

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»**

**ФАКУЛЬТЕТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ, ПРАВА ТА
МІЖНАРОДНИХ ВІДНОСИН**

**КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН І ПОЛІТИЧНОГО
МЕНЕДЖМЕНТУ**

САМОЙЛЕНКО Тетяна Олександрівна
(студентка групи МВ-1)

КВАЛІФІКАЦІЙНА РОБОТА

**КІБЕРБЕЗПЕКА ЯК НОВИЙ ВИМІР МІЖНАРОДНИХ ВІДНОСИН ТА
ДИПЛОМАТІЇ**

(представлена на здобуття ступеня вищої освіти «бакалавр»
галузі знань 29 «Міжнародні відносини» спеціальності
291 «Міжнародні відносини, суспільні комунікації та регіональні студії»)

Допущено до захисту
протокол № _____
від _____
в. о. зав. кафедри міжнародних відносин
і політичного менеджменту
д.е.н., доц.
Ірина ГРАБЧУК

Керівник роботи:
PhD Олена ВОЙТЮК

(підпис)

Рецензент
к.філос.н., доц.
Оксана ЛИТВИНЧУК

(підпис)

Я, Самойленко Тетяна Олександрівна, цим засвідчую, що представлена до захисту кваліфікаційна робота виконана на основі власних наукових досліджень. Текст не містить доробку інших дослідників без відповідних посилань на їх праці.

Я попереджена про те, що буду недопущена до захисту, а в разі отримання диплому – буду позбавлена його відповідно до чинного законодавства України.

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1. КІБЕРБЕЗПЕКА ЯК НОВИЙ ВИМІР МІЖНАРОДНИХ ВІДНОСИН.....	7
1.1. Концептуальні основи кібербезпеки.....	7
1.2. Міжнародне співробітництво у сфері кібербезпеки.....	17
РОЗДІЛ 2. КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ДИПЛОМАТІЇ.....	27
2.1. Вплив глобальних викликів на дипломатію у галузі кібербезпеки.....	27
2.2. Кібердипломатія як нова форма співпраці у світі.....	33
РОЗДІЛ 3. КІБЕРБЕЗПЕКА УКРАЇНИ В КОНТЕКСТІ МІЖНАРОДНИХ ВІДНОСИН ТА ДИПЛОМАТІЇ.....	43
3.1. Сучасна політика України у галузі кібердипломатії.....	43
3.2. Міжнародне співробітництво України у сфері кібербезпеки.....	48
ВИСНОВКИ.....	57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ	59

ВСТУП

Актуальність теми. Стрімкий розвиток інформаційно-комунікаційних технологій (ІКТ) у ХХІ столітті докорінно змінив характер комунікації, економічної діяльності, державного управління та міжнародної взаємодії. Виникнення і стрімке розширення кіберпростору створило новий глобальний вимір, у якому взаємодіють не лише приватні особи та компанії, а й цілі держави та міждержавні об'єднання. Кіберпростір став невід'ємною складовою сучасного світу, що забезпечує функціонування критичної інфраструктури, фінансових систем, засобів масової інформації, органів влади та багатьох інших сфер життєдіяльності суспільства.

З одного боку, кіберпростір відкриває низку можливостей для економічного зростання, науково-технічного прогресу, культурного обміну та розвитку міжнародної співпраці. Завдяки інтеграції ІКТ країни можуть швидше впроваджувати інновації, брати участь у глобальних економічних процесах, обмінюватися знаннями й досвідом. Водночас, з іншого боку, цей простір став ареною для виникнення нових, часто невидимих та складних для ідентифікації загроз. Кіберзагрози, серед яких атаки на критичну інфраструктуру, розповсюдження шкідливого програмного забезпечення, злам державних і комерційних систем, кібершпигунство та кібертеракти, можуть призводити до значних економічних збитків, дестабілізації політичних систем, порушення функціонування державних інституцій і навіть підриву національної безпеки.

Світова спільнота дедалі гостріше усвідомлює, що кібербезпека вже давно вийшла за межі суто технічної чи національної проблематики. Сучасні кіберзагрози мають транснаціональний характер, а їхні наслідки можуть впливати на регіональну та глобальну стабільність. Зокрема, останніми роками все більше фіксується випадків міжнародних кібератак, спрямованих на втручання у виборчі процеси, маніпуляцію інформаційним простором, дестабілізацію суспільств та економік. Такі інциденти підкреслюють неможливість ефективної протидії

кіберзагрозам лише на рівні окремої держави, а потребують скоординованих міжнародних зусиль, вироблення спільних стандартів та механізмів співпраці.

У цьому контексті питання кібербезпеки набуває особливої актуальності у сфері міжнародних відносин та дипломатії. Кібербезпека стає ключовим елементом національної безпеки, важливим чинником формування зовнішньополітичних стратегій, а також предметом переговорів, міждержавних угод, діяльності міжнародних організацій. Від ефективності дипломатичних зусиль, спрямованих на врегулювання кіберконфліктів, забезпечення довіри та прозорості у кіберпросторі, залежить не лише безпека окремих країн, а й стабільність міжнародної системи загалом.

Актуальність дослідження цієї теми обумовлена необхідністю глибшого розуміння нових викликів, що постають перед міжнародною спільнотою у зв'язку з кіберзагрозами, а також пошуку ефективних шляхів інтеграції кібербезпеки у практику міжнародних відносин та дипломатії. Безпечний кіберпростір є однією з основних умов сталого розвитку сучасного суспільства, захисту національних інтересів та підтримки глобальної стабільності. Саме тому аналіз ролі кібербезпеки як нового виміру у міжнародних відносинах і дипломатії є надзвичайно важливим і своєчасним у сучасних реаліях.

Метою роботи є дослідження кібербезпеки як нового виміру міжнародних відносин та дипломатії в Україні та світі.

Для реалізації мети поставлено такі **завдання**:

- описати концептуальні основи кібербезпеки;
- розглянути міжнародне співробітництво у сфері кібербезпеки;
- проаналізувати вплив глобальних викликів на дипломатію в галузі кібербезпеки;
- охарактеризувати кібердипломатію як нову форму співпраці у світі;
- дослідити сучасну політику України у галузі кібердипломатії;
- з'ясувати основні принципи міжнародного співробітництва України у сфері кібербезпеки.

Об'єктом дослідження є міжнародні відносини в умовах цифрової трансформації.

Предметом дослідження є механізми та стратегії кібербезпеки в системі міжнародних відносин і дипломатії.

Методологія дослідження. У роботі застосовано загальнонаукові та спеціальні методи дослідження, зокрема узагальнення, аналіз та синтез, історичний та графічний метод.

Наукова новизна дослідження полягає у виявленні нових закономірностей впливу глобальних викликів на дипломатію у галузі кібербезпеки в контексті розвитку сучасних міжнародних відносин.

Апробація результатів роботи. Результати, які зазначено в кваліфікаційній роботі, були представлені тезами доповідей на Всеукраїнській науково-практичній конференції «Держава XXI століття: погляд молоді» (присвячена Дню науки) (м. Житомир, 20 травня 2025 року) за темою: «Дипломатія в контексті сучасних викликів у сфері кібербезпеки».

Структура та обсяг роботи зумовлені метою та завданнями дослідження. Робота складається зі вступу, трьох розділів, висновків, а також списку використаних джерел. Загальний обсяг роботи становить 68 сторінок. Список використаних літературних джерел налічує 74 найменування.

РОЗДІЛ 1

КІБЕРБЕЗПЕКА ЯК ФАКТОР МІЖНАРОДНИХ ВІДНОСИН

1.1. Концептуальні основи кібербезпеки

Науково-технічна революція (НТР), що розгорнулася у другій половині ХХ століття, стала каталізатором безпрецедентних змін у всіх сферах людського життя. Одним із найважливіших її наслідків був стрімкий розвиток комп'ютерних технологій, які, у свою чергу, започаткували нову епоху в історії цивілізації. Основою цього технічного прориву стало створення принципово нових засобів обробки, зберігання та передачі інформації. Комп'ютери, які спочатку сприймалися лише як інструмент для обчислень, з часом перетворилися на універсальні пристрої, що забезпечують обробку величезних обсягів даних у реальному часі.

Особливої важливості набув розвиток глобальної мережі Інтернет, який об'єднав мільйони комп'ютерів по всьому світу, дозволивши людям обмінюватися інформацією, спілкуватися та співпрацювати незалежно від географічного розташування. Інтернет став не просто технологічним досягненням, а соціальним явищем, яке вплинуло на всі аспекти сучасного суспільства: економіку, політику, освіту, культуру та навіть особисті стосунки.

Поява Інтернету спричинила формування нового середовища для взаємодії між різними акторами міжнародних відносин — державами, транснаціональними корпораціями, громадськими організаціями, а також окремими особистостями. Цей новий простір отримав назву віртуального, або кіберпростору, який відкрив принципово нові можливості для комунікації, ведення бізнесу, обміну знаннями та організації соціальних рухів. У кіберпросторі кордони між країнами стають умовними, а інформація поширюється миттєво, що створює абсолютно нові виклики та загрози, зокрема у сфері безпеки, конфіденційності та захисту прав людини.

Термін «кіберпростір» вперше був використаний американським письменником-фантастом Вільямом Гібсоном у 1982 році у його новелі «Burning Chrome». Однак лише у 1990-х роках, із масовим розповсюдженням Інтернету та персональних комп'ютерів, поняття «кіберпростір» стало офіційно вживатися у наукових, політичних та публіцистичних колах для позначення нового виміру людської діяльності.

Кіберпростір визначається як «взаємозалежна мережа інформаційно-технологічних інфраструктур, що включає Інтернет, телекомунікаційні мережі, комп'ютери, інформаційні системи, промислові системи управління, мережі та вбудовані процесори і контролери» [37, с. 67]. Хоча його поява й надала низку можливостей, не слід забувати й про загрози. Кіберзагрози можуть мати різноманітний характер і впливати на різні сфери як людського життя, так і функціонування держави.

Поява кіберзагроз змусила переосмислити поняття національної та міжнародної безпеки. Нові загрози кардинально відрізняються від традиційних, але завдають все такої ж, а часом навіть більшої, шкоди. Зазвичай, джерелами кібернетичних загроз є:

1. Зловмисники, які працюють на замовлення уряду;
2. Злочинні угруповання, які здійснюють атаки з метою заробітку;
3. Хакери;
4. Терористичні організації.

До загроз, які вони несуть, можна віднести такі:

1. Шкідливе програмне забезпечення (віруси, хробаки, шпигунські програми тощо). Це програмне забезпечення, створене з метою завдання шкоди, отримання несанкціонованого доступу або викрадення інформації. Воно включає віруси, черв'яки, трояни, шпигунські програми та інші небезпечні програми;
2. Фішинг. Це метод шахрайства, який полягає в обмані користувачів з метою отримання конфіденційної інформації, такої як паролі, номери кредитних карток чи особисті дані. Зазвичай фішинг реалізується через електронну пошту або підроблені веб-сайти, що імітують легітимні сервіси;

3. Програми-вимагачі. Це вид шкідливого програмного забезпечення, яке блокує доступ до системи або шифрує файли жертви, вимагаючи викуп для відновлення доступу. Зазвичай зловмисники просять оплату в криптовалюті, щоб ускладнити відстеження транзакцій;

4. Загрози для ідентичності. Це ризики, пов'язані з викраденням або зловживанням особистими даними особи. Це може включати крадіжку ідентичності, де зловмисники використовують чужі дані для отримання кредитів, відкриття рахунків або виконання шахрайських дій. Такі загрози часто виникають через фішинг, злами або витоки даних;

5. Порухення безпеки корпоративної електронної пошти. Це несанкціонований доступ до електронних поштових скриньок співробітників компанії, що може призвести до витоку конфіденційної інформації. Такі порушення можуть відбуватися через фішинг, зловмисне програмне забезпечення або слабкі паролі, і можуть мати серйозні наслідки для організації, включаючи фінансові втрати та репутаційні ризики;

6. Атаки типу «відмова в обслуговуванні (DoS-атаки) та розподілені атаки на відмову в обслуговуванні (DDoS-атаки). Атака типу «відмова в обслуговуванні» (DoS-атака) – це спроба зробити комп'ютерну систему або мережу недоступною для користувачів, зазвичай шляхом перевантаження її запитами. Розподілена атака на відмову в обслуговуванні (DDoS-атака) – це форма DoS-атаки, яка використовує кілька скомпрометованих комп'ютерів або пристроїв для одночасного нападу на ціль, що робить її більш потужною та важчою для відбиття. Обидва типи атак можуть спричинити серйозні збої в роботі сервісів і сайтів;

7. Удосконалені постійні загрози (APT). Це складні, цілеспрямовані атаки, зазвичай здійснювані організованими групами з високим рівнем технічних знань. АРТ намагаються отримати тривалий доступ до системи або мережі, часто з метою шпигунства або крадіжки чутливої інформації. Ці атаки можуть бути важкими для виявлення і вимагають комплексних заходів безпеки для їх запобігання та виявлення;

8. Внутрішні загрози. Це ризики, які походять зсередини організації, зазвичай від її співробітників або підрядників. Ці загрози можуть бути навмисними або ненавмисними. Внутрішні загрози можуть призвести до витоків конфіденційної інформації, фінансових втрат або шкоди репутації. Управління такими загрозами вимагає політик безпеки та навчання персоналу [27].

Слід зазначити, що кібератаки стали одним з основних причин зростання кількості викликів у сучасному кіберпросторі. З розвитком цифрового суспільства та впровадженням новітніх технологій постійно зростає масштаб і частота кіберінцидентів, що створює серйозні загрози для безпеки як окремих користувачів, так і цілих організацій та держави. До основних викликів, які пропонуються у сфері кібербезпеки, можна віднести декілька ключових аспектів, як от: зростання складності кібератак; людський фактор; швидкий розвиток технологій; треті сторони та брак кваліфікованих фахівців з кібербезпеки. Їхній зміст висвітлено у табл. 1.1.

Таблиця 1.1

Виклики у сфері кібербезпеки

№	Виклики	Зміст
1	Зростання складності кібератак	Останнім часом зростає складність кібератак, а також методи їх здійснення, як-от АТР, завдяки чому зловмисники довше можуть залишатися непоміченими. Сучасні загрози вже не обмежуються лише програмами-вимагачами, які шифрують файли; тепер вони також погрожують витоком конфіденційних даних. Це створює серйозні проблеми для бізнесу, оскільки навіть сплата викупу не гарантує повернення даних. Такі кампанії часто є етапними, використовуючи початкову інформацію для подальших, більш серйозних атак.
2	Людський фактор	Людський фактор є основною причиною порушень кібербезпеки, оскільки співробітники часто стають найслабшою ланкою в захисті організації. Поширені помилки, такі як використання слабких паролів і піддавання фішингу, залишають організації вразливими. Незважаючи на інформаційні кампанії, фішинг залишається ефективним методом для кіберзлочинців. Крім того, випадкове викриття даних трапляється, коли співробітники ненавмисно розголошують конфіденційну інформацію через неналежні канали, такі як особисті електронні пошти або незахищені хмарні сервіси.

Продовження табл. 1.1

№	Виклики	Зміст
3	Швидкий розвиток технологій	Нові технології, хоча й підвищують ефективність і інноваційність, також створюють нові вразливості для кіберзлочинців. Наприклад, Інтернет речей (IoT) розширює можливі точки атаки через підключення безлічі пристроїв, які часто не мають належної безпеки. Швидке впровадження хмарних обчислень також приносить переваги, але викликає проблеми безпеки, такі як публічно відкриті сховища, що можуть призводити до витоку конфіденційної інформації.
4	Треті сторони	Останнім часом зростають ризики для кібербезпеки через залучення сторонніх постачальників і партнерів у бізнес-процеси. Хоча ці відносини важливі для функціонування компанії, вони можуть стати вразливими, якщо постачальники не дотримуються належних стандартів безпеки. Один злам у системі стороннього постачальника може викликати каскадний ефект, впливаючи на весь ланцюг поставок. Більшість організацій не мають можливостей для ефективного моніторингу безпеки своїх постачальників, що посилює ризик витоку даних і перебоїв у наданні послуг.
5	Брак кваліфікованих фахівців у сфері кібербезпеки	Зі збільшенням частоти та складності кіберзагроз попит на таких фахівців ніколи не був настільки високим, але пропозиція не відповідає потребам. Це створює труднощі для організацій у виявленні, реагуванні та пом'якшенні атак, оскільки вони не можуть ефективно використовувати необхідні інструменти та стратегії безпеки через брак відповідних кадрів.

Джерело: [68]

Останніми роками кількість і масштаб кіберзагроз стає все більшою. Згідно з даними Європейського репозиторію кіберінцидентів (рис. 1), в період з 1 січня 2000 р. до 31 грудня 2024 р. було зафіксовано 3389 кіберзагроз, і з них половина, 1838 загроз, – лише за останні 3 роки [44].

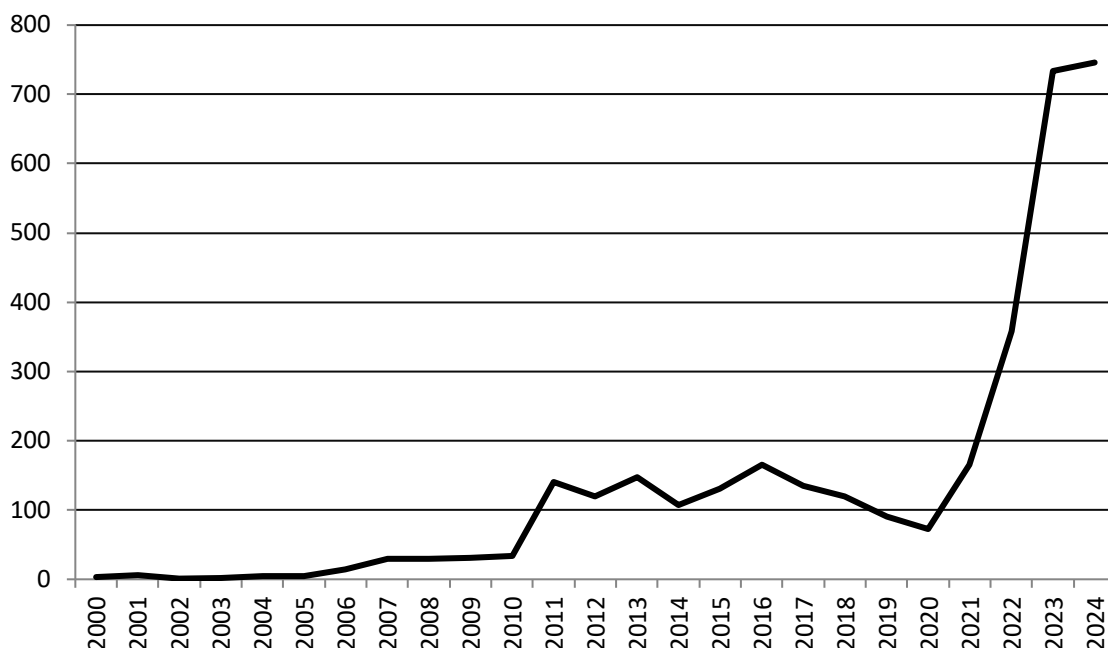


Рис. 1.1. Кількість кіберінцидентів в період з 1 січня 2000 р. до 31 грудня 2024 р.

Ці дані показують, що кіберзагрози є серйозною проблемою для кожної з країн. У зв'язку з цим, питання кібербезпеки стало надзвичайно актуальним.

Слід зазначити, що поняття «кібербезпека» є відносно новим. Вважається, що даний термін виник в 1990-х рр. у США, хоча сама концепція почала виникати ще в 70-х рр. XX ст. З огляду на це, єдиного чіткого визначення поки ще немає, а тому його розуміють і трактують по-різному. Наприклад, якщо розглядати кібербезпеку з точки зору національного законодавства України, Законом «Про основні засади забезпечення кібербезпеки України» вона визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [17]. Тобто, як ми можемо бачити, національне законодавство розглядає кібербезпеку лише з точки зору безпеки держави та її громадян.

Якщо розглядати визначення, яке пропонує Міжнародний союз електрозв'язку (МСЕ), то кібербезпека розглядається як сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можуть бути використані для захисту кіберсередовища та активів організацій і користувачів [57, с. 1]. Дане визначення є більш широким, і акцентує увагу на способах забезпечення кібербезпеки.

Національний інститут стандартів і технології (NIST) США пропонує таке визначення терміну кібербезпека – це запобігання пошкодженню, захист та відновлення комп'ютерів, електронно-обчислювальних машин, систем електронних комунікацій, послуг електронних комунікацій, проводового зв'язку та електронних комунікацій, у тому числі інформації, що міститься в них, з метою забезпечення її доступності, цілісності, автентичності, конфіденційності та неспростовності [64, с. 401]. Тобто, визначення NIST більше акцентує свою увагу на переліку того, що має захищатись від кіберзагроз.

Зі свого боку Асоціація аудиту і контролю інформаційних систем (ISACA) визначає кібербезпеку як захист інформаційних активів шляхом протидії загрозам інформації, що обробляється, зберігається та транспортується інформаційними системами, об'єднаними в мережу Інтернет [5, с. 42]. Це визначення більш стисле і лаконічне, і не містить жодної зайвої інформації.

З огляду на всі запропоновані вище дефініції, я вважаю, що найкращим визначенням кібербезпеки буде таке. Кібербезпека – це комплекс заходів, які вживаються суб'єктами міжнародного або національного права з метою захисту персональних даних, важливої та конфіденційної інформації, кіберпростору, а також для забезпечення безперешкодного функціонування держави та електронних сервісів. В умовах стрімкого розвитку технологій та зростання кібератак, ефективна кібербезпека стає невід'ємною частиною функціонування сучасних суспільств. Завдяки системному підходу та співпраці між державними органами, приватним сектором і міжнародними організаціями, вдається створити більш безпечне цифрове середовище.

Не зважаючи на те, яке визначення кібербезпеки використовується, її метою залишається забезпечення конфіденційності, цілісності та доступності інформації (табл. 1.2).

Таблиця 1.2

Складові мети кібербезпеки

№	Складова мети кібербезпеки	Зміст
1	Конфіденційність	Дані або інформація не надаються та не розголошуються неавторизованим особам або процесам.
2	Цілісність	Дані або інформація не були змінені або знищені несанкціонованим чином.
3	Доступність	Дані або інформація доступні та можуть бути використані на вимогу уповноваженою особою.

Джерело: [45]

Створення сильної та ефективної стратегії забезпечення кібербезпеки вимагає серйозного підходу. Зазвичай, такі стратегії містять в собі такі елементи:

1. Ефективний план реагування на інциденти та кризові ситуації;
2. Управління кіберзахистом;
3. Надійний захист від загроз;
4. Постійний моніторинг безпеки.

Так, план реагування на інциденти та кризові ситуації має на меті швидко та ефективну реакцію на ситуацію, що виникла, а також здатність управляти кризовою ситуацією таким чином, щоб усі сторони чітко розуміли план дій. Управління кіберзахистом означає, що організація повинна призначити сильну команду безпеки для управління планом реагування на інциденти та кризові ситуації. Зазвичай така команда складається з керівника з безпеки, загальних менеджерів з безпеки, інженерів та аналітиків. Зі свого боку, захист від загроз є одним з ключових інструментів, що допомагає захистити організацію від кіберзагроз. Також даний інструмент може допомогти у підвищенні готовності реагування на інциденти та кризові ситуації. Зазвичай, найкращі з таких інструментів містять в собі такі технології, як threat detection, тобто технологія, яка виявляє кіберзагрози; monitoring, тобто технологія, яка відстежує дані загрози;

penetration testing, тобто технологія, яка тестує програмне забезпечення; управління patch, тобто технологія, яка виявляє та заповнює прогалини в системі кібербезпеки; та endpoint protection, тобто технологія, яка захищає вхідні та вихідні точки пристроїв від кіберзагроз. Останній елемент, моніторинг безпеки, передбачає, що організація бачити і розуміє поточний стан кібербезпеки, взаємодію пристроїв і користувачів із системою, а також здатна ідентифікувати кіберінцидент. З цією метою організації дозволяють командам безпеки виявляти та виправляти різноманітні аномалії та відхилення від норми у системі безпеки [34].

Варто звернути свою увагу на те, що кібербезпека складається з низки ключових компонентів, які є життєво важливими для захисту цифрових активів та конфіденційних даних у сучасному світі. Оскільки кіберзагрози продовжують розвиватися та створювати проблеми, їхнє розуміння та впровадження є критично важливими для організацій та окремих осіб, щоб ефективно зменшувати ризики та підтримувати стійкість до кібератак. Так, до компонентів кібербезпеки відносять мережеву безпеку, захист кінцевих точок, шифрування даних, обізнаність та навчання з питань безпеки, реагування на інциденти та їх управління, управління та відповідність вимогам, а також управління ідентифікацією та доступом (табл. 1.3). Разом все це утворює основу надійної системи кібербезпеки.

Таблиця 1.3

Основні компоненти кібербезпеки

№	Компонент кібербезпеки	Зміст
1	Мережева безпека	Це передбачає створення потужних захисних механізмів, таких як віртуальні приватні мережі (VPN) для створення безпечних з'єднань через загальнодоступні мережі, системи виявлення атак (IDS) для моніторингу та аналізу мережевого трафіку на наявність ознак злочинної діяльності, а також брандмауери для фільтрації вхідного та вихідного мережевого трафіку.
2	Захист кінцевих точок	Це включає використання технологій виявлення та реагування на кінцеві точки (EDR) для моніторингу та реагування на поведінку кінцевих точок у режимі реального часу, антивірусного програмного забезпечення для виявлення та видалення шкідливого програмного забезпечення, а також

Продовження табл. 1.3

№	Виклики0,	Зміст
2	Захист кінцевих точок	захисту пристроїв для захисту даних кінцевих точок від несанкціонованого використання.
3	Шифрування даних	Конфіденційність та цілісність вимагають захисту конфіденційних даних шляхом їх кодування у нечитабельний код. Методи безпеки, такі як симетричне та асиметричне шифрування, гарантують безпеку інформації під час обробки, передачі та зберігання, навіть якщо вона потрапить не в ті руки.
4	Обізнаність та навчання з питань безпеки	Створення культури безпеки в організації вимагає навчання користувачів та персоналу найкращим практикам кібербезпеки. Це включає навчання людей сучасним методам, зокрема фішинговим електронним листам та методам соціальної інженерії, шляхом проведення навчальних сесій та надання порад щодо виявлення та обробки подій безпеки.
5	Реагування на інциденти та їх управління	Щоб мінімізувати наслідки порушень та зберегти безперервність бізнесу, необхідно встановити політики та процедури для виявлення, обробки та відновлення після інцидентів кібербезпеки. Це передбачає формування групи реагування на інциденти, завданням якої є виявлення та припинення порушень безпеки, а також розробка детального плану реагування на інциденти, який визначає, що слід робити у разі кібератаки.
6	Управління та відповідність вимогам	Вимога дотримання бізнес-стандартів та правових норм має вирішальне значення для зниження ризиків та підтримки відповідальності. Для ефективного управління ризиками це включає впровадження правил безпеки, процедур та засобів контролю. Це включає регулярний аудит та аналіз дотримання вимог для виявлення областей, які потребують розвитку та коригування.
7	Управління ідентифікацією та доступом	Уникнення небажаного доступу до систем і даних значною мірою залежить від управління онлайн-ідентифікаторами, верифікацією та контролем доступу. Щоб отримати доступ, користувачі повинні спочатку надати кілька форм верифікації за допомогою таких методів, як багатофакторна автентифікація (MFA). Аналогічно, контроль доступу на основі ролей (RBAC) гарантує, що користувачам надаються дозволи відповідно до їхніх посад та обов'язків в організації.

Джерело: [32]

Всі ці аспекти допомагають сформувати необхідний фундамент для розуміння концепції кібербезпеки. В умовах глобалізації та зростання кількості кіберзагроз, особливої актуальності набуває формування єдиних міжнародних стандартів і налагодження глобальної співпраці у сфері кібербезпеки. Важливим є усвідомлення, що забезпечення кібербезпеки неможливе без комплексного підходу, що передбачає інтеграцію технічних рішень, правового регулювання, організаційної політики та розвитку культури безпеки серед користувачів. Лише поєднання цих компонентів дозволяє ефективно протидіяти сучасним кіберзагрозам і забезпечувати стійкість цифрового простору.

1.2. Міжнародне співробітництво у сфері кібербезпеки

Кібербезпека сьогодні є глобальною проблемою, а її забезпечення неможливе без об'єднання зусиль різних держав, міжнародних організацій та приватних корпорацій. Інформаційні технології, що стрімко проникають у всі сфери життя, створюють нові можливості для розвитку, але водночас породжують і безпрецедентні ризики, які не знають кордонів. Взаємозалежність національних інфраструктур, глобалізація бізнесу та зростання ролі цифрової економіки обумовлюють необхідність формування ефективної системи міжнародного співробітництва у сфері кібербезпеки.

Кіберпростір не має фізичних кордонів, тому атаки, що здійснюються в одній країні, можуть мати значний вплив на інші держави чи навіть цілі регіони. Враховуючи асиметричний та анонімний характер кіберзагроз, міжнародна співпраця є життєво важливою для:

1. Своєчасного обміну інформацією про загрози;
2. Координації дій у випадку масштабних кібератак;
3. Розробки спільних стандартів і протоколів безпеки;
4. Забезпечення дотримання міжнародного права в кіберпросторі.

Початок міжнародному співробітництву у сфері кібербезпеки було покладено підписанням Будапештської конвенції про кіберзлочинність 2001 року. Даний

документ передбачає, що сторони повинні співпрацювати між собою з різних питань, що стосуються кібербезпеки та кіберзлочинності, зокрема з метою розслідування та судового розгляду таких злочинів [35]. Слід зазначити, що Конвенція має на меті збалансувати ефективну правоохоронну діяльність із захистом основних прав людини, установити рамки взаємоповаги між країнами у сфері забезпечення кібербезпеки, надати країнам дозвіл для обміну інформацією та ресурсами з метою розслідування кіберзлочинів та гармонізувати національне законодавство та посилити співпрацю в міжнародних відносинах у контексті кібербезпеки.

Також варто звернути свою увагу на головні напрямки міжнародного співробітництва, які визначені Глобальним порядком денним кібербезпеки МСЕ (GCA). Запроваджений у 2007 р. тодішнім Генеральним секретарем МСЕ доктором Хамадуном І. Туре, GCA є основою для міжнародної співпраці, спрямованої на підвищення довіри та безпеки в інформаційному суспільстві. Глобальний порядок денний розроблений для співпраці та ефективності, заохочення співпраці з усіма відповідними партнерами та між ними, а також спирається на існуючі ініціативи, щоб уникнути дублювання зусиль [46]. Згідно з ним, до головних напрямів міжнародного співробітництва у сфері кібербезпеки належать правові заходи, технічні та процедурні заходи, організаційні структури, розвиток можливостей та міжнародне співробітництво (табл. 1.4)

Таблиця 1.4

Головні напрями міжнародного співробітництва у сфері кібербезпеки

№	Напрямок	Зміст
1	Правові заходи	Дана область прагнула розробити рекомендації щодо того, як злочинні дії, вчинені через ІКТ, можуть бути врегульовані через законодавство в міжнародно сумісний спосіб.
2	Технічні та процедурні заходи	Дана область зосереджена на ключових заходах для подолання уразливостей у програмних продуктах, включаючи акредитаційні схеми, протоколи та стандарти.
3	Організаційні структури	Дана область розглянула загальні рамки та стратегії реагування для запобігання, виявлення, реагування на кібернапади та управління кризами, включаючи захист критичних інформаційних інфраструктурних

Продовження табл. 1.4

№	Напрямок	Зміст
3	Організаційні структури	систем країн.
4	Розвиток можливостей	Дана область розробила стратегії для механізмів підвищення потенціалу для підвищення обізнаності, передачі знань та зміцнення кібербезпеки в національному політичному порядку денному.
5	Міжнародне співробітництво	Дана область розробила стратегію для міжнародної співпраці, діалогу та координації у боротьбі з кіберзагрозами.

Джерело: [63, с. 2]

Важливу роль у міжнародному співробітництві відіграють також різні міжнародні організації. Наприклад, Європейський Союз (ЄС) постійно виживає найрізноманітніші заходи для забезпечення кібербезпеки на міжнародному рівні. Так, в 2013 р. було прийнято першу Стратегію кібербезпеки ЄС «Відкритий, безпечний та захищений кіберпростір», яка визначала кібербезпеку як нову сферу діяльності Союзу. Згідно зі стратегією, основними принципами кібербезпеки включають такі пункти: основні цінності ЄС застосовуються як у цифровому, так і у фізичному світі; захист основних прав, свободи вираження поглядів, персональних даних і приватності; доступ для всіх; демократичне та ефективне багатостороннє управління; спільна відповідність за забезпечення безпеки (табл. 1.5)

Таблиця 1.5

Основні принципи в Стратегії кібербезпеки ЄС

№	Основні принципи	Зміст
1	Основні цінності ЄС застосовуються як у цифровому, так і у фізичному світі	Закони і норми, які застосовуються в інших сферах повсякденного життя, мають діяти і в кіберпросторі.
2	Захист основних прав, свободи вираження поглядів, персональних даних і приватності	Кібербезпека може бути надійною і ефективною лише в тому випадку, коли вона ґрунтується на основних правах і свободах людини, закріплених у Хартії основоположних прав ЄС та основних цінностях ЄС. У свою чергу, права людини не можуть бути захищені без безпечних мереж і систем.
3	Доступ для всіх	Обмежений доступ до інтернету, його відсутність, а також цифрова неграмотність є несприятливим

Продовження табл. 1.5

№	Основні принципи	Зміст
3	Доступ для всіх	фактором для громадян, оскільки цифровий світ став важливою складовою у суспільстві. Кожен повинен мати доступ до Інтернету та безперешкодного потоку інформації.
4	Демократичне та ефективне багатостороннє управління	Цифровий світ не контролюється лише одним суб'єктом. В наш час участь у повсякденному управлінні Інтернет-ресурсами, протоколами, стандартами і майбутньому розвитку Інтернету беруть кілька зацікавлених сторін, серед яких багато комерційних і неурядових організацій.
5	Спільна відповідальність за забезпечення безпеки	Зростаюча залежність від ІКТ у всіх сферах людського життя призвела до появи низки вразливих місць, які необхідно належним чином визначити, ретельно проаналізувати і виправити або зменшити. Усі відповідні суб'єкти повинні визначити цю спільну відповідальність, вжити заходів для свого захисту і, за необхідності, забезпечити скоординоване реагування з метою зміцнення кібербезпеки.

Джерело: [43, с. 3-4]

Пізніше, у 2017 р., ЄС прийняв другу Стратегію кібербезпеки «Стійкість, стримування та оборона: Побудова міцної кібербезпеки для ЄС». Дана стратегія пропонує зацікавленим сторонам зосередитися на трьох пріоритетних сферах: Безпека в критично важливих програмах або програмах з високим рівнем ризику, кібербезпека широко розгорнутих цифрових продуктів, мереж, систем і послуг; а також використання методів «безпеки за задумом» в недорогих, цифрових, взаємопов'язаних масових споживчих пристроях, які складають Інтернет речей (табл. 1.6)

Таблиця 1.6

Основні пріоритети в Стратегії кібербезпеки ЄС

№	Основні пріоритети	Зміст
1	Безпека в критично важливих програмах або програмах з високим рівнем ризику	Системи, від яких ми залежимо в нашій повсякденній діяльності, від наших автомобілів до машин на заводах, від найбільших систем, таких як літаки або електростанції, до найменших, таких як медичні прилади, стають все більш цифровими і взаємопов'язаними. Тому основні ІКТ-компоненти в таких продуктах і системах потребують ретельної оцінки безпеки.

Продовження табл. 1.6

№	Основні піоритети	Зміст
2	Кібербезпека широко розгорнутих цифрових продуктів, мереж, систем і послуг	Це включає в себе продукти, мережі, системи і послуги, що використовуються як приватним, так і державним сектором для захисту від атак і виконання регуляторних зобов'язань, таких як шифрування електронної пошти, брандмауери і віртуальні приватні мережі; вкрай важливо, щоб поширення використання таких інструментів не призвело до появи нових джерел ризику або нових вразливостей.
3	Використання методів «безпеки за задумом» в недорогих, цифрових, взаємопов'язаних масових споживчих пристроях, які складають Інтернет речей	Схеми в рамках цієї концепції можуть бути використані для сигналізації про те, що продукти створені з використанням найсучасніших безпечних методів розробки, що вони пройшли адекватне тестування на безпеку і що постачальники зобов'язалися оновлювати своє програмне забезпечення в разі виявлення нових вразливостей або загроз.

Джерело: [60, с. 5]

Останньою стратегією ЄС стала Стратегія кібербезпеки для цифрового десятиліття, прийнята наприкінці 2020 р. [67]. Дана стратегія спрямована на забезпечення глобального та відкритого Інтернету з надійними бар'єрами для подолання ризиків для безпеки та основних прав і свобод людей у Європі. Вона також містить конкретні пропозиції для вирішення трьох основних сфер діяльності: стійкість, технологічний суверенітет та лідерство; розбудова оперативного потенціалу для запобігання, стримування та реагування; та розвиток глобального та відкритого кіберпростору (табл. 1.7)

Таблиця 1.7

Основні сфери діяльності ЄС в контексті Стратегії

№	Сфера діяльності	Складові
1	Стійкість, технологічний суверенітет та лідерство	1. Стійка інфраструктура та критично важливі послуги; 2. Розбудова Європейського кіберщита; 3. Надбезпечна комунікаційна інфраструктура; 4. Забезпечення безпеки широкосмугових мобільних мереж наступного покоління;

Продовження табл. 1.7

№	Сфера діяльності	Зміст
1	Стійкість, технологічний суверенітет та лідерство	5. Інтернет безпечних речей; 6. Посилення глобальної безпеки Інтернету; 7. Посилена присутність у ланцюжку поставок технологій; 8. Кіберкваліфікована робоча сила ЄС.
2	Розбудова оперативного потенціалу для запобігання, стримування та реагування	1. Об'єднаний кіберпідрозділ; 2. Боротьба з кіберзлочинністю; 3. Інструментарій ЄС для кібердипломатії; 4. Посилення можливостей кіберзахисту.
3	Розвиток глобального та відкритого кіберпростору	1. Лідерство ЄС у сфері стандартів, норм та рамок у кіберпросторі; 2. Співпраця з партнерами та багатосторонньою спільнотою зацікавлених сторін; 3. Зміцнення глобального потенціалу для підвищення глобальної стійкості.

Джерело: [67, с. 5-22]

Ще одним таким документом, який регулює забезпечення кібербезпеки в ЄС, є Регламент Європейського парламенту та Ради «Про встановлення заходів для забезпечення високого загального рівня кібербезпеки в установах, органах, службах та агентствах Союзу» [51]. Даний документ встановлює заходи, спрямовані на досягнення високого рівня кібербезпеки в межах суб'єктів Союзу. Він також встановлює вимоги для підвищення рівня кібербезпеки в установах, органах, службах та агентствах ЄС; зобов'язує установи впроваджувати заходи та політики для захисту своїх інформаційних систем і даних; передбачає проведення регулярних оцінок ризиків для виявлення вразливих сторін та розробки заходів для їх усунення; стимулює співпрацю між різними установами ЄС для обміну інформацією про загрози та заходи кіберзахисту; зобов'язує установи забезпечувати навчання персоналу з питань кібербезпеки та встановлює механізми моніторингу виконання вимог регламенту та звітності про досягнуті результати [51].

Також активну участь у міжнародному співробітництві щодо кібербезпеки бере Організація Північноатлантичного договору (НАТО). В контексті кібербезпеки Альянс розробляє численні ініціативи, Зокрема: навчальні та освітні програми, навчання і воєнні тренування й спільні доктрини та стратегії, що допомагає зміцнити його стабільність [65]. Одним з таких прикладів є Зобов'язання щодо кібероборони. Даний документ передбачає визнання нових загроз лідерами країн НАТО та зобов'язання забезпечити захист своїх країн; зміцнення кіберзахисту національних інфраструктур, співпрацювати відповідно до політики НАТО та підтримувати колективну безпеку; підтримку співпраці між НАТО та ЄС у сфері кібербезпеки; сприяння співпраці через інтернаціональні проєкти, навчання та обмін інформацією для кіберзахисту; розвиток можливостей для захисту інфраструктури, а також щорічну оцінку виконання зобов'язань та відстеження прогресу [38]. Ще одним з таких документів є Стратегічна концепція НАТО 2022 [19]. У даній стратегії наголошується, що «забезпечення колективної стійкості наших суспільств є вирішальним для виконання усіх основоположних завдань Альянсу і підґрунтям наших зусиль убезпечити наші країни, суспільства і спільні цінності. У ній також підкреслюється наскрізна необхідність інвестицій у технологічні інновації і включення таких аспектів, як зміна клімату, людська безпека і тематика жінок, миру і безпеки до усіх основоположних завдань Альянсу» [19, с. 1]. Таким чином, НАТО робить усе можливе для забезпечення кібербезпеки у Євроатлантичному регіоні шляхом міжнародного співробітництва країн-членів у даній сфері.

Зі свого боку, Організація Об'єднаних Націй (ООН) 24 грудня 2024 р. ухвалила Конвенцію проти кіберзлочинності. Дана конвенція застосовується для запобігання, розслідування, та кримінального переслідування правопорушень, включаючи заморожування, арешт, конфіскацію та повернення доходів, одержаних від таких правопорушень, а також для збору, отримання, збереження та обміну доказами в електронній формі для цілей кримінального розслідування або судового розгляду [70].

Незважаючи на важливість і позитивні зрушення у розвитку міжнародного співробітництва у сфері кібербезпеки, цей процес залишається далеким від ідеалу та супроводжується низкою серйозних обмежень і недоліків. У реальній практиці взаємодія між державами часто стикається з різноманітними перешкодами, які ускладнюють досягнення спільних цілей у сфері кіберзахисту. Слід враховувати, що кожна країна має власні підходи, пріоритети та рівень розвитку кіберінфраструктури, що, у свою чергу, створює додаткові виклики для ефективної координації зусиль. Крім того, існують окремі фактори, які суттєво стримують подальший розвиток міжнародної співпраці у цій галузі та потребують додаткової уваги з боку світової спільноти. До таких факторів належать швидкий технологічний прогрес, проблеми з атрибуцією, недостатня прозорість, різні національні погляди, геополітична напруженість, правові та регуляторні виклики, різниця в ресурсах, непередбачувані наслідки, еволюція характеру кіберзагроз та етичні міркування (табл. 1.8)

Таблиця 1.8

Обмеження та недоліки сучасного міжнародного співробітництва у сфері кібербезпеки

№	Обмеження і недоліки	Зміст
1	Швидкий технологічний прогрес	Темпи технологічних змін у сфері кібербезпеки неймовірно швидкі. Як наслідок, результати досліджень можуть швидко застаріти, а нові загрози або технології можуть бути неадекватно розглянуті в дослідженні.
2	Проблеми з атрибуцією	Однією з постійних проблем у сфері кібербезпеки є точне віднесення кібератак до конкретних акторам. Анонімність і методи приховування, що використовуються суб'єктами кіберзагроз, ускладнюють остаточну ідентифікацію атак, що впливає на атаки, що впливає на точність аналізу діяльності, яка фінансується державою.
3	Недостатня прозорість	Національні держави часто діють з певним ступенем секретності щодо своїх стратегій і можливостей у сфері кібербезпеки. Обмежена прозорість може перешкоджати всебічному розумінню заходів, що вживаються державами у відповідь на кіберзагрози, що потенційно може призвести до неповного або упередженого аналізу.
4	Різні національні погляди	Держави мають різні погляди на кібербезпеку, що ґрунтуються на їхньому геополітичному контексті,

Продовження табл. 1.8

№	Обмеження і недоліки	Зміст
4	Різні національні погляди	культурних цінностях та історичному історичного досвіду. Ці відмінності можуть ускладнювати зусилля зі створення універсальних норм і угод, а також можуть призвести до різного тлумачення загроз кібербезпеці та відповідної реакції на них.
5	Геополітична напруженість	Геополітична напруженість і суперництво між країнами можуть перешкоджати ефективній глобальній співпраці у сфері кібербезпеки. Політичні міркування, історичні конфлікти та недовіра можуть перешкоджати створенню механізмів співпраці, обмежуючи ефективність міжнародних зусиль з протидії кіберзагрозам.
6	Правові та регуляторні виклики	Нормативно-правова база кібербезпеки в різних країнах дуже відрізняється. Гармонізація цих рамок для сприяння глобальному співробітництву створює проблеми через відмінності в правових традиціях, підходах до приватного життя та пріоритетах національної безпеки.
7	Різниця в ресурсах	Існують значні розбіжності в ресурсах і можливостях країн для вирішення проблем кібербезпеки. Країни, що розвиваються, та економічно неблагополучні країни можуть зіткнутися з проблемами у впровадженні надійних заходів кібербезпеки, що потенційно може поглибити глобальну кібернетичну нерівність.
8	Непередбачувані наслідки	Реакція держави на кіберзагрози може мати непередбачувані наслідки, включаючи ескалацію напруженості або введення обмежень, які ненавмисно впливають на індивідуальні свободи. Аналіз потенційних непередбачуваних наслідків дій держави є складним і відповідальним завданням.
9	Еволюція характеру кіберзагроз	Кіберзагрози постійно еволюціонують, а противники адаптують свою тактику і методи. Передбачення та протидія новим загрозам є складним завданням, а ефективність реакції держави може бути обмежена динамічним характером ландшафту кібербезпеки.
10	Етичні міркування	Використання наступальних кіберпотужностей викликає етичні міркування, в тому числі питання пропорційності, супутньої шкоди і потенційної мілітаризації кіберпростору. Етичні проблеми можуть бути неадекватно враховані у відповідях держав і міжнародних угодах.

Джерело: [55, с. 17-18]

Враховуючи зазначені проблеми, можна сказати, що формування сектору кібербезпеки на міжнародному та національному рівнях все ще триває. Оскільки даний процес стикається з багатьма викликами через інноваційний характер питань кібербезпеки, усі актори міжнародних відносин повинні докласти активні зусилля для налагодження міжнародного співробітництва з питань кібербезпеки в різних формах. Основними напрямками такого співробітництва можуть стати розробка нормативно-правової бази, технічних та процедурних засад кібербезпеки, створення організаційних структур, підготовка кадрів та координація дій зацікавлених сторін. При цьому значна увага повинна приділятися врахуванню існуючих національних та регіональних ініціатив з метою уникнення дублювання функцій [73, с. 8].

Отже, можна зробити висновок, що міжнародне співробітництво у сфері кібербезпеки є надзвичайно важливим і актуальним у сучасному світі. Це підтверджується, зокрема, створенням Глобального порядку денного кібербезпеки, що об'єднує зусилля різних держав у протистоянні кіберзагрозам. Додатковим свідченням значущості такого співробітництва виступає активна політика ключових міжнародних організацій, таких як ЄС, НАТО та ООН. Прийняті цими організаціями стратегії та конвенції стали не лише основою для спільних дій у сфері кібербезпеки, а й сприяють гармонізації підходів та обміну досвідом між державами-членами. Також важливо зазначити, що розвиток співробітництва у даній сфері все ще триває. Таким чином, ефективне міжнародне партнерство у сфері кібербезпеки дозволяє країнам більш результативно реагувати на сучасні виклики та загрози у цифровому просторі.

РОЗДІЛ 2

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ДИПЛОМАТІЇ

2.1. Вплив глобальних викликів на дипломатію у галузі кібербезпеки

Сучасна дипломатія зазнала суттєвої трансформації, яка зумовлена стрімким розвитком цифрових технологій. Кіберпростір сформував новий вимір для міждержавної дипломатичної взаємодії. Якщо раніше ключовими функціями дипломатичної діяльності були представництво держави, офіційна комунікація, проведення переговорів та збирання інформації, то нині до цього спектра додано завдання із запобігання та врегулювання кіберінцидентів. Така еволюція дипломатії відображає глибокі зміни у природі сучасної міжнародної взаємодії, які визначаються не лише політичною чи економічною конкуренцією, а й боротьбою за безпеку у віртуальному просторі.

Дипломатичні відносини у ХХІ ст. дуже відрізняються від тих, що були у ХVІІ ст., коли почала формуватися дипломатія у її сучасному вигляді. Тоді посланці королів і королев подорожували світом, щоб доставити важливі документи або передати важливі новини правителю іншої держави, одночасно обговорюючи відносини між двома країнами. Сьогодні главам держав навіть не потрібно залишати свій кабінет, щоб передати свої думки чи наміри — це можна зробити через виступ перед ЗМІ або один пост у соціальних мережах. І весь світ одразу дізнається про наміри конкретної держави у її зовнішній політиці [30].

Цифрова трансформація змінила дипломатію, розширивши взаємодію між державами, міжнародними організаціями та недержавними акторами. Традиційна дипломатія, що базувалася на особистих переговорах, поступилася місцем цифровим технологіям, які дозволили взаємодіяти через соціальні мережі та миттєві повідомлення. Це дало можливість урядам безпосередньо спілкуватися з глобальною аудиторією. Це призвело до появи ще одного виду дипломатії — цифрової дипломатії (або «твітердипломатія»), яка полегшила комунікацію та участь у публічній дипломатії, а також підвищила ефективність зовнішньої

політики завдяки аналізу даних і штучному інтелекту. Однак вона також породила виклики, пов'язані з безпекою, маніпуляціями інформацією та ризиками в міжнародних відносинах. Необхідно знайти баланс між використанням нових технологій і управлінням їхніми ризиками [74, с. 3].

До того ж, технологічний прогрес призвів до зростання залежності країн від цифрової інфраструктури, що, зі свого боку, підвищило їхню вразливість до кібератак, витоків конфіденційної інформації та маніпулятивних інформаційних впливів. Це суттєво змінює характер дипломатичних відносин між державами у глобальному контексті. Зростання кількості кіберзагроз стало значним викликом для дипломатії. Так, загрозами, які мають суттєвий вплив на дипломатію, можуть бути (табл. 2.1):

1. Ескалація ландшафту загроз;
2. Кібервійни, що спонсоруються державами;
3. Кібертероризм;
4. Економічне шпигунство та крадіжка інтелектуальної власності;
5. Вплив на міжнародні відносини;
6. Нагальна потреба в міжнародній співпраці;
7. Розбудова стійкості кіберзахисту [72].

Таблиця 2.1

Кіберзагрози, які мають суттєвий вплив на дипломатію

№	Кіберзагрози	Зміст
1	Ескалація ландшафту загроз	Стрімкий розвиток технологій випереджає заходи безпеки, що створюють сприятливі умови для кіберзагроз. Кількість кібератак на критичну інфраструктуру, фінансові системи та урядові установи зростає, чому багато з них організовують державні структури з метою порушення роботи інших країн, викрадання інформації чи впливу на політичні події. Яскравим прикладом є російська атака хакерів на Національний комітет Демократичної партії США у 2016 році, яка призвела до витоків важливої інформації та вплинула на хід президентських виборів. Це продемонструвало, як кібероперації можуть вплинути на політичні процеси та сприяти дестабілізації суспільства.

Продовження табл. 2.1

№	Кіберзагрози	Зміст
2	Кібервійни, що спонсоруються державами	Кібервійна, яку підтримує держава, стала інструментом у міжнародних відносинах, дозволяючи країнам анонімно досягти своїх геополітичних цілей і зменшити ризик прямої відплати. Держави як Китай, росія, Північна Корея та Іран активно вибирають кібершпигунство, діючи складні атаки для отримання розвідувальних даних і порушення роботи важливих систем. Яскравим прикладом є атака SolarWinds 2020 року, яка вразила урядові установи та приватні компанії США. Китай також звинувачують у масштабній крадіжці інтелектуальної власності для отримання конкурентних переваг, що підриває економічну безпеку та ускладнює дипломатичні відносини.
3	Кібертероризм	Загрози в кіберпросторі створюють не лише державні, а й недержавні суб'єкти, такі як терористичні організації та злочинні угруповання. Терористи використовують Інтернет для пропаганди, вербування та координації атак, як це робила ІДІЛ через соціальні мережі, надихаючи окремих осіб на теракти. Злочинні синдикати виконують кібератаки, зокрема із застосуванням програм-вимагачів проти лікарень, шкіл і бізнесу. Яскравим прикладом стала атака WannaCry у 2017 році, яка завдала шкоди сотням тисяч комп'ютерів у 150 країнах і спричинила значні фінансові збитки.
4	Економічне шпигунство та крадіжка інтелектуальної власності	Економічне шпигунство та крадіжка інтелектуальної власності є серйозними загрозами для світової економіки. Як державні, так і недержавні суб'єкти розміщують кібератаки з наданням вироблення комерційних таємниць і цінної інформації, щоб отримати перевагу та завдати шкоди конкурентам. Прикладом є діяльність китайських хакерів, які щорічно завдають американським компаніям і економіці США збитків на мільярди доларів через крадіжку інтелектуальної власності. Така ситуація викликає заклики до посилення міжнародної співпраці та впровадження ефективних заходів кібербезпеки.
5	Вплив на міжнародні відносини	Кіберзагрози суттєво впливають на міжнародні відносини, часто спричиняючи напругу та підлив довіри між державами. Визначте винуватця кібератаки складно, наша країна традиційно заперечує свою причетність, навіть при наявності доказів, що ускладнює узгоджену реакцію та формування міжнародних правил у кіберпросторі. У відповідь на кібератаки держава використовує дипломатичні заходи, наприклад санкції чи публічний суд, як це зробили США та їхні

Продовження табл. 2.1

№	Кіберзагрози	Зміст
5	Вплив на міжнародні відносини	союзники щодо росії. Однак такі дії можуть більше загострити міжнародну напругу й підвищити ризик ширших конфліктів.
6	Нагальна потреба в міжнародній співпраці	Для подолання складних викликів у сфері кібербезпеки потрібна тісна міжнародна співпраця та встановлених чітких правил у кіберпросторі. Важливо створити комплексну систему управління кібербезпекою для зниження ризиків і забезпечення стабільності. Міжнародні організації, такі як ООН і G20, активно працюють над розвитком діалогу та співпраці в цій сфері. Значних успіхів досягла група експертів ООН щодо визначення норм поведінки влади, зокрема заборони нападу на критичну інфраструктуру. Важливу роль відіграють і регіональні союзи, наприклад, Центр кіберзахисту НАТО, який обмінює повідомлення та розробляє спільні механізми захисту. Двосторонні угоди, як-от Кіберугода між США та Китаєм, також допомагають обмежити кіберкрадіжки й сприяють відповідній поведінці в цифровому середовищі.
7	Розбудова стійкості кіберзахисту	Хоча міжнародна співпраця є надзвичайно важливою, окремі країни також повинні інвестувати у створення стійкої кіберзахисту. Це включає розробку надійної політики кібербезпеки, розширення можливостей національних кіберагентств та сприяння державно-приватному партнерству. Інвестування в освіту та навчання з кібербезпеки є важливим для задоволення зростаючого попиту на кваліфікованих фахівців. Встановлення стандартів кібербезпеки та передового досвіду може допомогти організаціям захистити свої мережі та дані від потенційних загроз. Крім того, просування культури обізнаності з кібербезпекою серед громадян може зменшити ризик кіберінцидентів, спричинених людською помилкою.

Джерело: [72]

Насамперед, це стосується саме кібератак, адже саме вони завдають чи не найбільшої шкоди для функціонування держав. Вони негативно впливають на національну безпеку, економічну стабільність та глобальне співробітництво. Слід зазначити, що на противагу від традиційних військових атак, кібератаки можуть виконуватися дистанційно і часто без явних слідів. Це значно ускладнює адекватну реакцію держав. Кіберзагрози не обмежуються лише державними

агентами. Недержавні організації, включно з хакерами та різноманітними злочинними угрупованнями, також можуть використовувати вразливі місця у цифрових системах, що ще більше ускладнює дипломатичні відповіді. Подібні явища спричиняють зростання напруженості у міждержавних відносинах, тому що кібератаки здатні підірвати взаємну довіру та дестабілізувати усталений міжнародний порядок. У контексті ескалації кіберзагроз відбувається трансформація принципів і норм, що регулюють сучасну міжнародну дипломатію. Кіберрозвідка та інформаційно-психологічні операції, зокрема кампанії з дезінформації, є серйозним викликом для дипломатичної взаємодії, оскільки підривають довіру громадськості та суттєво ускладнюють міждержавну співпрацю [59, с. 2].

Кібератаки перестали бути просто інструментом для крадіжки інформації; вони використовуються для підриву економіки, послаблення політичних систем і підриву довіри до урядів. Цей зсув підвищив ставки на кібербезпеку, перетворивши її на ключову сферу національної оборонної стратегії. Зростання цих загроз також виявило прогалини в міжнародних нормах і системах управління. Чинне міжнародне право часто не встигає за швидкою еволюцією кібертактики та складнощами визначення авторства в кіберпросторі. Як наслідок, міжнародне співтовариство стикається зі значними труднощами в розробці єдиної відповіді на кіберзагрози, яка б збалансувала безпеку із захистом прав і свобод особистості. Постійне зростання кіберзагроз підкреслює нагальну потребу в глобальному співробітництві та створенні надійних норм і правил кібербезпеки, здатних врахувати мінливий характер цих ризиків [59, с. 3].

Виклики кібербезпеки все частіше визнаються невід'ємною частиною кібердипломатії, оскільки вони переплітають технічні загрози з ширшими політичними та військовими стратегіями. Ризик кібератак, спрямованих на критично важливу інформаційну інфраструктуру, має значні наслідки для міжнародних відносин, що вимагає спільних підходів між державами для підвищення кіберстійкості. Концепція кіберконфлікту підкреслює постійні

суперечки в кіберпросторі, що ще більше ускладнює дипломатичні зусилля і міркування національної безпеки.

Дипломатія відіграє ключову роль у встановленні співпраці між державними та недержавними утвореннями в кіберпросторі. Однак, використання дипломатичних стратегій у цій сфері пов'язане зі складнощами. Швидкий та значний прогрес у кібертехнологіях розмиває межі між фізичною та цифровою взаємодією спільноти. Кіберсфера, що розвивається, суттєво впливає на те, як країни сприймають свої інтереси в сучасному світі. Ця сфера перетворилася на вразливе місце для урядів, які намагаються збалансувати зменшення загрози з використанням можливостей, що виникають. З розширенням перспектив інновацій у кіберпросторі зростає ймовірність як конкуренції, так і потенційного конфлікту [54].

З огляду те, що дипломатичні інструменти не завжди здатні забезпечити оперативне реагування на виклики у сфері кібербезпеки, у довгостроковій перспективі саме дипломатія може стати основою для формування стійкого та безпечного кіберпростору. Її стратегічне значення полягає у створенні міжнародних норм і механізмів, які здатні знизити ймовірність здійснення актів кібернетичної агресії.

Також серйозною проблемою є захист конфіденційних дипломатичних даних. Так, нещодавні розслідування показали, що деякі конфіденційні документи, зокрема іноземні дипломатичні телеграми, можна знайти у відкритому доступі в Інтернеті. Виявлено неадекватність систем шифрування для зв'язку цифровими засобами, а це означає, що отримані дані можуть бути використані хакерами [41].

Для захисту конфіденційної дипломатичної інформації важливий спільний і транснаціональний підхід. Серед можливих заходів, які можна застосувати в даній сфері, слід відзначити, зокрема формування міжнародних коаліцій для обміну інформацією, проведення спільних навчань у сфері кібербезпеки та створення колективних механізмів реагування на кібератаки. Наприклад, нещодавно прокурор Міжнародного кримінального суду (МКС) зазначив, що вже

розглядається можливість розслідування кібератак Офісом прокурора як міжнародних злочинів згідно з Римським статутом. Це означає, що в майбутньому кібератаки, які здійснюються, будуть підпадати під юрисдикцію МКС як воєнні злочини, злочини проти людяності, а також злочини агресії. Водночас, для цього необхідно враховувати масштаби, наслідки та наміри, що стоять за конкретними атаками [28]. Таким чином, це стане першим кроком на шляху розслідування кіберінцидентів і притягнення винуватців до відповідальності.

Отже, можна стверджувати, що сучасна дипломатія справді зазнала суттєвих трансформацій під впливом нових викликів, головним із яких є кібернетичні загрози. Ці загрози, зокрема кібератаки, стали дієвим інструментом для здійснення впливу на внутрішні справи інших держав, що ускладнює традиційні підходи до міжнародних відносин. Водночас дипломатія змушена адаптуватися до нових реалій, розробляючи механізми реагування на подібні виклики. Варто відзначити, що дипломатичні зусилля вже спрямовані на пошук ефективних шляхів подолання цієї проблеми, і в довгостроковій перспективі саме дипломатія може стати ключовим інструментом для забезпечення міжнародної безпеки у кіберпросторі. Таким чином, сучасна дипломатія демонструє свою здатність до змін та активного реагування на нові загрози, що постають перед світовою спільнотою.

2.2. Кібердипломатія як нова форма співпраці у світі

Стрімкий розвиток інформаційних технологій та цифрової інфраструктури став підґрунтям для виникнення абсолютно нових форм міжнародної взаємодії. Сучасне суспільство дедалі більше залежить від кіберпростору, який охоплює глобальні комунікаційні мережі, інформаційні системи та цифрові платформи. Державні та недержавні суб'єкти дедалі частіше використовують кіберпростір та Інтернет для маніпуляцій, порушень роботи, шахрайства, вимагання, крадіжки даних та відмивання грошей. Інтернет став ареною геополітичних битв та поширення дезінформації. Політичний вимір також важливий, як ми

неодноразово бачили на виборах у США, у кібератаках на кампанію Макрона, німецький Бундестаг та інші парламенти й міністерства [71]. У цих умовах зростає роль кібербезпеки як ключового чинника національної безпеки та міжнародних відносин. Це в свою чергу ввело в обіг нові терміни: «цифрова дипломатія» та «кібердипломатія». Зазвичай їх використовують як синоніми, але якщо з трактуванням першого терміну в науковців не виникає питань, то другий часто трактують як цифрову дипломатію, електронну дипломатію, медіа дипломатію тощо [11].

Загалом, кібердипломатію визначають як використання дипломатичних стратегій і переговорів для вирішення питань, пов'язаних з кіберпростором, включаючи кібербезпеку, управління Інтернетом і цифрові права. Оскільки цифровий ландшафт продовжує розширюватися, значення кібердипломатії зростає, сильно впливаючи на міжнародні відносини [42].

Практика кібердипломатії випередила її концептуалізацію майже на десятиліття, і донині серед її практиків існують розбіжності щодо того, що саме вона означає або чим відрізняється від інших видів дипломатії. Однак існує певний консенсус щодо центральної ролі міжнародної кібербезпеки та того, що кібердипломатія існує, перш за все, для запобігання конфліктам у кіберпросторі та через нього. Як ми обговоримо в наступному розділі, частково це походить від того, як ця галузь поступово формувалася завдяки зустрічі різних дипломатичних практик, габітусів та стратегій, запозичених з інших дипломатичних галузей [33, с. 449].

Суть кібердипломатії полягає у використанні дипломатичних засобів та ініціатив для досягнення цілей у складному та постійно змінюваному кіберпросторі, як зазначено в національній стратегії. Держави застосовують спільні правила, протоколи та моделі поведінки для покращення взаємодії між суб'єктами державного і приватного секторів.

Метою кібердипломатії є міжнародне співробітництво для зменшення наслідків кіберагресії, атак на критичну інфраструктуру, витоків даних, кіберзлочинності, кібершпигунства, онлайн-крадіжок та наступальних

кібероперацій, які здійснюють державні або недержавні актори. У зв'язку з особливостями кіберпростору важливо займатися кібердипломатією, а не покладатися лише на кібербезпеку.

Варто звернути увагу на те, що основою кібердипломатії є кібердіалог. Ззавичай його проводять за допомогою дипломатичних інструментів. Кібердіалог слугує майданчиком для міжнаціонального спілкування та обговорення шляхів вирішення кіберконфліктів, попереджаючи та запобігаючи їх переростанню в глобальні геополітичні проблеми та кібервійни [13, с. 72].

Як і в інших дипломатичних починаннях, кібердипломатія працює шляхом побудови стратегічних партнерств з іншими країнами світу для посилення колективних дій та співпраці проти спільних загроз, об'єднання коаліцій односторонців з життєво важливих політичних питань, обміну інформацією та національними ініціативами, а також протидії зловмисникам [58].

Загально визнане визначення кібернетичної дипломатії звучить таким чином: «кібердипломатія – це мистецтво, наука і сукупність засобів, за допомогою яких нації чи окремі індивіди захищають свої інтереси та сприяють політичним, економічним чи культурним відносинам в кіберпросторі» [10, с. 79].

Поняття кібердипломатії зародилося наприкінці XX століття, коли Інтернет почав відігравати все більшу роль у глобальних комунікаціях. На початковому етапі основна увага приділялася формуванню нормативної основи для регулювання Інтернету, і важливу роль у цьому процесі відігравали такі структури, як Інтернет-корпорація з присвоєння імен і номерів (ICANN), яка, хоч і не є класичною міжнародною організацією, мала суттєвий вплив. На початку 2000-х років відбулися значущі події, зокрема створення Групи урядових експертів ООН, яка розглядала питання інформаційних загроз, можливості міжнародної співпраці та інші аспекти інформаційної безпеки. З 2004 року кілька таких груп продовжували дослідження у цій сфері, підготувавши низку звітів із рекомендаціями, які були позитивно сприйняті Генеральною Асамблеєю ООН та підтримані державами-членами. Упродовж останніх років кібердипломатія значно розширила свою сферу діяльності, охопивши питання кібербезпеки, боротьби з

кіберзлочинністю й захисту критично важливої інфраструктури. Провідні міжнародні організації, зокрема, ООН, ЄС та НАТО розробили комплексні стратегії кібердипломатії для захисту національних інтересів і підтримки глобальної стабільності [33, с. 2]

З моменту прийняття концепції кібердипломатії у зовнішній політиці різних країн, вони переважно покладалися на підписання двосторонніх, тристоронніх та багатосторонніх угод про кібербезпеку, взаємний ненапад та обмін інформацією в кіберпросторі як на засіб врегулювання конфліктів, а також вирішення конфлікту інтересів, що виникають у кіберпросторі [53, с. 26].

Слід зазначити, що у сучасних міжнародних відносинах саме діяльність найбільших міжнародних організацій і провідних держав формує архітектуру глобальної кібербезпеки й кібердипломатії. Їхні підходи виражають баланс між прагненням до універсальних стандартів, національними інтересами та конкурентною боротьбою за технологічне лідерство.

Так, ООН виступає центральною глобальною платформою для обговорення кіберзагроз та розробки міжнародних правил поведінки держав у кіберпросторі. Її діяльність у цій сфері ґрунтується на принципах багатосторонності, інклюзивності та верховенства міжнародного права. Серед основних досягнень Організації у сфері кібердипломатії можна виділити три: міжнародна система звітності кібератак; вона ж «Points of Contact» Конвенція ООН про кіберзлочинність та Глобальний цифровий договір [52]. Оскільки Конвенцію було розглянуто у Розділі 1, акцентуємо увагу на інших двох аспектах.

Управління ООН з питань роззброєння (UNODA) оголосило про запуск Глобального довідника контактних осіб (PoC) та онлайн-порталу в межах робочої групи ООН з безпеки ІКТ. Цей довідник має зміцнити довіру й співпрацю між державами, використовуючи наявні регіональні ініціативи для підтримки безпечного та мирного ІКТ-середовища. 8 січня 2024 року UNODA закликала держав-членів призначити контактних осіб. Станом на 9 травня свою відповідь надали 92 країни. Перша тестова онлайн-зустріч відбулася 10 червня 2024 року. Організація також працює над онлайн-курсами для контактних осіб, та заохочує

залучення фінансування для подальшої розробки навчальних модулів. У відповідь на запит щодо письмових пропозицій UNODA отримало матеріали від 17 країн, усі вони доступні на офіційному сайті. Основні рекомендації включають посилення національної координації, підтримку актуальності довідника, постійне підвищення кваліфікації контактних осіб і обмін досвідом між існуючими мережами [49].

Щодо Глобального цифрового договору, це комплексна глобальна рамка для цифрової співпраці та управління штучним інтелектом. Він визначає дорожню карту для глобальної цифрової співпраці, спрямовану на використання величезного потенціалу цифрових технологій та подолання цифрової нерівності. 22 вересня 2024 року світові лідери зібралися в Нью-Йорку на Саміт майбутнього, де вони ухвалили Пакт майбутнього, який включає Глобальний цифровий договір [48].

Метою даного договору є інклюзивне, відкрите, стале, справедливе, безпечне та надійне цифрове майбутнє для всіх. Цей Глобальний цифровий договір визначає цілі, принципи, зобов'язання та дії, які ми вживаємо для її досягнення у невійськовій сфері. Для досягнення цієї мети, пропонується виконання таких цілей:

1. Ліквідація всіх цифрових розривів та прискорення прогресу у досягненні Цілей сталого розвитку;
2. Розширення доступу до цифрової економіки та вигоди від неї для всіх;
3. Сприяння створенню інклюзивного, відкритого, безпечного та захищеного цифрового простору, який поважає, захищає та просуває права людини;
4. Просування відповідальних, справедливих та інтероперабельних підходів до управління даними;
5. Посилення міжнародного управління штучним інтелектом на благо людства [47, с. 1].

Ще однією складовою у діяльності ООН в сфері кібердипломатії є проєкт «Кібердипломатія у Тихому океані» (табл. 2.1), який діяв з червня 2021 року по

травень 2023 року. Цей проєкт мав на меті розвинути потенціал місцевих лідерів, посадовців та переговорників у Тихоокеанському регіоні для участі в кібердискусіях ООН, розуміння поставлених на карту питань та розширення участі своїх країн у кібердипломатії на підтримку вільного та відкритого Інтернету та відповідальної поведінки держав у кіберпросторі. Варто звернути увагу на те, що проєкт також надавав стратегічні консультації щодо Робочої групи відкритого складу (OEWG) та процесів боротьби з кіберзлочинністю, а також підтримуватиме розробку заходів зміцнення довіри [69].

Таблиця 2.2

Концепція проєкту «Кібердипломатія в Тихому океані»

№	Аспекти	Складові
1	Спонсори	Австралія – Міністерство закордонних справ та трогівлі.
2	Виконавці	Незалежний дипломат (Бельгія, Швейцарія, США).
3	Партнери	Незалежний дипломат (Бельгія, Швейцарія, США)
4	Теми та предмети	1. Політика та стратегія кібербезпеки; 2. Стратегії; 3. Міжнародні договори, норми та кібердипломатія; 4. Стандарти кібербезпеки.
5	Регіон	Тихий океан.
6	Країни	1. Австралія; 2. Фіджі; 3. Кірибаті; 4. Науру; 5. Нова Зеландія; 6. Папуа-Нова Гвінея; 7. Самоа; 8. Соломонові острови; 9. Тонга; 10. Тувалу; 11. Вануату.

Джерело: [69]

Розглядаючи діяльність ЄС, варто зазначити, що у червні 2017 року він створив Рамкову інструкцію для спільного дипломатичного реагування ЄС на зловмисну кібердіяльність. Ця інструкція дозволяє Союзу та його державам-членам використовувати всі заходи в рамках Спільної зовнішньої та безпекової політики (СЗПБ), включаючи санкції, якщо це необхідно для запобігання,

протидії, стримування та реагування на зловмисну кібердіяльність, спрямовану на цілісність та безпеку ЄС та його держав-членів [62].

В цьому ж році з'явився інструментарій кібердипломатії ЄС. Це структура, розроблена Європейським Союзом для посилення його здатності запобігати, стримувати та реагувати на зловмисну кібердіяльність, яка може загрожувати його зовнішній безпеці. Цей інструментарій є частиною зусиль ЄС щодо сприяння глобальним, відкритим, стабільним та безпечним кіберопераціям. Він відображає зобов'язання ЄС використовувати дипломатичні, економічні та спільні заходи, що ґрунтуються на верховенстві права, для вирішення складних викликів у кіберсфері. Ключові компоненти Інструментарію кібердипломатії включають дипломатичні заходи, обмежувальні заходи, співпрацю та координацію, розвиток потенціалу та кіберзахист і зовнішні дії (табл. 2.2).

Таблиця 2.3

Ключові компоненти Інструментарію кібердипломатії ЄС

№	Компонент	Зміст
1	Дипломатичні заходи	Інструментарій кібердипломатії ЄС надає Європейському Союзу набір дипломатичних заходів для реагування на кіберзагрози та інциденти, які можуть загрожувати безпеці та стабільності Союзу та його держав-членів. Серед них — засудження кібератак, дипломатичні демарші та міжнародні дискусії для підтримки норм. ЄС прагне стримувати атаки та підтримувати правила у кіберпросторі, акцентуючи на міжнародній співпраці і створенні коаліцій для колективного реагування на загрози. Також підкреслюється участь ЄС у міжнародних форумах для сприяння прозорості та мирному вирішенню конфліктів у кіберсфері.
2	Обмежувальні заходи	Обмежувальні заходи мають вирішальне значення в інструментарії ЄС з кібердипломатії, оскільки вони діють як кіберзахист від діяльності, яка ставить під загрозу інтереси ЄС. Це включає цільові кіберсанкції, такі як заморожування активів і заборона на поїздки для осіб або організацій, відповідальних за кібератаки. Санкції спрямовані на притягнення винних до відповідальності та демонстрацію рішучості ЄС у захисті своїх інтересів.
3	Співпраця та координація	Співпраця та координація є важливими компонентами Інструментарію кібердипломатії ЄС. Це дозволяє державам-членам узгоджувати свої

Продовження табл. 2.3

№	Компонент	Зміст
3	Співпраця та координація	відповіді на кіберзагрози та підвищувати колективну кібербезпеку через обмін розвідувальними даними та кращими практиками.
4	Розвиток потенціалу	Розвиток потенціалу є ключовим елементом Інструментарію кібердипломатії ЄС, метою якого є зміцнення кіберстійкості держав-членів ЄС та третіх країн. Союз надає технічну допомогу, навчання та ресурси для покращення можливостей національних інституцій у запобіганні та реагуванні на кіберзагрози. Зусилля включають розвиток колективного механізму оборони та комунікаційних технологій у ЄС, а також підтримку правової та регуляторної бази для ефективного управління кібербезпекою. Це передбачає допомогу країнам у розробці законів відповідно до міжнародних стандартів.
5	Кіберзахист і зовнішні дії	Інструментарій кібердипломатії ЄС інтегрує кіберзахист у ширші зовнішні дії, підкреслюючи необхідність проактивного та надійного підходу до захисту кіберпростору, особливо в контексті війни між росією та Україною, яка ставить під загрозу міжнародну безпеку. ЄС стратегічно узгоджує цілі кібербезпеки з зовнішньою політикою, забезпечуючи захист ІТ-інфраструктури та соціальних структур від кіберзагроз. Підхід передбачає посилення можливостей кіберзахисту військових і цивільних структур, координацію оборонних зусиль та забезпечення безперервності операцій.

Джерело: [61]

Також важливою є Ініціатива ЄС з кібердипломатії – проєкт, що фінансується Союзом та спрямований на підтримку політики, дослідження, інформаційно-просвітницьку роботу та нарощування потенціалу в галузі кібердипломатії. Метою даного проєкту є визначення можливостей для посилення зближення між ЄС та іншими зацікавленими сторонами щодо застосування чинного міжнародного права в кіберпросторі та розробки кібернорм і заходів зміцнення довіри. В межах співробітництва у контексті Ініціативи, ЄС зосереджується на таких темах:

1. Запобігання конфліктам та просування відповідальної поведінки в кіберпросторі за допомогою міжнародного права, норм та заходів зміцнення довіри;
2. Кіберстійкість та захист критичної інфраструктури;
3. Кіберзлочинність та кримінальне правосуддя в кіберпросторі;
4. Нові та перспективні технології з потенційним руйнівним ефектом [31].

Говорячи про НАТО, основним документом, який регулює його кібердипломатичну діяльність є 14-й Талліннський документ «Кібердипломатія: від концепції до практики». Даний документ Комісії НАТО покликаний сприяти стратегічному діалогу щодо кібербезпеки в Альянсі і за його межами. Він розглядає кібербезпеку з міждисциплінарної точки зору, досліджуючи широке коло питань, в тому числі оцінку кіберзагроз, внутрішні і міжнародні правові дилеми, питання управління, розподіл ролей і обов'язків у кіберсфері, мілітаризацію кіберпростору і технічні питання. Зосереджуючись на найбільш актуальних дискусіях з питань кібербезпеки, Талліннський документ має на меті підтримати створення правової та політичної архітектури, яка б відповідала специфічним викликам кіберпростору. Завдяки своєму перспективному підходу він прагне підвищити обізнаність і спровокувати критичне мислення, необхідне для прийняття обґрунтованих рішень на політичному і стратегічному рівнях [40, с. 3].

Отже, у світлі стрімкої цифровізації та зростаючих кіберзагроз кібердипломатія стає невід'ємною складовою сучасної системи міжнародних відносин і глобальної безпеки. Її динамічний розвиток обумовлений не лише зростанням ризиків у кіберпросторі, а й необхідністю формування спільних підходів до регулювання, захисту прав людини та розбудови довіри між державами. Міжнародні організації, такі як ООН, ЄС та НАТО, продовжують удосконалювати нормативну базу, створювати дієві механізми координації та реагування на кіберінциденти, а також забезпечувати розвиток потенціалу держави у сфері кібербезпеки. Позиція співпраці, обмін кращими практиками й

адаптація до нових викликів, пов'язаних із впровадженням штучного інтелекту, масовим використанням Інтернету речей та хмарних технологій, є пріоритетними напрямками для глобальної кібердипломатичної спільноти. Таким чином, кібердипломатія стає не лише інструментом розв'язання відносин у віртуальному просторі, а й потужним чинником формування нової парадигми міжнародних відносин у ХХІ столітті, де безпека, довіра та багатостороння співпраця є основою глобальної стабільності та процвітання.

РОЗДІЛ 3

КІБЕРБЕЗПЕКА УКРАЇНИ В КОНТЕКСТІ МІЖНАРОДНИХ ВІДНОСИН ТА ДИПЛОМАТІЇ

3.1. Сучасна політика України у галузі кібердипломатії

В епоху стрімкої цифровізації суспільства поняття кібербезпеки та кібердипломатії набувають особливої актуальності. Україна, перебуваючи на передовій лінії гібридної війни, гостро відчуває необхідність не лише у захисті власного кіберпростору, але й у формуванні ефективної кібердипломатії – сукупності інструментів, механізмів і стратегій, спрямованих на забезпечення національних інтересів у глобальному інформаційному середовищі. В умовах постійних зовнішніх кібератак, інформаційних кампаній та спроб дестабілізації суспільства, українська держава змушена невпинно вдосконалювати як технічні, так і дипломатичні засоби захисту, активно залучаючись до міжнародних процесів у сфері кібербезпеки.

Говорячи про кібердипломатію, слід звернути увагу на те, що в Україні її розглядають як використання інструментів дипломатії для забезпечення інтересів держави у кіберпросторі, а також з метою співробітництва з іншими суб'єктами міжнародних відносин. Значний поштовх до розвитку кібердипломатії в Україні дав 2014 рік, коли після Революції гідності та початку військової агресії росії країна стала об'єктом системних кібератак. Зокрема, відомі атаки на урядові портали, електроенергетичну інфраструктуру, банківський сектор, медіа і навіть виборчу інфраструктуру. Ці події довели, що питання кібербезпеки є не лише технічним, а й політичним, вимагаючи активної дипломатичної реакції та міжнародної підтримки.

Одним із ключових кроків на шляху до посилення кібердипломатії стало створення у 2016 році Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (НКЦК РНБО). Центр координує дії всіх державних органів у сфері кібербезпеки, забезпечує обмін інформацією та

оперативне реагування на кіберінциденти. В свою чергу, Міністерство закордонних справ (МЗС) створило спеціальний підрозділ для міжнародного співробітництва у сфері кібербезпеки, що дозволило брати активну участь у міжнародних перемовинах, робочих групах та форумах, присвячених питанням кіберзахисту.

У 2021 році набрала чинності Національна стратегія кібербезпеки України, яка визначила основні напрями розвитку кібербезпеки, підкресливши важливість міжнародної співпраці, участі у глобальних ініціативах та розвитку власної експертизи. Хоча концепція кібердипломатії не згадується у стратегії публічної дипломатії, прийнятій МЗС, Стратегія кібербезпеки України 2021 року передбачала необхідність елементу участі України в міжнародному кіберпросторі та поширення власних інтересів на міжнародних та європейських платформах, включаючи встановлення тісніших контактів з міжнародними зацікавленими сторонами [56].

Починаючи з 2023 року органи державної влади України почали приділяти все більшу увагу кібердипломатії. Так, у липні відбулось засідання НКЦК, на якому було обговорено питання щодо розбудови української кібердипломатії. Слід зазначити, що в ході даного засідання всі учасники обговорення підтримали пропозицію щодо необхідності формування підходів до реалізації заходів щодо подальшого розвитку кібердипломатії за участі МЗС [39, с. 30]. Таким чином, кібердипломатія стала офіційним напрямом діяльності України.

Це дуже важливий крок для нашої країни, адже саме кібердипломатія може стати чудовим інструментом для досягнення своїх зовнішніх інтересів. Для цього потрібно виконати 2 умови: перша – закріплений чіткий розподіл обов'язків між державними органами у сфері кібердипломатії, і друга – план дій з кібердипломатії повинен містити чіткі цілі. Також необхідно виокремити перелік партнерів, з якими потрібно посилити співпрацю. Слід пам'ятати, що кібердипломатія – це сфера, в якій Україна може будувати ефективні та вигідні партнерства, поширювати свої практики та відстоювати і забезпечувати свої національні інтереси в кіберпросторі [9].

Ще одним кроком у сфері кібердипломатії стало започаткування Талліннського механізму (Механізму) – міжнародного формату забезпечення стійкості цифрової інфраструктури України до кіберзагроз. У Талліннському механізмі взяли участь 11 держав: сама Україна, а також Канада, Данія, Естонія, Франція, Німеччина, Нідерланди, Польща, Швеція, Велика Британія та США. В рамках Механізму буде відбуватися координація допомоги Україні для забезпечення національної кібербезпеки, захисту критичної інфраструктури та попередження російської кіберагресії [20]. Щодо самого документу, в ньому описується сфера діяльності Талліннського механізму. Так, проаналізувавши даний документ можна зазначити:

1. Механізм допомагає Україні захищати себе в кіберпросторі та підвищувати довгострокову кіберстійкість;
2. Він виступає координаційним центром для допомоги зі сторони країн-учасниць, при цьому не заважаючи їм діяти окремо або в будь-яких інших ініціативах;
3. Діяльність Механізму поділяється на три основні напрями: короткострокова підтримка, середньострокова розбудова та довгострокова підтримка кібернетичного потенціалу України;
4. Усі дії відбуваються у співпраці з Україною та згідно принципу «нічого про Україну без України»;
5. До роботи також можуть долучатися не лише держави, а й інші бажані суб'єкти міжнародних відносин, такі як приватний сектор, міжнародні організації тощо;
6. Механізм має доволі гнучку структуру, усі рішення приймаються консенсусом, а досвід країн застосовується з метою підвищення ефективності роботи [66].

На актуальність розвитку кібердипломатії в Україні вказує також Законопроект про зміни до Закону «Про дипломатичну службу», поданий на розгляд до Верховної Ради України Президентом Володимиром Зеленським. За його словами, нові норми, введені у Законопроект, повинні зробити систему

української дипломатії більш сучасною та дадуть їй змогу бути більш дієвою, аніж зараз [4]. На даний момент Законопроект готується до другого читання. Слід зазначити, що крім загальних змін певних пунктів Закону, також офіційно вводиться поняття кібердипломатії (Частина 1, ст. 2, п. 5¹) та міжнародного співробітництва у сфері кібердипломатії (Частина 1, ст. 6, п. 8¹ та ст. 7, п. 25) [15, с. 1-2]. Враховуючи запропоновані зміни, актуальним було б створення окремої дипломатичної посади – кібердипломат. Зважаючи на це, під час Міжнародного форуму з кібербезпеки 2024 Секретар РНБО України Олексій Данилов анонсував появу даної посади. «У нашій країні так само скоро з'явиться, я думаю, обов'язково така посада – кібердипломата, тому що це дуже-дуже важливий напрямок боротьби за світло в цьому світі», – повідомив Секретар у своїй промові [29].

15-16 травня 2024 року проходила перша в Україні науково-практична міжнародна конференція з питань кібердипломатії. Метою заходу було обговорення і дослідження кібердипломатії та її впливу на майбутнє міжнародних відносин в умовах швидкого технологічного прогресу. У конференції взяли участь представники суб'єктів забезпечення кібербезпеки, політики, дипломати, науковці та представники профільних навчальних закладів [5]. В ході конференції стало відомо про те, що МЗС почало працювати над розробкою Стратегії кібердипломатії для України. Про це заявив заступник міністра закордонних справ з питань цифрового розвитку, цифрових трансформацій і цифровізації Антон Дем'янішин. За його словами, це пов'язане з тим, що діяльність МЗС неможлива без запровадження сучасних цифрових технологій, що здатні підвищити ефективність роботи дипломатів [8]. Також в ході даної конференції кібердипломатію для України було визначено як важливий інструмент для підтримки стабільності в кіберпросторі, обговорили необхідність його захисту та розглянули питання ролі штучного інтелекту в кібердипломатії, його впливу на ухвалення стратегічних рішень у міжнародних відносинах. Крім того, експерти вказали на важливість впровадження Стратегії кібердипломатії, адже вона враховує прозорість і взаємозв'язок цифрового середовища, важливість співпраці

між країнами, а також обміну досвідом з метою зміцнення кібербезпеки та побудови міцної довіри у кіберпросторі [21].

Наприкінці минулого року, 28 листопада в Дипломатичній академії при МЗС України відбувся науково-практичний круглий стіл «Кібердипломатія: Стратегії та практики для України, Європи та світу». Захід відкрив Антон Демьохін, який наголосив на важливості участі науковців та експертів у формуванні і розвитку української кібердипломатії, а також презентував стратегічні завдання відповідного відділу МЗС. Основні цілі – створення правил поведінки в кіберпросторі, зменшення цифрового розриву, зміцнення глобальної кіберстійкості та розвиток міжнародних партнерств у сфері кібербезпеки. Учасники підтримали проєкт Стратегії кібердипломатії України та домовились надалі його доопрацьовувати. Також обговорювались питання протидії дезінформації, використання кібердипломатії для захисту інтересів України, її роль в економічній та гендерній безпеці, а також можливість впровадження навчальної дисципліни «Основи кібердипломатії» у вишах. Після круглого столу планується публікація матеріалів та статей, що сприятиме подальшому розвитку наукових досліджень і впровадженню практик кібердипломатії в Україні [1].

Отже, формування та розвиток кібердипломатії в Україні є об'єктивною необхідністю для зміцнення національної безпеки, забезпечення захисту державного суверенітету, а також для посилення ролі нашої країни у глобальних процесах. В умовах зростаючих кіберзагроз Україна змушена активно шукати нові підходи до захисту своїх інтересів у цифровому просторі. У цьому контексті особливо важливою є співпраця з іншими державами, зокрема в рамках Талліннського механізму, яка сприяє обміну досвідом і впровадженню передових практик у сфері кібердипломатії. Крім того, Україна впроваджує власні проєкти та ініціативи, що дозволяє їй не лише реагувати на сучасні виклики, а й формувати власний внесок у розвиток міжнародної кібербезпеки. Таким чином, активний розвиток кібердипломатії забезпечує Україні не лише зміцнення внутрішньої безпеки, а й розширює її можливості для ефективної взаємодії на світовій арені.

3.2. Міжнародне співробітництво України у сфері кібербезпеки

Розглядаючи міжнародне співробітництво у сфері кібербезпеки, важливо зазначити, що для України це питання є дуже актуальним, особливо в умовах війни. Україна – держава, що перебуває на передовій кіберконфліктів, а отже особливо гостро відчуває необхідність розвитку ефективної системи кіберзахисту, яка неможлива без тісної співпраці з міжнародною спільнотою. Так, вона активно співпрацює з ЄС, НАТО, США, Словенією та Латвією.

лише у 2024 році Команда реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) при Державній службі спеціального зв'язку та захисту інформації України (Держспецзв'язку) зафіксувала 4315 кіберінцидентів, що на 69,8% більше, ніж 2541 інцидент, зареєстрований попереднього року. Фахівці CERT-UA попереджають про продовження тенденції до зростання кібератак, спрямованих переважно на критичну інфраструктуру України. Ворог не припиняє спроб дестабілізувати Україну за допомогою кібервійни, що свідчить про те, що кіберсфера залишається ключовим полем битви в триваючому конфлікті [36]. Відтак, міжнародне співробітництво у сфері кібербезпеки стало для України не лише фактором посилення власних оборонних можливостей, а й одним із ключових напрямів зовнішньополітичної діяльності та інтеграції у глобальні безпекові структури.

На жаль, українські фахівці з кібербезпеки не здатні самотужки впоратися з усіма викликами, і саме тому існує необхідність співробітництва з іншими країнами та організаціями. З цієї причини ми продовжуємо активно розбудовувати міжнародну співпрацю. Так, лише за останні 2 роки Україна досягла багато нового у даній сфері, а саме:

1. У листопаді 2023 року було підписано Робочу Угоду про співпрацю з Європейською агенцією кібербезпеки (ENISA);
2. 7-8 лютого 2024 року в Києві відбувся перший міжнародний форум з кібербезпеки 2024, темою якого була стійкість під час кібервійни;

3. У серпні 2024 року відбулись: шостий раунд Кібердіалогу Україна-США, зустріч представників Національного координаційного центру кібербезпеки (НКЦК) з Посольством Японії та Японським агентством міжнародного співробітництва (JICA), а також підписання Меморандуму про співпрацю у сфері кібербезпеки та кіберзахисту між Держспецзв'язку та Міністерством оборони Латвії [18, с. 25-26].

Необхідно зазначити, що метою міжнародного співробітництва України у сфері забезпечення кібербезпеки в першу чергу є зміцнення взаємної довіри між акторами (держави, міжнародні урядові та неурядові організації, транснаціональні корпорації тощо) у сфері кібербезпеки; вироблення спільних підходів до протидії кіберзагрозам; об'єднання зусиль у розслідуванні та запобіганні кіберзлочинам; недопущення використання кіберпростору в протиправних цілях; виконання Україною зобов'язань в рамках укладених міжнародних договорів у питанні співробітництва у сфері кібербезпеки з іншими державами, їх збройними силами, правоохоронними органами і спеціальними службами, міжнародними організаціями; а також з метою оптимізації надання міжнародної технічної допомоги [12, с. 131]. Серед основних партнерів України, з якими вона активно співпрацює у даній сфері є міжнародні організації, фонди та країни.

Розглядаючи міжнародне співробітництво України та ЄС, варто зазначити, що воно постійно розвивається і поглиблюється, особливо після повномасштабного вторгнення росії в 2022 році. Ця ситуація значно підвищила важливість кібербезпеки для обох сторін, оскільки кібератаки стали одним із основних інструментів агресії. В результаті, Україна вже стала частиною екосистеми кібербезпеки ЄС, хоча процес інтеграції досі триває і вимагає адаптації нормативно-правової бази, розвитку інституцій та подальшої міжнародної співпраці. Хоча процес інтеграції досі триває, він вимагає адаптації нормативно-правової бази, розвитку інституцій та подальшої міжнародної співпраці.

Особливо важливим є те, що ЄС активно підтримує Україну в боротьбі з кіберзагрозами, які походять з боку рф. Так, серед заходів допомоги ЄС Україні є

доступ до Cyber Rapid Response Team (CRRT), обмін розвідувальною інформацією, технічна допомога, кібердіалоги між Україною та спільне реагування на кібератаки та введення санкцій проти хакерів з росії (табл. 3.1).

Таблиця 3.1

Підтримка ЄС у боротьбі з кіберзагрозами

№	Аспекти підтримки ЄС	Зміст
1	CRRT	Вперше в історії ЄС сформовано міжнародну команду швидкого реагування на кібератаки, яка допоможе Україні виявляти загрози та здійснювати цифрову криміналістику.
2	Обмін розвідувальною інформацією	Україна співпрацює з європейськими центрами кібербезпеки, що в свою чергу дозволяє швидко реагувати на нові загрози.
3	Технічна допомога	ЄС фінансує кіберзахист урядових мереж України, зокрема надає сервери, захищені маршрутизатори та програмне забезпечення для моніторингу загроз.
4	Кібердіалоги	Регулярні зустрічі між Україною та ЄС дозволяють узгодити стратегії, санкційну політику та майбутні заходи у сфері забезпечення кібербезпеки.
5	Спільне реагування	ІТ-фахівці з кількох європейських країн у квітні 2022 року допомогли зупинити атаку вірусу Industroyer2, що значно підвищило ефективність міжнародної технічної співпраці.
6	Санкції проти хакерів з рф	Важливим аспектом стали санкції ЄС проти російських хакерів. Зокрема це включало персональні санкції проти офіцерів ГРУ та ФСБ, які були причетні до атак; замороження активів російських кіберзлочинців та обмеження доступу до європейських фінансових систем; санкції проти груп Evil Corp та Trickbot, що значно ускладнило їхню діяльність; створення рамкової програми санкцій проти гібридних загроз, яка дозволила ЄС ввести обмеження проти хакерських груп та організацій, які атакують критичну інфраструктуру або поширюють дезінформацію.

Джерело: [6, с. 5].

Також необхідно зазначити, що зовсім нещодавно Україна та ЄС підписали меморандум про співпрацю у сфері кібербезпеки. Так, під час проведення 11-12 березня цього року Київського Міжнародного Форуму з кібербезпеки 2025 було офіційно оформлено стратегічне партнерство з Європейським Центром кіберкомпетентності (ЕССС). Даний документ передбачає співпрацю, що буде

орієнтована на створення механізмів швидкого реагування на кіберінциденти та підвищення захисту критично важливих об'єктів. Сторони також узгодили спільні дії щодо моніторингу, аналізу та запобігання кіберзагрозам, що допоможе зміцнити кіберстійкість як України, так і Європейського Союзу в умовах зростаючих кіберризиків [3]. Ці кроки показують, що для України і ЄС міжнародне співробітництво у сфері кібербезпеки є важливою частиною їхньої зовнішньої політики.

Ще одним партнером України в сфері кібербезпеки є НАТО. Першими кроками в даному співробітництві стало створення Робочої підгрупи з питань кіберзахисту у 2008 році. Це була ініціатива Служби безпеки України (СБУ) в межах Спільної робочої групи Україна – НАТО з питань воєнної реформи. Це стало першим кроком до розробки засад взаємодії між сторонами у сфері кібербезпеки, запровадження механізмів консультацій та швидкого обміну інформацією про кібератаки національного масштабу, а також розробки критеріїв оцінки кіберзагроз. Відтоді міжнародне співробітництво у сфері кібербезпеки між Україною та Альянсом значно розширилось [7, с. 204].

Наступним важливим кроком у зміцненні співпраці між Україною та НАТО стало підписання Меморандуму про домовленість між Урядом України та Організацією НАТО із зв'язку та інформації. Цей документ, підписаний 16 листопада 2022 року, стосується співробітництва в питаннях консультацій, управління, зв'язку, розвідки, спостереження та рекогносцировки в рамках програми НАТО «Партнерство заради миру». Згідно з Меморандумом, новими цілями співробітництва між Україною та НАТО стали підтримка реформ і трансформації сектору безпеки і оборони, а також покращення взаємного сумісництва між Збройними Силами України (ЗСУ) та силами НАТО. Це стало особливо актуальним у світлі сучасних викликів, з якими стикається Україна. З цією метою на обидві сторони було покладено зобов'язання обмінюватися знаннями в рамках партнерства, що дозволить ефективніше реагувати на загрози та підвищити рівень підготовки військових. Крім того, документ визначає сфери спільної діяльності, які сприятимуть більш тісній інтеграції України в європейські

та трансатлантичні структури безпеки. [14]. Також було окреслено напрями співробітництва між Україною та НАТО у сфері кібербезпеки у короткостроковій та середньостроковій перспективах. Це включає в себе спільні навчання, обмін інформацією про кіберзагрози та розвиток інфраструктури кіберзахисту, що є критично важливим для забезпечення національної безпеки України (табл. 3.2)

Таблиця 3.2

Напрями співробітництва між Україною та НАТО

№	Короткострокова перспектива	Середньострокова перспектива
1	Підтримка впровадження сучасних інформаційних технологій, комунікаційних сервісів (електронна передача повідомлень, відеотелеконференції, IP-телефонія, веб-сервіси, послуги збереження інформації і загального доступу до неї), а також протоколів та обробки даних у системі управління військами ЗСУ.	Допомога у визначенні потреб України для покращення її спроможностей в оборонному, оперативному та логістичному плануванні.
2	Підтримка в оцінці та запровадженні базових і функціональних служб, а також інформаційних технологій для обробки даних та їх відображення в системі управління військами ЗСУ.	Визначення і підтримка потреб України щодо підготовки, особливо в аспекті комплексних завдань модернізації та досягнення взаємосумісності систем зв'язку та інформації.
3	Підтримка у придбанні комунікаційних та інформаційних сервісів згідно з напрямами співробітництва, зазначеними у цьому Меморандумі, для ЗСУ, керуючись принципами та правилами закупівель товарів і послуг НАТО.	

Джерело: [14]

Ще одним вагомим кроком стало те, що Україна у 2024 році вперше офіційно взяла участь у навчаннях з кібероборони Locked Shields 2024, які були організовані Об'єднаним центром передових технологій з кібероборони НАТО (NATO CCDCOE). Ці щорічні навчання виходять за рамки традиційних кібервправ, залучаючи експертів з різних галузей для протидії кіберзагрозам.

Сильна сторона цих навчань полягає в комплексному підході, який поєднує технічні навички зі стратегічними, юридичними та комунікаційними знаннями для розробки різнобічної оборонної стратегії. Учасників закликають використовувати свої колективні навички, сприяючи створенню середовища, де співпраця є ключем до подолання складних викликів кібербезпеки [22]. Таким чином, ми можемо бачити, що співпраця між Україною та НАТО постійно розвивається. Україна почала брати участь у спільних навчаннях з Альянсом, що також показує важливість співробітництва для обох сторін.

Також слід звернути увагу на міжнародне співробітництво у сфері кібербезпеки між Україною та USAID, яке було започатковане у 2022 році через проєкт «Кібербезпека критично важливої інфраструктури України». Метою даного проєкту є посилення стійкості критичної інфраструктури України до кібератак шляхом формування довіри та співпраці між зацікавленими сторонами, які представляють органи влади, приватний бізнес, наукову спільноту та громадянське суспільство. Даний проєкт охоплює низку важливих складових, а саме:

1. Зміцнення кіберстійкості України за рахунок тісної співпраці з урядом України, зокрема Міністерство цифрової трансформації України, Державна служба спеціального зв'язку та захисту інформації України та Рада національної безпеки і оборони України;
2. Формування кадрового потенціалу України у сфері кібербезпеки;
3. Підтримку університетів для збільшення фахівців із кібербезпеки та покращення якості їхнього навчання;
4. Підвищення кваліфікації експертів із кібербезпеки через навчальні та практичні тренінги;
5. Налагодження контактів між українськими закладами вищої освіти із міжнародною академічною спільнотою;
6. Розбудова ринку кібербезпеки;
7. Підтримка запуску оновленого державного центру кіберзахисту держспецзв'язку [16].

Хоча діяльність USAID припинилася на початку цього року, проєкт досі продовжує своє існування та діяльність.

Окрім міжнародних урядових та неурядових організацій, Україна також активно співпрацює з іншими країнами. Наприклад, в липні 2022 року між Україною та Словенією було підписано Меморандум про взаєморозуміння. Даний документ має дати можливість об'єднання зусиль з метою розроблення та розповсюдження нових технологій кібербезпеки, а також напрацювання спільних підходів у протистоянні кіберагресії. Слід також зазначити, що Меморандум передбачає співробітництво між країнами у таких напрямках:

1. Підвищення взаємної присутності України та Словенії у міжнародних та регіональних організаціях і форумах з кіберзахисту;
2. Гармонізація законодавства і двостороннього правового та правоохоронного співробітництва у сфері боротьби з кіберзлочинністю та кібертероризмом;
3. Навчання експертів у сфері кібербезпеки та кіберзахисту;
4. Проведення досліджень у сфері кіберзахисту;
5. Обмін інформацією про кіберінциденти, способи виявлення вразливостей та реагування на кіберзагрози [24].

Ще одним партнером України є Польща, з якою 22 серпня того ж року було підписано Меморандум про взаєморозуміння у сфері кіберзахисту. Даний меморандум має посилити спільну боротьбу з кіберзлочинами та забезпечити оперативний та ефективний обмін інформацією. Також Україна та Польща спільно наращуватимуть присутність на міжнародній арені. Це включає в себе участь у міжнародних організаціях, виступи на конференціях з кібербезпеки, багатосторонні формати діалогу та консультації, а також запобігання поширенню шейків та дезінформації в інформаційному просторі [26].

Не слід забувати і про США. Так, в серпні 2024 року у Києві відбувся шостий раунд щорічного кібердіалогу Україна – США. В межах цього діалогу сторони обговорили різноманітні питання, що стосувалися кібербезпеки, а також шляхи подальшого співробітництва. Також американська делегація зазначила, що її

зобов'язання щодо підтримки України в забезпеченні стійкого кіберпростору залишаються непохотними. Такі заяви є прямою відповіддю США на агресію зі сторони рф. Також було обговорено сучасний ландшафт кіберзагроз, захист критичної інфраструктури та чутливих даних, а також інновації у сфері кібербезпеки та ІКТ, зв'язку і безпеки та конкурентоспроможності українських ІТ та телекомунікацій [25].

Також за декілька днів після кібердіалогу між Україною і США, Україна разом з Латвійською Республікою підписали Меморандум про взаєморозуміння між Міністерством оборони Латвійської Республіки та Адміністрацією Держспецзв'язку у сфері кібербезпеки та кіберзахисту. Враховуючи постійну і міцну підтримку від Латвії, варто зазначити, що дана подія стала черговим підтвердженням міцних та дружніх відносин між країнами. Згідно з Меморандумом, Україна та Латвійська Республіка зобов'язуються співпрацювати між собою у таких напрямках:

1. Обмін інформацією про кіберінциденти та кібератаки;
2. проведення спільних навчань та тренінгів;
3. Реалізація спільних проєктів із досліджень у сфері кібербезпеки та кіберзахисту;
4. Обмін досвідом та кращими практиками з питань протидії кіберзагрозам [2].

Слід також звернути увагу на те, що на початку травня цього року в межах конференції InfoSec Ukraine 2025, що пройшла в Києві, відбувся круглий стіл «Співпраця у сфері кібербезпеки та захисту критичної інфраструктури: країни Північної Європи та Україна». За результатами круглого столу було утворено Північноєвропейсько-українську робочу групу з кібербезпеки та захисту критичної інфраструктури. Дана група буде функціонувати як платформа для міжнародного співробітництва та розбудови інституційного потенціалу країн, а також з метою реалізації інноваційних проєктів. Щодо напрямів співробітництва, то вони включатимуть:

1. Розвиток децентралізованої інфраструктури кібербезпеки;

2. Розбудова спроможностей та формування професійної спільноти;
3. Регуляторна та правова гармонізація з Європейським Союзом;
4. Захист критичної інфраструктури;
5. Технічне співробітництво та інновації;
6. Навчання та обмін досвідом;
7. Залучення донорів та розробка проєктів [23].

Не зважаючи на активне міжнародне співробітництво України з міжнародними організаціями, фондами та іншими країнами, досі існує багато викликів та перешкод для забезпечення безпечного кіберпростору. Світ знаходиться в стані першої в світі кібервійни, основним полем якої є Україна. Швидкий розвиток кіберзагроз, їхня еволюція та зміна, недостатність кваліфікованих спеціалістів та вразливість критичної інфраструктури та державних сервісів – все це робить реагування на кіберзагрози та їх попередження все менш ефективним. В свою чергу, подальше поглиблення міжнародного співробітництва, навчання та залучення висококваліфікованих спеціалістів, а також адаптація систем забезпечення кібербезпеки до нових умов у кіберпросторі зможуть значно мінімізувати негативний вплив кіберзлочинів на державу.

ВИСНОВКИ

Дослідивши тему «Кібербезпека як новий вимір міжнародних відносин та дипломатії» можемо зробити такі висновки:

У сучасному світі кіберпростір за рівнем важливості і стратегічного значення не поступається фізичному простору. Це зумовлює зростання актуальності питань його безпеки для держав, міжнародних організацій та приватного сектору. Кібербезпека є однією з визначальних складових сучасної системи міжнародних відносин та дипломатії. Оскільки це відносно нове поняття, то не існує єдиного визначення цього терміну. Загалом, її теоретичні основи ґрунтуються на цілісному підході до захисту інформаційного простору, інфраструктури та користувачів від різноманітних кіберзагроз, які невпинно трансформуються й ускладнюються у відповідь на динамічний розвиток цифрових технологій.

Взаємодія між державами, що включає створення спільних проєктів, розробку міжнародних правил і стандартів, а також участь у спеціалізованих ініціативах, стає визначальним чинником для посилення глобальної кібербезпеки. Сутність цього процесу полягає у розумінні, що жодна країна, незалежно від рівня власного технічного розвитку чи ресурсів, не здатна самотійно ефективно протидіяти зростаючим загрозам кібератак і кіберзлочинності. Глобальний порядок кібербезпеки та Будапештська конвенція є ключовими факторами, які визначають принципи міжнародного співробітництва у сфері кібербезпеки. Також не слід забувати про міжнародні організації, зокрема ООН, ЄС, НАТО, які відіграють роль ключових платформ для обміну досвідом, координації спільних дій та формування узгодженої політики у сфері кіберзахисту, що дозволяє ефективніше реагувати на виклики цифрової епохи.

Сучасна дипломатія перебуває у процесі трансформації, тому що змушена адаптуватися до умов, де питання інформаційної безпеки, захисту критичної інфраструктури та реагування на кіберінциденти стали невід'ємною частиною міжнародної співпраці. Це призвело до розширення функціоналу дипломатичних місій, які тепер займаються не тільки політичними питаннями, а й технічними аспектами кібербезпеки. Особливої ваги набуває потреба у розробці єдиних

підходів до регулювання поведінки в кіберпросторі, організації регулярного обміну інформацією, а також забезпечення взаємної підтримки між країнами у випадках масштабних кібератак.

Кібердипломатія стала новою формою співпраця у світі. Суть цього явища полягає у спільному виробленні норм і правил поведінки у кіберпросторі, запобіганні виникненню кібервійн, створенні міжнародних механізмів координації та поглибленні довіри між державами. Кібердипломатія інтегрує як традиційні інструменти дипломатії, так і сучасні цифрові технології, зокрема використання соціальних мереж для комунікації та просування національних інтересів у глобальному інформаційному просторі. Провідні міжнародні організації відіграють у цьому процесі важливу роль. Вони приймають нові стратегії та концепції, що регулюють діяльність в галузі кібердипломатії.

В умовах гібридної війни та постійних кібератак розвиток кібердипломатії став одним із основних пріоритетів державної політики України. Впровадження ефективних елементів кібердипломатії дає можливість Україні не лише забезпечувати захист власного інформаційного простору, а й виступати активним гравцем на міжнародній арені. Створення спеціалізованих установ, участь у міжнародних ініціативах та програмах з підвищення кваліфікації фахівців сприяють розвитку національної системи кібербезпеки.

Міжнародне співробітництво України у сфері кібербезпеки є одним із ключових чинників її стійкості в сучасному цифровому світі. Україна вже має значний практичний досвід у протидії масштабним кібератакам, що робить її цінним партнером для інших держав і міжнародних організацій. Так, Україна активно співпрацює зокрема з країнами ЄС, США та НАТО. Участь у спільних проєктах, постійний обмін досвідом, впровадження новітніх технологій та міжнародних стандартів, а також модернізація законодавства дозволяють нашій державі не лише ефективно захищати власні національні інтереси, а й робити вагомий внесок у зміцнення глобальної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Антон Демьохін відкрив науково-практичний круглий стіл «Кібердипломатія: Стратегії та Практики для України, Європи та Світу». *Міністерство закордонних справ України*. URL: <https://surli.cc/rklhvm> (дата звернення: 20.04.2025).
2. Держспецзв'язку та Міністерство оборони Латвії підписали Меморандум про співпрацю у сфері кібербезпеки та кіберзахисту. *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://surli.cc/tmmgug> (дата звернення: 23.04.2025).
3. Деркач О. Україна та ЄС підписали меморандум про співпрацю в сфері кібербезпеки. *PaySpace Magazine*. URL: <https://surli.cc/mohtgq> (дата звернення: 21.04.2025).
4. Завдяки новому законодавству українські дипломати матимуть більше інструментів для реалізації цілей нашої держави – Президент. *Офіційне інтернет-представництво Президента України*. URL: <https://surli.cc/tquwtb> (дата звернення: 18.04.2025).
5. За сприяння НКЦК відбулася Перша науково-практична міжнародна конференція з питань кібердипломатії. *Рада національної безпеки і оборони України*. URL: <https://www.mbo.gov.ua/ua/Diialnist/6884.html> (дата звернення: 19.04.2025).
6. Костюченко Я. М. Співпраця України та ЄС у сфері кібербезпеки: механізми боротьби з кіберзлочинністю. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2025. № 15. URL: <https://doi.org/10.54929/2786-5746-2025-15-01-10> (дата звернення: 21.04.2025).
7. Ларіончева Н. Міжнародна Співпраця У Сфері Кібербезпеки. *Вісник Прикарпатського університету. Серія: Політологія*. 2025. № 20. С. 201–207. URL: <https://doi.org/10.32782/2312-1815/2025-20-24> (дата звернення: 21.04.2025).

8. МЗС розробляє Стратегію кібердипломатії для України. *Головні новини з України сьогодні - Kyiv Post*. URL: <https://surli.cc/gumndn> (дата звернення: 19.04.2025).
9. Омеляненко В. Не лише навчатися, але й навчати: що забезпечує успіхи кібердипломатії України. *Європейська правда*. URL: <https://surl.li/rcevgm> (дата звернення: 18.04.2025).
10. Пасічна В. Кібердипломатія Та Її Вплив На Інформаційне Суспільство. *Цифрова дипломатія України: синергія реального і віртуального* : 36. тез, м. Львів, 24 листоп. 2023 р. Львів, 2023. С. 79–81. URL: <https://surl.li/gikhla> (дата звернення: 11.04.2025).
11. Петькун С. М., Верховцева І. Г. «Цифрова Дипломатія» Та «Кібердипломатія»: Поняттєві Аспекти. *Теоретико-Прикладні Аспекти Розвитку Цифрової Держави В Україні* : тези доп., 14 лист. 2024, Київ, 2024. С. 300–303. URL: <https://surl.li/vjzsmz> : 13.04.2025).
12. Поляков О. М. Активізація Міжнародної Співпраці У Сфері Забезпечення Кібербезпеки: Шляхи Удосконалення В Реаліях Сьогодення. *Правова Інформатика*. 2021. № 2. С. 129–138. URL: <https://surli.cc/fufwlt> (дата звернення: 21.04.2025).
13. Поляков О. М. Кібердипломатія Як Важливий Напрямок Міжнародно-Правового Співробітництва В Умовах Режиму Воєнного Стану. *New Ukrainian Law*. 2025. № 6. С. 70–76. URL: <https://doi.org/10.51989/nul.2024.6.10> (дата звернення: 13.04.2025).
14. Про домовленість між Урядом України та Організацією НАТО із зв'язку та інформації стосовно співробітництва з питань консультацій, управління, зв'язку, розвідки, спостереження та рекогносцировки в рамках програми НАТО «Партнерство заради миру»: Меморандум від 16.11.2022 № 950_001-22. URL: https://zakon.rada.gov.ua/laws/show/950_001-22#Text (дата звернення: 22.04.2025).
15. Проект Закону про внесення змін до Закону України «Про дипломатичну службу» щодо вдосконалення проходження дипломатичної

служби. 2023. 13 с. URL: <https://itd.rada.gov.ua/billInfo/Bills/pubFile/2136252> (дата звернення: 19.04.2025).

16. Проєкт «USAID в Україні». *Національний технічний університет "Дніпровська політехніка"*. URL: <https://bit.nmu.org.ua/usaidd/> (дата звернення: 22.04.2025).

17. Про Основні Засади Забезпечення Кібербезпеки України: Закон України Від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#text> (дата звернення: 06.04.2025).

18. Річний Аналітичний Огляд. Жовтень 2023 -- Листопад 2024. Нац. Координац. Центр Кібербезпеки. 32 с. URL: <https://surli.cc/jibefa> (дата звернення: 20.04.2025).

19. Стратегічна Концепція НАТО – 2022 : Концепція Від 29.06.2022. URL: <https://surli.li/vcijmj> (дата звернення: 10.04.2025).

20. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі. *Міністерство закордонних справ України*. URL: <https://surli.li/rwmgko> (дата звернення: 18.04.2025).

21. У Києві відбулась перша науково-практична міжнародна конференція з питань кібердипломатії. *Міністерство закордонних справ України*. URL: <https://surli.cc/ecbkux> (дата звернення: 20.04.2025).

22. Україна візьме участь у навчаннях з кібероборони NATO CCDCOE Locked Shields. *Рада національної безпеки і оборони України*. URL: <https://www.rnbo.gov.ua/ua/Diialnist/6854.html> (дата звернення: 22.04.2025).

23. Україна та країни Скандинавії працюватимуть над підвищенням стійкості до кібер- та гібридних загроз – створено робочу групу. *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://surli.cc/jzfbrz> (дата звернення: 23.04.2025).

24. Україна та Словенія посилюють співробітництво у сфері кіберзахисту. *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://surli.cc/hodjhl> (дата звернення: 22.04.2025).

25. Україна та США провели Шостий раунд Кібердіалогу. *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://surli.cc/ejeaga> (дата звернення: 23.04.2025).
26. Уряди України та Польщі підписали меморандум про співпрацю у сфері кіберзахисту. *Урядовий Портал*. URL: <https://surli.cc/djmscg> (дата звернення: 23.04.2025).
27. Що Таке Кібербезпека? Захисний Комплекс Microsoft. *Microsoft – AI, Cloud, Produktivität, Computing, Gaming Und Apps*. URL: <https://surli.li/jirzam> (дата звернення: 05.04.2025).
28. Abbakumova D. Cyber Challenges And Modern Diplomacy. *News*. URL: <https://surli.li/myolur> (дата звернення: 12.04.2025).
29. 10 панельних дискусій, понад 35 доповідей експертів: У Києві відбувся Міжнародний форум з кібербезпеки 2024. *Рада національної безпеки і оборони України*. URL: <https://www.rnbo.gov.ua/ua/Diialnist/6780.html> (дата звернення: 19.04.2025).
30. Abbakumova D. Global Challenges - Diplomacy Today. *Global Challenges*. URL: <https://surli.lu/nntdac> (дата звернення: 14.04.2025).
31. About: EU Cyber Direct. *Horizon*. URL: <https://eucyberdirect.eu/about> (дата звернення: 17.04.2025).
32. Ajith. What Are The Main Components Of Cybersecurity?. *Digitdefence*. URL: <https://surli.li/oxufhb> (дата звернення: 07.04.2025).
33. Barrinha A. Cyber-Diplomacy: The Emergence Of A Transient Field. *The Hague Journal Of Diplomacy*. 2024. С. 1–28. URL: <https://doi.org/10.1163/1871191x-bja10183> (дата звернення: 13.04.2025).
34. BDO Digital. Чотири Елементи Сильної Стратегії Кібербезпеки. *Міжнародна Аудиторська Компанія BDO*. URL: <https://surli.li/wflnfc> (дата звернення: 07.04.2025).
35. Budapest Convention On Cybercrime: Convention Від 23.11.2001 № 185. URL: <https://rm.coe.int/1680081561> (дата звернення: 07.04.2025).

36. CERT-UA recorded 4,315 cyber incidents in 2024. *State Service of Special Communications and Information Protection of Ukraine*. URL: <https://surli.cc/nfoxni> (дата звернення: 20.04.2025).
37. Committee On National Security Systems (CNSS) Glossary. 4009-Те Вид. 2015. 165 С. URL: <https://surli.lt/cgttfo> (дата звернення: 05.04.2025).
38. Cyber Defence Pledge. *North Atlantic Treaty Organization*. URL: https://www.nato.int/cps/en/natohq/official_texts_133177.htm (дата звернення: 09.04.2025).
39. Cyber Digest. Нац. Координац. Центр Кібербезпеки, 2023. 43 с. URL: <https://surli.li/limavi> (дата звернення: 17.04.2025).
40. Cyber Diplomacy: From Concept to Practice: Tallinn Paper № 14. URL: <https://surli.lu/rklyci> (дата звернення: 17.04.2025).
41. Cyber Security Challenges Involved In Protecting Sensitive Diplomatic Data / The European Institute For International Relations. 2023. URL: <https://surli.li/ilduwo> (дата звернення: 14.04.2025).
42. Cyberdiplomacy / R. T. Lanciero Та Ін. Lisboa: Instituto Da Defesa Nacional, 2024. 8 С. URL: <http://hdl.handle.net/10400.26/52415> (дата звернення: 13.04.2025).
43. Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace: Strategy Від 07.02.2013. URL: <https://surli.li/imvwec> (дата звернення: 08.04.2025).
44. Dashboard - Eurepos: European Repository Of Cyber Incidents. *Eurepos: European Repository Of Cyber Incidents*. URL: <https://eurepos.eu/dashboard/> (дата звернення: 05.04.2025).
45. Essential Functions Of A Cybersecurity Program / S. Akridge Та Ін. ISACA. URL: <https://surli.li/zufizs> (дата звернення: 07.04.2025).
46. Global Cybersecurity Agenda (GCA). *ITU*. URL: <https://www.itu.int/en/action/cybersecurity/pages/gca.aspx> (дата звернення: 08.04.2025).

47. Global Digital Compact: Compact від 22.09.2024 № A/79/L.2. URL: <https://surl.li/vkjrhl> (дата звернення: 15.04.2025).
48. Global Digital Compact. *United Nations Office for Digital and Emerging Technologies*. URL: <https://surl.li/egqhcj> (дата звернення: 15.04.2025).
49. Global POC directory established by OEWG on ICT security | Digital Watch Observatory. *Digital Watch Observatory*. URL: <https://surl.li/ovekfg> (дата звернення: 15.04.2025).
50. ISACA Glossary: Glossary. 159 С. URL: <https://surl.li/gwjwlv> (дата звернення: 06.04.2025).
51. Laying Down Measures For A High Common Level Of Cybersecurity At The Institutions, Bodies, Offices And Agencies Of The Union: Regulation Від 13.12.2023. URL: https://eur-lex.europa.eu/legal-content/en/txt/?uri=oj:l_202302841 (дата звернення: 09.04.2025).
52. Kleinwächter W. UN Cyberdiplomacy I: PoC, Cybercrime and the Global Digital Compact. *CircleID - Breaking Internet News, Opinions and Blogs*. URL: <https://circleid.com/posts/un-cyber-diplomacy-poc> (дата звернення: 15.04.2025).
53. KUMAR A. Cyber Diplomacy - The Concept, Evolution and its Applicability. *International Journal of Cyber Diplomacy*. 2022. Т. 3. С. 23–32. URL: <https://doi.org/10.54852/ijcd.v3y202203> (дата звернення: 12.04.2025).
54. Kaloudis M. Digital Sovereignty As A Weapon Of Diplomacy In Cyber Warfare In Democracies. *National Security In The Digital And Information Age*. URL: <https://www.intechopen.com/chapters/1175430> (дата звернення: 12.04.2025).
55. Leung M. Cyber Security Challenges In International Relations: State Responses And Global Cooperation. *International Journal Of Open Publication And Exploration*. 2015. Т. 3, № 2. С. 13–19. URL: <https://surl.li/fqhebg> (дата звернення: 10.04.2025).
56. Omelianenko V. EU's and Ukraine's approaches to digital diplomacy in the geopolitics of technologies: Research. 2023. 20 с. URL: <https://surli.cc/djasvb> (дата звернення: 17.04.2025).

57. Overview Of Cybersecurity Information Exchange: Recommendation Від 20.04.2011 № ITU-T X.1500. URL: <https://surl.li/pkyegx> (дата звернення: 06.04.2025).
58. Painter C. Diplomacy in Cyberspace. *American Foreign Service Association*. URL: <https://afsa.org/diplomacy-cyberspace> (дата звернення: 11.04.2025).
59. Rehman S., Rassias M. Security Challenges In The 21st Century: Addressing Cybersecurity Threats In International Diplomacy. 2024. URL: <https://doi.org/10.13140/rg.2.2.18074.15046> (дата звернення 14.04.2025).
60. Resilience, Deterrence And Defence: Building Strong Cybersecurity For The EU: Strategy Від 13.09.2017. URL: <https://surl.li/jxnaoy> (дата звернення: 08.04.2025).
61. Sadoian L. The EU Cyber Diplomacy Toolbox: Shaping Global Cybersecurity Standards | UpGuard. *Compliance and Regulations*. URL: <https://www.upguard.com/blog/eu-cyber-diplomacy-toolbox> (дата звернення: 16.04.2025).
62. Sanctions against cyber-attacks. *European Council*. URL: <https://surl.li/xqzudv> (дата звернення: 16.04.2025).
63. Schjøberg S. Report Of The Chairman Of HLEG. Moss, 2008. 21 С. URL: <https://surl.li/tzhptf> (дата звернення: 08.04.2025).
64. Security And Privacy Controls for Information Systems And Organizations. 2020. 492 С. URL: <https://doi.org/10.6028/nist.sp.800-53r5> (дата звернення: 06.04.2025).
65. Stevens T., Burton J. НАТО І Стратегічна Конкуренція В Кіберпросторі. *NATO Review*. URL: <https://surl.li/xkujmt> (дата звернення: 09.04.2025).
66. Tallinn Mechanism: Statement. URL: <https://surli.cc/yptbba> (дата звернення: 18.04.2025).
67. The EU's Cybersecurity Strategy For The Digital Decade: Strategy Від 16.12.2020. URL: <https://surl.lu/gvqzbs> (дата звернення: 09.04.2025).

68. Top 5 Cyber Security Challenges. *Sentinelone*. URL: <https://surl.li/nymeze> (дата звернення: 05.04.2025).
69. UN Cyber Diplomacy in the Pacific - Cybil Portal. *Homepage - Cybil Portal*. URL: <https://cybilportal.org/projects/un-cyber-diplomacy-in-the-pacific/> (дата звернення: 16.04.2025).
70. United Nations Convention Against Cybercrime: Convention Від 24.12.2024 № 79/243. URL: <https://surl.li/oeqcaу> (дата звернення: 10.04.2025).
71. What Is Cyber Diplomacy?. *The EU Cyber Diplomacy Toolbox: An In-Depth Analysis Of Cyber Diplomacy*. URL: <https://surl.li/rixryg> (дата звернення: 12.04.2025).
72. Windear. Cyber Security Threats In International Relations: Navigating A Digital Battlefield - Windear Consulting. *Windear Consulting*. URL: <https://surl.li/qmrvey> (дата звернення: 11.04.2025).
73. Zinchenko O. Cyber Security In International Relations: Risks And Prospects. *Eximia*. 2025. Т. 14, № 1. С. 1–20. URL: <https://surl.lu/odtgyz> (дата звернення: 10.04.2025).
74. Zishan A., Muhammad Y. The Evolution Of Diplomacy In The Digital Age: Opportunities And Challenges. 2024. URL: <https://doi.org/10.13140/rg.2.2.16396.42889> (дата звернення 11.04.2025).

АНОТАЦІЯ

Самойленко Т.О. Кібербезпека як новий вимір міжнародних відносин. Здобувач освіти освітнього ступеня «бакалавр» спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» освітньо-професійної програми «Міжнародні відносини і геополітична безпека». Державний університет «Житомирська політехніка», 2025.

У першому розділі висвітлено питання концептуальних основ кібербезпеки, такі як: причини виникнення, визначення, мету, елементи забезпечення та складові компоненти. Визначено необхідність міжнародного співробітництва у сфері кібербезпеки, а також нормативно-правові акти, що регулюють дану діяльність в межах таких міжнародних організацій, як ЄС, НАТО та ООН.

У другому розділі висвітлено глобальні виклики, з якими стикається дипломатія, та їхній вплив на неї. Розглянуто поняття кібердипломатії, її суть, а також кібердипломатію у діяльності провідних міжнародних організацій світу, а саме: ООН, ЄС та НАТО.

У третьому розділі висвітлено сучасну політику України у галузі кібердипломатії, зокрема нормативно-правові акти та ініціативи, покладені в основу функціонування кібердипломатії в країні. Також розглянуто особливості міжнародного співробітництва України з ЄС, НАТО, США, Словенією та Республікою Латвія у сфері кібербезпеки.

Ключові слова: кібербезпека, міжнародне співробітництво, дипломатія, кібердипломатія, міжнародні організації, Україна.

Samoylenko T. O. Cybersecurity as a New Dimension of International Relations. Student of the bachelor's degree in specialty 291 «International relations, public communications, and regional studies» of the educational and professional program «International relations and geopolitical security». State University «Zhytomyr Polytechnic», 2025.

The first chapter highlights the conceptual foundations of cybersecurity, such as: the causes of its emergence, definitions, objectives, elements of provision, and key components. The necessity of international cooperation in the field of cybersecurity is determined, as well as the regulatory legal acts governing this activity within international organizations such as the EU, NATO, and the UN.

The second chapter addresses the global challenges facing diplomacy and their impact on it. The concept of cyber diplomacy, its essence, and the role of cyber diplomacy in the activities of leading international organizations—namely, the UN, EU, and NATO—are considered.

The third chapter examines the current policy of Ukraine in the field of cyber diplomacy, particularly the regulatory legal acts and initiatives underlying the functioning of cyber diplomacy in the country. It also explores the specifics of Ukraine's international cooperation with the EU, NATO, the USA, Slovenia, and the Republic of Latvia in the field of cybersecurity.

Keywords: cybersecurity, international cooperation, diplomacy, cyber diplomacy, international organization, Ukraine.