобальної політики. Тому проблема створення міжнародного правового поля, що регулює кіберпростір, залишається актуальною для науковців та практиків.

Метою даного дослідження є вивчення ролі кібербезпеки та інформаційних технологій у сучасних міжнародних відносинах, а також визначення їх впливу на політику та безпеку на глобальному рівні.

Відповідно до мети формулюємо такі **завдання**:

- визначити теоретико-методологічні засади кібербезпеки та її роль у міжнародних відносинах;

- дослідити вплив інформаційних технологій на розвиток міжнародної політики та дипломатії;

- проаналізувати основні кіберзагрози, які впливають на глобальну безпеку;

- розглянути політичні, правові та соціальні аспекти кібербезпеки в контексті міжнародних відносин.

Об'єктом дослідження є процеси, що відбуваються у сфері кібербезпеки та інформаційних технологій, які мають безпосередній вплив на міжнародні відносини та політику глобального рівня.

Предметом дослідження є роль кібербезпеки в міжнародних відносинах, а також взаємодія між державами, міжнародними організаціями та недержавними акторами в контексті кіберзагроз.

Методи дослідження. Для досягнення поставленої мети та завдань у дослідженні застосовуватимуться такі методи: аналіз і синтез, порівняльний метод, метод кейс-стаді, контент-аналіз, а також методи міжнародного права для дослідження правового регулювання кіберпростору. Важливим є також використання інтердисциплінарного підходу, що дозволяє інтегрувати знання з галузі політичних наук, міжнародних відносин, комп'ютерних наук та права.

Практичне значення дослідження. Результати дослідження мають важливе практичне значення для формування державної політики в сфері кібербезпеки, а також для розробки рекомендацій щодо вдосконалення міжнародного правового поля, яке регулює діяльність у кіберпросторі. Окрім

того, вони можуть бути використані у навчальному процесі для підготовки фахівців у сфері міжнародних відносин, кібербезпеки та права.

Апробація роботи. Окремі положення дипломної роботи доповідалися на Всеукраїнській науково-практичній конференції «Від війни до миру: філософія політики у світі геополітичних конфліктів, кризи демократії та нових форм влади» (Тернопіль, 13-14 травня 2024 р.)

Структура роботи визначається метою та завданнями дослідження. Дипломна робота, зміст якої викладено на 34 сторінках. Вона складається зі вступу, трьох проблемних розділів, висновків та списку використаних джерел із 32 найменуваннями.

РОЗДІЛ 1. Теоретико-методологічна основа кібербезпеки в контексті міжнародних відносин

У сучасному світі, де глобалізація та інформаційні технології стали основними драйверами розвитку, кібербезпека набуває надзвичайно важливого значення в контексті міжнародних відносин. Сучасні технології, зокрема Інтернет, соціальні мережі та великі дані, стали не лише інструментами економічного розвитку і комунікації, а й новими майданчиками для політичних взаємодій, які можуть впливати на національні інтереси і безпеку держав.

Кібербезпека як наукова дисципліна виникла на стику кількох галузей знань: комп'ютерних наук, міжнародних відносин, права та політики. Ключовим елементом теоретичних основ кібербезпеки є розуміння кіберпростору як середовища, що не має фізичних кордонів, що робить його не тільки новим простором для взаємодії держав і недержавних акторів, але й новою ареною для протистояння у рамках міжнародної політики.

«Однією з основних теоретичних концепцій кібербезпеки є ідея кіберсуверенітету, яка передбачає, що кожна держава повинна мати контроль над своїм кіберпростором і захист від зовнішніх кіберзагроз. Вона бере свій початок з традиційного поняття суверенітету в міжнародних відносинах, але адаптоване до умов глобальної мережі» [16, с. 34].

Кіберсуверенітет передбачає не тільки можливість захищати свої національні інформаційні інфраструктури, але й право на самостійне визначення політики в кіберпросторі без втручання з боку інших держав.

Іншою важливою теоретичною концепцією є кібербезпека як складова частина національної безпеки. Залежно від конкретних умов, кіберзагрози можуть ставати частиною загроз для національної стабільності та суверенітету. Це означає, що країни повинні розглядати кібербезпеку на рівні стратегії

національної безпеки, враховуючи те, як інформаційні технології можуть впливати на політичні процеси, економічну стабільність та соціальний порядок.

Також значну роль «у теоретичному осмисленні кібербезпеки відіграють концепції глобального управління в кіберпросторі. Ця ідея передбачає, що кібербезпека має бути предметом міжнародної співпраці, а не лише внутрішньою справою окремих держав» [1].

Вона грунтується на розумінні того, що кіберзагрози є транснаціональними, і для їх ефективного подолання необхідна колективна дія на міжнародному рівні. У цьому контексті важливим є розвиток міжнародних стандартів, угод та механізмів співпраці між державами щодо захисту від кіберзагроз.

Методологічні підходи до дослідження кібербезпеки в контексті міжнародних відносин є міждисциплінарними та інтегрують знання з різних наукових галузей, включаючи політичні науки, міжнародне право, інформатику та соціологію. Основними методами дослідження є:

1. Аналіз і синтез. Це основні методи, які дозволяють систематизувати інформацію про кіберзагрози, їх вплив на міжнародні відносини, а також сформулювати пропозиції щодо зміцнення кібербезпеки на глобальному рівні.
2. Порівняльний метод. Використовується для порівняння різних підходів до кібербезпеки, які застосовуються в різних країнах або міжнародних організаціях. Це дозволяє виявити найбільш ефективні стратегії та практики в сфері кібербезпеки.
3. Метод кейс-стаді. Використовується для детального аналізу конкретних випадків кіберзагроз або атак, що відбулися на міжнародному рівні. Це

дозволяє глибше зрозуміти характер кіберзагроз, реакцію держав та міжнародних акторів, а також наслідки таких атак.

4. Методи міжнародного права. Оскільки кібербезпека має значний правовий аспект, важливим є застосування правових методів для вивчення міжнародних угод та конвенцій, що регулюють кіберпростір, а також аналізу розвитку міжнародного права в цьому контексті.

Теоретична основа кібербезпеки не була б повною без вивчення природи та різновидів кіберзагроз, з якими стикаються держави та міжнародні організації. Однією з основних рис сучасних кіберзагроз є їх глобальний характер. Вони можуть здійснюватися з будь-якої точки світу, що ускладнює ідентифікацію джерела загрози та ефективне реагування на неї [32].

Кіберзагрози можна поділити на кілька категорій:

1. «Кібератаки на інфраструктуру. Це можуть бути атаки на енергетичні системи, фінансові установи, медичні заклади або навіть транспортні мережі. Такі атаки мають прямий вплив на безпеку держав і можуть спричинити серйозні економічні та соціальні наслідки.
2. Кібершпигунство. Це збори розвідувальної інформації через кіберпростір. Держави активно використовують кібершпигунство для отримання секретної інформації з інших країн або міжнародних організацій» [2, с. 57].
3. Інформаційні війни та пропаганда. Сучасні інформаційні технології дозволяють державам і політичним акторам вести війни через інформаційні канали. Вони включають маніпулювання громадською думкою, дезінформацію та вплив на вибори в інших країнах.
4. Кібертероризм. Важливий вид кіберзагрози, що передбачає використання кіберзасобів для досягнення політичних чи ідеологічних цілей через створення хаосу або заподіяння шкоди [31].

Таким чином, теоретико-методологічні основи кібербезпеки в контексті міжнародних відносин включають не тільки теоретичне осмислення кіберпростору як нової арени міжнародних відносин, але й розробку методів для вивчення кіберзагроз, їх впливу на політичні та економічні процеси, а також національні та міжнародні стратегії захисту. Враховуючи глобальний характер кіберзагроз, кібербезпека має стати важливим аспектом не лише національної безпеки кожної країни, а й частиною міжнародної співпраці в галузі безпеки та правового регулювання кіберпростору.

РОЗДІЛ 2. Інформаційні технології та їх вплив на міжнародні відносини

2.1. Цифрові технології як новий інструмент глобальної політики

Цифрові технології стали важливим елементом сучасної глобальної політики, і їх вплив на міжнародні відносини зростає з кожним роком. Інформаційно-комунікаційні технології, такі як Інтернет, соціальні мережі, великі дані, штучний інтелект та інші новітні технології, відкривають нові можливості для держав і міжнародних акторів у сфері дипломатії, економіки, безпеки та навіть у веденні війни.

«Цифрові інструменти дозволяють значно змінити структуру та динаміку міжнародних відносин, створюючи нові форми взаємодії, але водночас і нові виклики для глобальної стабільності» [30].

Інтернет і цифрові платформи сприяли розвитку цифрової дипломатії, де держави почали використовувати онлайн-канали для комунікації не лише з іншими урядами, а й безпосередньо з громадянами та міжнародною спільнотою. Це дозволяє країнам швидше реагувати на події, оперативно публікувати заяви, коментарі та пропозиції, а також активно вести інформаційну кампанію щодо власних політичних або економічних інтересів.

Однією з ключових особливостей цієї нової форми дипломатії є значно більша доступність і швидкість передачі інформації, що може змінювати ставлення громадськості та міжнародних акторів до певних політичних ініціатив чи ситуацій.

У зв’язку з цією зміною також зростає роль інформаційних війн у глобальній політиці. Держави, а також політичні групи та окремі актори, можуть маніпулювати громадською думкою через цифрові платформи, використовуючи інформаційні війни як інструмент зовнішньої політики. Це можуть бути кампанії

з дезінформації, маніпуляції фактами або навіть прямі атаки на інформаційні системи іншої країни. Використання таких технологій в інформаційних кампаніях дозволяє значно впливати на політичні процеси в інших країнах, наприклад, підривати стабільність, створюючи соціальне напруження чи підтримуючи політичні рухи, вигідні певним державам.

«Цифрові технології також сприяють розвитку нових форм економічного впливу. Завдяки розвитку фінансових технологій, криптовалют та електронної комерції, країни можуть здійснювати міжнародний економічний вплив через цифрові платформи» [25].

Протягом останніх десятиліть ми стали свідками того, як нові цифрові технології дозволяють створювати нові бізнес-моделі, що поєднують традиційну економіку з інноваціями. Наприклад, глобалізація фінансових ринків і зростання електронних платежів змінюють структуру міжнародної торгівлі та фінансів, надаючи більші можливості для економічних стратегій, заснованих на цифрових технологіях.

У той же час цифрові технології створюють нові загрози для національної безпеки. Кіберзагрози стали невід'ємною частиною глобальної політики, а кібервійни - новою формою геополітичних конфліктів. Атаки на критичні інфраструктури, банки, енергетичні мережі та інші важливі об'єкти можуть суттєво порушити стабільність і економіку країни. Водночас кіберзагрози мають потенціал для масштабного впливу, оскільки вони можуть бути реалізовані через мережу Інтернет, де кордони між країнами стають нечіткими і важко визначити джерело атаки.

«Ще одним важливим аспектом використання цифрових технологій у глобальній політиці є м'яка сила, яку країни використовують для впливу на міжнародні відносини. Завдяки сучасним технологіям держави можуть

просувати свою культурну та ідеологічну політику через медіа, Інтернет-ресурси, соціальні мережі та культурні обміни. Такі інструменти дозволяють надавати значну підтримку національним інтересам без використання силових методів, але з великим потенціалом для змін у міжнародному впливі» [20].

Таким чином, цифрові технології не лише трансформують саму природу політичних відносин, але й дають нові можливості для маніпулювання міжнародною ситуацією, що значно ускладнює глобальне управління та міжнародне співробітництво. Зокрема, цифрові інструменти стають важливими в умовах глобальної конкуренції, де інформація і здатність її контролювати можуть стати вирішальними для досягнення стратегічних цілей.

У зв’язку з цим на порядок денний постає питання розвитку міжнародних норм і стандартів, які дозволять ефективно регулювати діяльність у цифровому середовищі та забезпечити безпеку й стабільність на глобальному рівні.

Процес цифровізації значною мірою вплинув на трансформацію міжнародних відносин, а цифрові технології стали невід'ємною частиною глобальної політики. Вони відкрили нові можливості для співпраці між державами, але одночасно створили нові ризики та загрози для стабільності в міжнародному середовищі [15].

Однією з основних складових цієї трансформації є зміна концепції державного суверенітету, що стає дедалі менш чітким в умовах безперервної інтеграції національних економік у глобальну цифрову мережу. Взаємодія держав на цифрових платформах все більше визначається не лише традиційними політичними та економічними чинниками, а й новими правилами, що формуються в цифровому середовищі.

У цьому контексті важливим аспектом є не тільки вплив цифрових технологій на дипломатію та економіку, але й виникнення нових проблем у галузі

права та регулювання. Відсутність міжнародно визнаних стандартів для регулювання кіберпростору призводить до ситуації, коли держави змушені самостійно розробляти механізми захисту своїх національних інтересів у цифровій сфері.

«Одним із важливих аспектів цього питання є необхідність у створенні глобальних правових норм для регулювання кібербезпеки, боротьби з кіберзлочинністю та забезпечення конфіденційності даних. Ці питання стосуються не тільки національних урядів, але й великих транснаціональних корпорацій, які мають доступ до величезних масивів даних, що використовуються для ведення бізнесу на міжнародному рівні» [10].

Крім того, важливо враховувати, що цифрові технології змінюють не лише способи взаємодії між державами, але й загальний порядок ведення глобальної політики. Вони сприяють формуванню нових глобальних акторів, які можуть бути не тільки державами, а й потужними приватними компаніями та міжнародними організаціями.

Враховуючи це, цифрові технології створюють умови для глобальної координації зусиль у боротьбі з новими викликами, такими як кіберзагрози або зміни клімату, де потрібен ефективний міжурядовий і міжсекторальний діалог. Цифрові платформи допомагають краще координувати міжнародні операції, вести спільну політику щодо боротьби з транснаціональними проблемами і одночасно дозволяють ефективніше відслідковувати реалізацію домовленостей між державами [5].

Усе це ставить перед міжнародними організаціями та державами нові завдання, пов'язані з адаптацією до нових реалій. Міжнародні інституції, такі як ООН, Всесвітня організація торгівлі, а також нові, спеціалізовані органи, повинні активно включати цифрові технології в механізми глобального управління.

Однак існує проблема, яка полягає в різному рівні розвитку цифрових інфраструктур та політик серед країн. У цьому контексті важливою є концепція цифрової нерівності, яка означає нерівний доступ до цифрових технологій і можливостей на глобальному рівні. Це не лише економічний, а й політичний виклик, що може призвести до додаткової маргіналізації деяких країн або регіонів на світовій арені.

Водночас, не можна забувати й про те, що технології, такі як штучний інтелект, блокчейн і великі дані, розвиваються із швидкістю, яка значно випереджає нормативне регулювання. Це відкриває нові можливості для розвитку, але й створює значні ризики, коли технології використовуються не в інтересах загального блага, а для досягнення вузько політичних чи економічних цілей [3].

У таких умовах критично важливим є передбачення та адаптація нормативних актів, здатних охопити швидко змінювані технології, а також міжнародне співробітництво для формулювання універсальних стандартів, які зможуть забезпечити безпеку і захист прав людини в цифровому просторі.

Таким чином, у світі, що швидко цифровізується, виникає новий етап глобальної політики, в якому цифрові технології стають не тільки важливим інструментом для національного розвитку, а й основним фактором глобальної конкуренції. Важливо, щоб держави розуміли не лише економічний, але й політичний та соціальний вплив цифрових технологій на міжнародні відносини.

2.2. Кіберзагрози та нові форми конфліктів у міжнародній політиці

У сучасному світі кіберзагрози стали невід'ємною частиною міжнародної політики, оскільки вони можуть серйозно вплинути на безпеку держав, економіку та соціальну стабільність. З кожним роком все більше країн усвідомлюють, що

традиційні методи забезпечення безпеки вже не є достатніми для захисту від нових форм атак, які реалізуються через Інтернет. Кіберзагрози можуть бути як зовнішніми, так і внутрішніми, і вони мають здатність перекроювати міжнародні відносини, ставлячи під загрозу стабільність на глобальному рівні. Атаки на важливі інфраструктурні об'єкти, такі як енергетичні мережі, фінансові системи чи урядові сервери, можуть мати далекосяжні наслідки для держави та її міжнародних партнерів.

«Одним із найбільших викликів є те, що в кіберпросторі важко відстежити джерело атаки, оскільки кібероперації можуть бути здійснені анонімно, що ускладнює визначення відповідальних за них. Ця анонімність дає можливість державам або неурядовим акторам здійснювати кібератаки на інші країни, не зважаючи на міжнародне право або дипломатичні норми» [29].

Наприклад, в разі кібератак на критичні інфраструктури іншої держави складно довести, що це була державна ініціатива, оскільки атаки можуть бути здійснені через проксі-сервери або інші способи маскування ідентичності. Це відкриває нові можливості для ведення прихованих конфліктів, де основним інструментом є кібернапади.

У міжнародній політиці кіберзагрози використовуються не тільки для економічного саботажу, але й для політичного впливу. Кібератаки на державні органи можуть бути спрямовані на дискредитацію урядів або навіть зміщення політичних лідерів. Також важливою частиною цього процесу є використання кіберзагроз для підриву довіри до національних виборчих систем, що може впливати на результат виборів і навіть на внутрішню стабільність країни [4].

Крім того, цифрові атаки можуть бути направлені на втручання в зовнішньополітичні процеси, наприклад, через поширення фейкових новин чи

дезінформації, що може призвести до зміни політичних настроїв у сусідніх країнах.

Такі загрози вимагають від держав розробки нових стратегії безпеки, включаючи вдосконалення кіберзахисту та розширення міжнародного співробітництва в сфері кібербезпеки. Однак важливою проблемою залишається відсутність єдиного міжнародного правового механізму, який би чітко визначав, як слід реагувати на кібернапади, і який би встановлював глобальні стандарти для боротьби з такими загрозами [6].

Багато країн намагаються створити власні нормативні акти, проте це може призвести до фрагментації у глобальній кібербезпеці, оскільки різні держави мають різний рівень технологічної підготовленості та різні погляди на регулювання кіберпростору.

Загалом, кіберзагрози в міжнародній політиці визначають нові правила гри у сфері безпеки. Вони змушують держави адаптувати свої зовнішньополітичні стратегії до нових реалій, де кібербезпека стає не лише питанням національного захисту, а й елементом глобального управління. Враховуючи, що кібернапади можуть мати руйнівний ефект на міжнародні відносини, важливо розвивати міжнародні угоди та механізми співпраці, які дозволяють ефективно реагувати на ці нові виклики [28].

Окрім безпосередніх загроз для інфраструктури, економіки та політичної стабільності, кіберзагрози також активно використовуються для формування глобальних альянсів та міжнародних стратегій впливу. У сучасному світі, де інформація є одним з найцінніших ресурсів, держави, що володіють потужними кіберздатностями, можуть використовувати свої можливості для просування власних інтересів через управління даними, виведення конкурентів з ринку або навіть маніпулювання соціальними настроями в інших країнах.

«Кібероперації можуть стати інструментом не лише політичного впливу, але й елементарної геополітичної гри, де контролювання інформаційних потоків стає важливим фактором сили» [7].

Цифрові технології дають можливість створювати нові форми міжнародних відносин, де ключову роль відіграють не лише традиційні дипломатичні канали, але й платформи соціальних мереж, форуми в Інтернеті, форуми в онлайн-просторі, що створює додаткові канали для комунікації та потенційного впливу.

Така ситуація уможливлює «глобальну конкуренцію за дані», де країни намагаються отримати контроль над інформаційними ресурсами, що лежать в основі сучасних економічних і політичних відносин. Адже дані стали новою формою валютної цінності, зокрема для таких гравців на міжнародній арені, як великі технологічні компанії [27].

Однією з найбільших проблем у кіберпросторі є питання цифрового суверенітету, яке стосується здатності держави контролювати інформаційні потоки всередині своїх кордонів, а також захищати своїх громадян від впливу ззовні. Це питання стає дедалі важливішим у контексті глобальної інтеграції, коли дані перетинають національні кордони, а іноземні технологічні компанії мають доступ до критично важливої інформації, що потенційно може бути використана проти національних інтересів. Цифровий суверенітет також включає контроль над ключовими цифровими інфраструктурами, такими як національні сервери, хмарні обчислення та комунікаційні мережі, що дозволяє забезпечити стабільність і захист від зовнішнього кібервпливу [8].

У результаті таких змін держави все більше усвідомлюють необхідність створення глобальних стандартів для забезпечення кібербезпеки. Виникає потреба в нових міжнародних угодах, які б забезпечували координацію зусиль

щодо боротьби з кіберзлочинністю, встановлення правил використання інформаційних технологій у конфліктних ситуаціях і розробки стандартів для захисту конфіденційності даних.

Це потребує створення механізмів для співпраці між державами на рівні обміну інформацією про загрози, а також розробки міжнародних стратегій з протидії кібератакам, які можуть використовуватись для саботажу, економічного підриву або навіть військових конфліктів.

Таким чином, кіберзагрози стають не просто питанням безпеки окремих країн, а й важливою частиною глобальної політики, де боротьба за контроль над інформацією і даними визначає успіх у сучасному світі. У зв’язку з цим питання кіберзахисту та міжнародного співробітництва в кіберпросторі виходять на перший план у глобальній політичній та економічній боротьбі. У той же час країни повинні активно розвивати свою кіберзахисну інфраструктуру, зокрема, у співпраці з іншими державами, аби ефективно протистояти новим викликам цифрового світу.

«Цифрові загрози та розвиток технологій призвели до виникнення нових форм конфліктів у міжнародній політиці, де традиційні методи ведення війни все частіше змінюються на технологічні і інформаційні війни. Технології не тільки змінюють характер конфліктів, а й визначають їхню інтенсивність і спосіб реалізації» [26].

Одним із яскравих прикладів таких змін є поява кіберконфліктів, де замість фізичних зіткнень держави все частіше застосовують атаки на інформаційні системи, енергетичну інфраструктуру або фінансові структури інших країн. Такі конфлікти можуть бути менш помітними для широкої громадськості, але вони здатні мати далекосяжні наслідки для економік і стабільності держав, не викликаючи при цьому безпосереднього фізичного руйнування.

Іншим важливим аспектом є зміна характеру політичних суперечок, що виходять за межі класичних дипломатичних і військових засобів. Тепер держави можуть вести війни за допомогою інформаційних стратегій, маніпулюючи громадською думкою за допомогою соціальних медіа, фейкових новин, кібератак і навіть підривної діяльності всередині інших країн [9].

Ці нові форми конфліктів, відомі як гібридні війни, можуть бути дуже складними для визначення їхніх ініціаторів, оскільки зловмисники часто використовують анонімні канали або приховані впливи, такі як фінансування радикальних політичних рухів або підтримка протестів, що сприяє політичній дестабілізації.

З розвитком нових технологій, таких як штучний інтелект та блокчейн, конфлікти набувають ще більшого масштабу, коли країни намагаються не лише впливати на внутрішні політичні процеси інших держав, але й забезпечити технологічну перевагу у глобальній економіці. В цьому контексті технологічні війни часто стають елементом конкурентної боротьби на світових ринках, коли держави борються за доступ до стратегічних ресурсів, таких як дані, інтелектуальна власність, або навіть нові інноваційні технології.

Технологічний контроль над ресурсами, що знаходяться в Інтернеті, або здатність впливати на їхню доступність, стає важливим інструментом у нових конфліктах, де економічна та політична сила визначається здатністю маніпулювати технологіями [24].

У таких умовах світова політика переживає перехід від традиційної концепції збройних конфліктів до концепції конфліктів без застосування сили, де важливими інструментами стають не лише військові сили, але й технологічні платформи, юридичні системи, інформаційні ресурси та економічні механізми. Відтак нові форми конфліктів створюють необхідність в адаптації міжнародних

інституцій до цих викликів. Це передбачає не тільки розробку нових норм міжнародного права, що стосуються кібербезпеки та інформаційних війн, але й реформи в рамках міжнародних організацій, таких як ООН або СОТ, для більш ефективної регуляції і вирішення суперечок в умовах технологічної глобалізації.

«Такий перехід до нових форм конфліктів робить міжнародну політику набагато складнішою і багатовимірною. У той час, як традиційні методи вирішення міжнародних суперечок, такі як дипломатія і переговори, залишаються важливими, нові технології вимагають від держав і міжнародних організацій постійної готовності реагувати на нові виклики» [11].

Цей процес не лише змінює саму природу конфліктів, але й вимагає від держав гнучкості, стратегічного мислення та здатності адаптуватися до умов постійно змінюваного цифрового середовища, яке визначає правила гри в глобальній політиці.

Поступово нові форми конфліктів виходять за рамки лише кібер- або інформаційних війн, стаючи частиною більш широких і складних геополітичних процесів. З технологічною еволюцією виникають нові глобальні і локальні загрози, пов’язані з екологічними змінами, такими як зміни клімату, і їхнім впливом на міжнародні відносини.

В останні десятиліття проблема зміни клімату стала не лише питанням екологічної безпеки, але й новим полем для міжнародної конкуренції та конфліктів. Технології, що допомагають досліджувати та контролювати екологічні зміни, стають важливим інструментом в геополітичних і економічних суперечках. Наприклад, країни, що мають доступ до передових технологій у сфері відновлюваних джерел енергії чи водних ресурсів, отримують конкурентну перевагу в умовах глобальних змін клімату [23].

В умовах глобальної екологічної кризи виникають нові економічні і соціальні розподіли ресурсів, що можуть стати основою для екологічних конфліктів. Наприклад, боротьба за доступ до водних ресурсів може призвести до міждержавних суперечок, а також до конфліктів між різними соціальними групами, які будуть мати різний рівень доступу до таких ресурсів.

Це створює додаткові виклики для міжнародних організацій, які повинні не лише вирішувати проблеми, пов'язані з технологіями та кібербезпекою, але й координувати міжнародні зусилля для боротьби з новими, більш комплексними глобальними загрозами [12].

Важливою складовою цієї еволюції конфліктів стає також перерозподіл глобальних сил, який відбувається внаслідок технічних досягнень і їх впливу на національні інтереси. З розвитком нових технологій, таких як штучний інтелект і квантові обчислення, країни отримують можливість контролювати і використовувати інформацію та ресурси таким чином, щоб зміцнити своє економічне становище на міжнародній арені.

Країни, що опиняються позаду у технологічному розвитку, можуть відчувати збільшення економічної та політичної залежності від більш розвинених держав, що в свою чергу призводить до нових форм нерівності на глобальному рівні.

«Це, в свою чергу, може стати причиною нового роду політичних і економічних суперечок, де інноваційні технології та їх доступність стають основним ресурсом для стратегічного впливу» [22].

Такі зміни у глобальній політиці визначають необхідність створення нових міжнародних механізмів співпраці та регулювання. У зв'язку з цим, міжнародні організації та держави повинні формувати нові стратегії для управління не лише

класичними геополітичними конфліктами, а й тими, що виникають на тлі технологічних трансформацій і екологічних змін.

Такий підхід дозволяє не тільки знижувати ризики виникнення конфліктів, але й ефективніше управляти існуючими суперечностями в міжнародних відносинах, сприяючи розвитку більш збалансованої і стабільної глобальної політики.

РОЗДІЛ 3. Політичні аспекти кібербезпеки на глобальному рівні

Політичні аспекти кібербезпеки на глобальному рівні становлять важливий елемент міжнародних відносин, оскільки кіберпростір дедалі більше впливає на геополітичну ситуацію. Кожна країна має свою стратегію кібербезпеки, що залежить від її технологічного розвитку, політичних інтересів, рівня загроз і зовнішньої політики. Кібербезпека стає не лише питанням національного захисту, але й ключовим елементом міжнародних відносин, де взаємодія між державами визначається здатністю ефективно протидіяти кібератакам, здійснювати кібердипломатію та забезпечувати безпеку глобальних цифрових інфраструктур.

На глобальному рівні кібербезпека стає предметом все більшої політичної уваги. Держави створюють міжнародні механізми для боротьби з кіберзагрозами, намагаючись виробити загальні правила гри у кіберпросторі. Однак цей процес ускладнюється через відсутність єдиного міжнародного правового регулювання в галузі кібербезпеки, що дає можливість різним державам застосовувати різні підходи до цього питання [13].

У більшості випадків країни намагаються формувати національні стратегії кібербезпеки, які, з одного боку, враховують їхні внутрішні потреби, а з іншого - мають на меті забезпечити участь у глобальних ініціативах, спрямованих на боротьбу з кіберзлочинністю та кібератаками.

Кібербезпека має важливе значення в контексті міжнародних відносин через здатність держав впливати на інші країни, застосовуючи технології для дипломатичного тиску, стратегічних маніпуляцій або навіть саботажу. Кібератаки можуть бути використані для зміни політичного курсу держави, а також для підриву довіри до її урядів, що робить кіберзагрози не тільки технічними, але й політичними [21].

Наприклад, в останні роки спостерігається використання кіберзагроз як частини гібридних війн, де країни застосовують інформаційні атаки для впливу на політичні процеси в інших державах. Кіберінциденти можуть призвести до дипломатичних скандалів або навіть до серйозних політичних криз.

З іншого боку, зростаючі загрози у кіберпросторі сприяють розвитку міжнародної співпраці в цій сфері. Міжнародні організації, такі як ООН, ЄС, НАТО, а також національні уряди активно працюють над створенням загальних стандартів і принципів для забезпечення кібербезпеки.

Це включає в себе розробку протоколів для захисту критичної інфраструктури, боротьби з кіберзлочинністю, обміну інформацією про кіберзагрози та забезпечення безпеки даних. На цьому етапі важливою є також роль великих міжнародних корпорацій, які контролюють основні технології і мають вплив на формування політики в сфері кібербезпеки [14].

Водночас політичні аспекти кібербезпеки не обмежуються лише питанням міжнародної співпраці. Вони включають також внутрішньополітичні аспекти, зокрема управління кіберзахистом на національному рівні, захист приватності громадян і балансування між національною безпекою та правами людини.

«Країни прагнуть уникати надмірного втручання в особисте життя своїх громадян, при цьому не знижуючи ефективність кіберзахисту. Це викликає численні дебати щодо встановлення лінії між забезпеченням безпеки і дотриманням фундаментальних прав людини в умовах зростаючого використання цифрових технологій для спостереження та контролю» [21].

З огляду на це, політичні аспекти кібербезпеки на глобальному рівні стають все більш комплексними, зокрема через те, що новітні технології створюють нові можливості для державного та недержавного впливу в кіберпросторі. Відповідно, держави зобов’язані активно співпрацювати для вироблення ефективних заходів,

спрямованих на захист від кіберзагроз, одночасно вирішуючи важливі питання щодо прав людини, економічної безпеки та цифрового суверенітету [16].

У процесі розвитку політичних аспектів кібербезпеки на глобальному рівні виникає також важливе питання цифрового суверенітету, яке набуває дедалі більшого значення в контексті міжнародних відносин. Кожна країна прагне мати контроль над своїми цифровими інфраструктурами, даними та інформаційними потоками, що стає важливим аспектом національної безпеки. Зростаючий вплив міжнародних технологічних корпорацій та їхній контроль над глобальними цифровими мережами ставлять під сумнів здатність окремих країн ефективно захищати свої інтереси в кіберпросторі [19].

В таких умовах виникає потреба в тому, щоб на міжнародному рівні був знайдений баланс між відкритістю глобальної інформаційної мережі та захистом суверенітету держав. Цифровий суверенітет стає важливою частиною геополітичної стратегії, де країни намагаються створювати власні інфраструктури для обробки даних і захисту критичних інформаційних систем від зовнішнього втручання.

Цей процес вимагає нових підходів до регулювання цифрових технологій та міжнародних угод в цій сфері, що визначаються не лише політичними, а й економічними та юридичними факторами. Країни з високим рівнем технологічного розвитку мають змогу розробляти власні механізми для контролю кіберпростору, але на міжнародній арені ці розбіжності можуть спричиняти суперечки та конфлікти [17].

Наприклад, деякі держави виступають за введення нових законів, які обмежують доступ іноземних компаній до внутрішніх ринків, щоб запобігти загрозам для національної безпеки, в той час як інші країни підтримують більш відкриту модель обміну даними та інформацією.

Іншою важливою тенденцією є перехід від традиційної дипломатії до кібердипломатії, яка передбачає використання новітніх технологій для формування міжнародних відносин і вирішення конфліктів у кіберпросторі. Держави все частіше починають використовувати онлайн-ресурси для проведення переговорів, врегулювання суперечок або навіть для захисту своїх інтересів через кіберзасоби, такі як вплив на вибори або маніпуляція громадською думкою в інших країнах. Це стає новим методом ведення зовнішньої політики, де традиційні канали дипломатії поступаються місцем більш швидким і ефективним цифровим платформам [18].

Цифрові технології також змінюють підхід до міжнародних криз, оскільки здатність швидко поширювати інформацію і реагувати на глобальні загрози може значно прискорити або, навпаки, ускладнити дипломатичні процеси. Наприклад, цифрові платформи можуть бути як інструментами для мирного врегулювання конфліктів, так і для їх ескалації, коли дезінформація або кіберзлочинність використовуються для розпалювання напруги між країнами.

Такий динамічний розвиток цифрової дипломатії змушує держави переглядати свої політики у сфері кібербезпеки, сприяючи більш тісній співпраці на глобальному рівні, водночас підвищуючи потребу в міжнародних стандартах кібербезпеки [7].

Таким чином, політичні аспекти кібербезпеки не обмежуються лише захистом від зовнішніх загроз. Вони також включають питання національного контролю, глобальної співпраці і нових технологічних стратегій, які визначають сучасний міжнародний ландшафт. Країни, які прагнуть досягти переваги в цьому новому середовищі, повинні не лише адаптувати свої інфраструктури до сучасних загроз, але й ефективно взаємодіяти з іншими державами, щоб забезпечити безпеку та стабільність на глобальному рівні.

ВИСНОВКИ

Аналіз політичних аспектів кібербезпеки на глобальному рівні показує, наскільки важливою є роль кіберпростору в сучасному світі, який швидко змінюється під впливом технологічних інновацій та нових глобальних викликів. Сучасна кібербезпека вже давно вийшла за межі традиційного захисту від кіберзагроз і стала складною складовою міжнародних відносин, що включає в себе економічні, соціальні та політичні аспекти.

У світі, де технології стали основним інструментом впливу на держави, економіку і громадян, питання кібербезпеки стали обов’язковим для кожної країни, яка прагне захистити свої національні інтереси.

Кібербезпека є важливою частиною національної безпеки та стратегії розвитку будь-якої держави. Залежно від рівня технологічного розвитку, політичних та економічних умов кожна країна розробляє свою стратегію кібербезпеки, яка відповідає її особливим потребам. Технологічні досягнення дозволяють країнам створювати національні кіберзахисні стратегії, але одночасно вони також повинні взаємодіяти на глобальному рівні через міжнародні організації та формувати правила для забезпечення загальної кібербезпеки.

Однак, розбіжності в підходах до цього питання, а також відсутність єдиного глобального правового поля щодо кіберзагроз часто призводять до конфліктів і суперечок серед держав, що ще більше ускладнює процес вирішення цієї проблеми на міжнародному рівні.

Однією з ключових тем у контексті кібербезпеки є концепція цифрового суверенітету. З розвитком інформаційних технологій і зростаючою залежністю від цифрових інфраструктур країни почали приділяти більше уваги тому, як забезпечити контроль над своїми цифровими ресурсами. Це стало необхідністю

для підтримки національної безпеки, економічної стабільності та політичного суверенітету. Країни прагнуть не тільки захистити свої інформаційні системи від зовнішніх кіберзагроз, а й мати змогу контролювати потоки даних та інформації, що рухаються через їхні території.

Водночас зростаюче значення технологій і платформ, що контролюються міжнародними корпораціями, підриває суверенітет держав у кіберпросторі, що створює нові виклики для політики в цій сфері.

Не менш важливим аспектом є роль міжнародних організацій у розвитку стандартів і норм кібербезпеки. Оскільки кіберзагрози не мають кордонів, то жодна країна не може ефективно протистояти їм у поодинці. Тому на міжнародному рівні необхідна ефективна співпраця держав, розробка загальних принципів та механізмів для реагування на кіберзагрози.

Однак, через різні підходи до визначення кіберзагроз і різну політичну ситуацію в окремих країнах, досягнення єдиного консенсусу в питаннях кібербезпеки є дуже складним завданням. Проблеми, що виникають у результаті міжнародних кіберінцидентів, часто потребують складних політичних і юридичних рішень, які вимагають більшої співпраці та розробки міжнародних стандартів.

Зокрема, важливими є механізми кібердипломатії, які дозволяють державам вести переговори і вирішувати суперечності в кіберпросторі. Кібердипломатія стає важливим інструментом у вирішенні міжнародних конфліктів, адже вона дає змогу державам впливати на один одного через цифрові технології, без використання традиційних методів військової чи економічної сили.

За допомогою цифрових платформ країни можуть обмінюватися інформацією про кіберзагрози, координувати спільні дії щодо боротьби з

кіберзлочинністю, а також розвивати правила і норми для кіберпростору. Однак, кібердипломатія також стикається з низкою проблем, таких як відсутність єдиних стандартів, нерівність технологічного розвитку між країнами та політичні розбіжності в питаннях кібербезпеки.

Іншою важливою темою є розвиток нових форм конфліктів у міжнародних відносинах, що виникають через кіберзагрози. Кіберконфлікти стають новим методом впливу на держави і суспільства, оскільки можливість втручання в цифрові інфраструктури дозволяє здійснювати різноманітні види маніпуляцій. Це можуть бути атаки на критичні інфраструктури, втручання в вибори, підрив довіри до урядів, або дезінформаційні кампанії.

Ці нові методи ведення конфліктів змінюють характер традиційних воєн і міжнародних суперечок, додаючи нові складнощі в дипломатичні процеси. Вони також створюють нові виклики для національних систем безпеки, оскільки країни змушені впроваджувати нові стратегії для захисту своїх кіберінфраструктур від подібних атак.

Нарешті, політичні аспекти кібербезпеки на глобальному рівні також пов’язані з проблемами прав людини та економічної безпеки. Країни повинні знаходити баланс між забезпеченням національної безпеки в кіберпросторі та захистом прав своїх громадян. В умовах глобальної цифрової інтеграції важливо забезпечити конфіденційність і свободу особистості, одночасно захищаючи державу від кіберзагроз. Це особливо важливо в країнах, де технології спостереження використовуються для контролю за громадянами, що може створити небезпеку для демократії та політичних прав.

У підсумку, політичні аспекти кібербезпеки на глобальному рівні стають одним із найважливіших факторів у сучасних міжнародних відносинах. Вони охоплюють не лише технологічні та економічні питання, але й політичні,

юридичні та соціальні виклики, що виникають через нові цифрові загрози. Кібербезпека не є просто питанням захисту від атак, а є складною та багатогранною проблемою, що вимагає комплексного підходу на рівні держав, міжнародних організацій і корпорацій. Тому важливо, щоб країни продовжували розвивати свої стратегії кібербезпеки, одночасно забезпечуючи міжнародну співпрацю та дотримуючись принципів відкритості та безпеки у цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк В. Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. Державне управління: удосконалення та розвиток. 2021. № 7. С. 24-56

2. Боднар І. Інформаційна безпека як основа безпеки. Механізм регулювання економіки. 2019. №1. С. 68–78

3. Боднар І. Р. Роль держави у формуванні інформаційної політики. Вісник ЛКА. 2021. Вип. 34. С. 291–296.

4. Бондаренко В. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: http://www.crime-research.iatp.org.ua/library/strateg.htm.

5. Брусиловська О. та ін. Міжнародні відносини та зовнішня політика в еру «пост-правди»: монографія. 2024. Київ: Вадекс. 368 с.

6. Глобальні тренди міжнародних відносин. Монографія. Київ: Вадекс, 2020. 217 с.

7. Гончарук-Чолач Т. В., Лазарович М. В., Джугла Н. В. Цифрова революція в політиці та її вплив на постінформаційне суспільство. Актуальні проблеми філософії та соціології. 2025. Вип. 52. С. 38-49

8. Гончарук-Чолач Т. В., Лазарович М. В., Докаш О. Ю. Штучний інтелект в політичних маніпуляціях та трансформація виборчої культури. Політикус. 2025. № 1. С. 57-71

9. Гончарук-Чолач Т. В., Джугла Н. В., Чигур Р. Ю. Аналітичний екскурс в методичні теорії демократії. Науковий огляд. № 1 (64). 2020. С. 10-20

10. Гурковський В. І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2020. № 2(26). С. 72–77.

11. Ждамарова А.В. Зовнішня політика сучасної держави: основні підходи до визначення поняття. Науковий вісник Ужгородського національного університету, Вип. 6. 2023. С. 72-78.

12. Закіров М. Сучасні інформаційно-комунікаційні технології як фактор еволюції соціально-політичних відносин. Наукові праці Національної бібліотеки України. 2023. Вип.46. С. 11-24.

13. Запорожець Т. Цифрова платформа інтелектуального управління у безпековій сфері. Цифрове врядування : монографія. Нац. акад. держ. упр. при Президентові України. Київ : ІДЕЯ ПРИНТ, 2020. С. 267-280

14. Захаренко К. В. Міжнародний досвід інформаційної безпеки. Сучасне суспільство: політичні науки, соціологічні, культурологічні науки. 2023. Вип. 1 (17). С. 95–109.

15. Захаренко К. В. Теоретичні засади дослідження інформаційної безпеки. Міжнародні відносини, суспільні комунікації та регіональні студії. 2022. № 2 (4). С. 107–116.

16. Карпчук Н. Міжнародна інформація та суспільні комунікації: навч. посіб. Для туд. закл. вищ. освіти. Луцьк. URL: https://evnuir.vnu.edu.ua/handle/123456789/14600

177. Кібербезпека в інформаційному суспільстві. Інформаційно-аналітичний дайджест. 2024. URL: https://ippi.org.ua/sites/default/files/2023-9.pd

18. Коваленко О. Теоретико-методологічні засади формування механізмів забезпечення кібербезпеки України на сучасному етапі державного будівництва. Věda a perspektivy. 2023. №6 (13). С. 21–23

19. Піпченко Н., Рижков М. Публічна дипломатія ЄС. «Принциповий прагматизм» ЄС – наслідки для Східної та Південно-Східної Європи» 2021 рік: матеріали міжнар.наук.-практ. конф., 21-22 травня. 2021 р. Київ: КНУ. С. 58-67

20. Пшетачник Я. Війна Росії проти України: хронологія кібератак. Дослідницька служба Європейського парламенту. European Parliament. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf

21. Сунь-цзи. Мистецтво війни. Пер. Г. Латник. Київ: Арій, 2014. С. 8–11

22. Усатюк К. Р. Сучасні інформаційні технології в міжнародних відносинах та зовнішній політиці держав. Соціально-політичні студії. Науковий альманах. Праці молодих науковців. 2024. Вип. 5. С. 146-153

23. Ченбай Н. Трансформації ідентичності в умовах інформаційно-технологічної революції (соціокультурний аспект). Вісник Національного авіаційного університету. Серія: Філософія. Культурологія. 2024. Вип. 2. С. 95-100

24. Шлапаченко В. М. Дезінформація як спосіб інформаційно-психологічного впливу. Інформаційна безпека людини, суспільства, держави. 2021. №2. С. 78–86.

25. Eldem T. International Cybersecurity Norms and Responsible Cyber Sovereignty. Istanbul hukuk mecmuasi. 2023. Vol. 79 (1). P. 347–378.

26. Kasper A., Osula A., Molnar A. EU cybersecurity and cyber diplomacy. IDP-internet law and politics. 2024. №34. P. 1–15. URL: https://raco.cat/index.php/IDP/article/ view/n34-kasper/487930

27. Kaufmann M., Jeandesboz J. Politics and ‘the digital’: From singularity to specificity. European Journal of Social Theory. 2024. №20 (3). С. 309–328.

28. Kaufmann M., Jeandesboz J. Politics and ‘the digital’: From singularity to specificity. European Journal of Social Theory. 2024. №20. P. 309–328

29. Makedon V., Drobyazko S., Shevtsova H., Maslosh O., Kasatkina M. Providing security for the development of high-technology organizations, Journal of Security and Sustainability Issues. 2023. № 8(4). P. 1313-1331

30. Measuring the Information Society Report 2024. International Telecommunication Union (ITU). URL: https://www.itu.int/en/ITUD/Statistics/ Documents/publications/misr2024/MIS R2018-Vol-2-E.pdf

31. Report on Information Technology (IT) 2024: Global Market Analysis from 2014 and Forecast to 2024. URL: https://www.businesswire.com/news/home/ 20190925005479/en/2024

32. U.S. Department of State Information Technology Tactical Plan (ITTP). Fiscal Years 2021–2024. Strategic planning office, 37. URL: https://2021-2024.state.gov/m/irm/ rls/c47770.htm