Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО

«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Механізми кібердипломатії як засоби формування міжнародних відносин для національної безпеки держави»

Виконавець: студент IV курсу, групи КБ-44 (мс)

_____ **Антон ІЛЬНІЦЬКИЙ**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я, прізвище**
Керівник		Володимир НАКОНЕЧНИЙ
Нормоконтроль		Леся БАРАНОВСЬКА

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО

29 листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-44(мс)** **Ільніцькому Антону В'ячеславовичу**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Механізми кібердипломатії як засоби формування міжнародних відносин для національної безпеки держави

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Нормативні акти у сфері кібербезпеки, аналітичні документи ООН, НАТО, ЄС, стратегічні документи України, дані МЗС, ДССЗЗІ, РНБО, досвід кібердипломатії США, Естонії, ЄС, Китайської Народної Республіки.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Аналіз термінології та моделей кібердипломатії, оцінка нормативної бази України, огляд міжнародних ініціатив, визначення викликів і розробка практичних рекомендацій з впровадження кібердипломатії як інструменту національної безпеки

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність формування рекомендацій щодо впровадження кібердипломатії в зовнішньополітичну діяльність України

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ (підпис) Володимир НАКОНЕЧНИЙ (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Антон ІЛЬНІЦЬКИЙ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.01.2025	*виконано*
2	Аналіз літератури	29.01.2025 – 11.02.2025	*виконано*
3	Визначення актуальності проблеми	12.02.2025 – 15.02.2025	*виконано*
4	Аналіз основних міжнародних концепцій і практик у сфері кібердипломатії	16.02.2025 – 04.03.2025	*виконано*
5	Дослідження нормативно-правової бази та стратегічних документів України у сфері кібербезпеки	05.03.2025 – 21.03.2025	*виконано*
6	Аналіз міжнародного співробітництва України в контексті кібердипломатії	22.03.2025 – 08.04.2025	*виконано*
7	Визначення інституційної архітектури та пропозиції щодо посилення кібердипломатичного потенціалу держави	09.04.2025 – 10.05.2025	*виконано*
8	Оформлення пояснювальної записки	11.05.2025 – 27.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2025 – 13.06.2025	*виконано*

Завдання видав _____ (підпис) Володимир НАКОНЕЧНИЙ (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Антон ІЛЬНІЦЬКИЙ (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 61 сторінку основного тексту, 7 рисунків та 1 таблицю. Список використаних джерел містить 33 найменувань і займає 4 сторінки.

Метою дослідження є комплексний аналіз механізмів кібердипломатії як інструментів формування міжнародних відносин, а також розробка рекомендацій щодо їх впровадження у практику зовнішньої та безпекової політики України з метою посилення її національної безпеки.

Об'єктом дослідження виступає процес міжнародних відносин у цифровому вимірі, зокрема механізми співпраці, регулювання та дипломатичного впливу в кіберпросторі.

Предметом дослідження є практики, інститути та нормативно-правові механізми кібердипломатії, що використовуються державами для протидії кіберзагрозам, захисту цифрового суверенітету та формування глобальної кібербезпеки.

Актуальність роботи обумовлена зростаючим значенням кіберпростору як сфери геополітичного протистояння, постійними кібератаками на критичну інфраструктуру України та необхідністю розбудови системи кібердипломатії як засобу міжнародної відповіді та стримування цифрової агресії.

Розвиток кібердипломатії є важливою складовою забезпечення кіберстійкості держави та інтеграції України до євроатлантичного безпекового простору.

Для досягнення поставленої в роботі мети необхідно виконання наступних задач:

- проаналізувати ключові теоретичні підходи до розуміння кібердипломатії;
- провести дослідження міжнародного досвіду реалізації цифрової дипломатії (США, ЄС, Естонії, Китаю);

- здійснити оцінку сучасного стану кібердипломатії в Україні, наявних стратегій та інституцій;
- визначити основні виклики, такі як нормативна невизначеність, кадровий дефіцит, слабка координація;
- розробити комплекс пропозицій щодо формування Стратегії кібердипломатії України, впровадження інституту цифрових аташе, удосконалення нормативно-правової бази у сфері кібербезпеки та налагодження сталого міжнародного співробітництва.

Практичні рекомендації передбачають створення міжвідомчої координаційної ради, підготовку кадрів цифрової дипломатії, участь у глобальних ініціативах (GGE, OEWG, IGF), а також гармонізацію українського законодавства з директивою NIS2 та Стратегією кібербезпеки ЄС.

Перспективами подальших досліджень є розробка механізмів міжнародно-правової відповідальності за кібератаки, моделювання цифрового суверенітету та вивчення впливу штучного інтелекту на процеси цифрової дипломатії.

Ключові слова: кібердипломатія, кібербезпека, національна безпека, міжнародне право, інформаційна політика, цифрова держава, кіберагресія, дипломатічна відповідь, NIS2, цифровий суверенітет.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 8
ВСТУП 10
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРДИПЛОМАТІЇ 12
1.1 Поняття та сутність кібердипломатії 12
1.2 Історичні передумови та етапи становлення кібердипломатії 15
1.3 Основні моделі та концепції кібердипломатії в міжнародній практиці 16
1.3.1 Американська модель: вільний і відкритий кіберпростір 18
1.3.2 Європейська модель: баланс між безпекою та правами людини 18
1.3.3 Китайсько-російська модель: кіберсуверенітет та державний контроль 19
1.3.4 Естонська модель: цифрова держава та кібербезпека 19
1.3.5 Гібридні моделі та багатосторонній підхід 20
1.3.6 Основні концепції кібердипломатії 20
Висновки до розділу 1 21
РОЗДІЛ 2. СУЧАСНИЙ СТАН КІБЕРДИПЛОМАТІЇ В УКРАЇНІ 22
2.1 Національні стратегії та нормативно-правове регулювання кібердипломатії в Україні 22
2.1.1 Кібердипломатія як пріоритет національної політики безпеки 23
2.1.2 Стратегія кібербезпеки України (2021) 25
2.1.3 Розробка Стратегії кібердипломатії України (2024–2025) 27
2.1.4 Інші стратегічні документи та ініціативи 29
2.2 Інституційна інфраструктура реалізації кібердипломатії в Україні 30
2.3 Аналіз реалізованих ініціатив та дій України в сфері кібердипломатії 33
Висновки до розділу 2 36
РОЗДІЛ 3. МЕХАНІЗМИ КІБЕРДИПЛОМАТІЇ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ 38
3.1 Формування партнерських зв’язків і участь у міжнародних організаціях 38
3.2. Протидія гібридним загрозам та цифрова дипломатія в умовах збройного конфлікту 41

3.3 Перспективи розвитку кібердипломатії: напрями вдосконалення державної політики 43
3.3.1 Інституційне укріплення кібердипломатії 44
3.3.2 Формування кадрового потенціалу та системи освіти 46
3.3.3 Удосконалення нормативно-правової бази 48
3.3.4 Розширення міжнародної присутності та суб’єктності України 49
Висновки до розділу 3 51
ВИСНОВКИ 53
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

APT	-	Advanced Persistent Threat – складна, цілеспрямована та довготривала кіберзагроза
CCDSOE	-	Cooperative Cyber Defence Centre of Excellence – Центр передового досвіду з кібероборони НАТО
CERT-UA	-	Computer Emergency Response Team of Ukraine – Команда реагування на комп'ютерні надзвичайні події в Україні
CSIRT	-	Computer Security Incident Response Team – Команда реагування на кіберінциденти
ДССЗЗІ	-	Державна служба спеціального зв'язку та захисту інформації України
ЄС	-	Європейський Союз
ІКТ	-	інформаційно-комунікаційні технології
КБ	-	кібербезпека
КСЗІ	-	комплексна система захисту інформації
МТД	-	міжнародна технічна допомога
NATO	-	North Atlantic Treaty Organization – Організація Північноатлантичного договору
NIS2	-	Network and Information Security Directive 2 – Директива ЄС про безпеку мереж і інформаційних систем
ООН	-	Організація Об'єднаних Націй
ОБСЄ	-	Організація з безпеки і співробітництва в Європі
РНБО	-	Рада національної безпеки і оборони України
СБУ	-	Служба безпеки України
GDPR	-	General Data Protection Regulation – Загальний регламент захисту даних (Регламент (ЄС) 2016/679 Європейського парламенту і Ради)
NIS Directive	-	Directive on Security of Network and Information Systems – Директива ЄС про безпеку мережевих та інформаційних систем (NIS1, Директива (ЄС) 2016/1148)
СЗРУ	-	Служба зовнішньої розвідки України

ВСТУП

У сучасному світі кіберпростір перетворився на ключову арену міжнародних відносин, де взаємодіють інтереси держав, міжнародних організацій, приватного сектору та суспільства. Зростання масштабів кібератак, цифрових впливів і гібридних загроз обумовило необхідність формування нових інструментів зовнішньої політики, серед яких особливе місце посідає кібердипломатія. Як результат — у XXI столітті цифрова дипломатія стає важливим чинником забезпечення національної безпеки та суверенітету держав.

Україна, перебуваючи в умовах гібридної війни, щоденно зіштовхується з викликами в кіберпросторі, що вимагає адекватної дипломатичної реакції на міжнародному рівні. Участь у глобальних кіберініціативах, формування стратегічних партнерств, розбудова правового поля та інституційної бази — усе це стає запорукою не лише безпеки цифрового середовища, а й загальної стабільності держави.

Дана тема є актуальною у зв’язку з необхідністю комплексного переосмислення ролі дипломатії у кіберпросторі та її впливу на безпекову політику держав.

Об’єктом дослідження є процес міжнародних відносин у сфері кібербезпеки.

Предметом дослідження виступають механізми кібердипломатії як інструменти забезпечення національної безпеки України.

Метою дослідження є аналіз теоретичних засад, правових і організаційних механізмів кібердипломатії та вивчення їхнього потенціалу для формування ефективної системи міжнародного співробітництва в контексті безпеки держави.

Завдання дослідження:

- розкрити сутність та еволюцію поняття кібердипломатії;
- проаналізувати ключові моделі та концепції кібердипломатії;

- дослідити інституційно-правову основу кібердипломатії в Україні;
- охарактеризувати участь України у міжнародних ініціативах у сфері кібербезпеки;
- визначити механізми, за допомогою яких кібердипломатія сприяє зміцненню національної безпеки;
- запропонувати напрями вдосконалення державної політики у сфері кібердипломатії.

Методи дослідження: теоретичний аналіз, порівняльно-правовий метод, метод системного підходу, контент-аналіз, метод кейс-стаді.

Наукова новизна дослідження полягає у комплексному розгляді кібердипломатії не лише як складової зовнішньої політики, а як інструмента стратегічного впливу на міжнародні відносини з метою забезпечення національної безпеки.

Практичне значення полягає у можливості використання результатів дослідження для формування державної політики у сфері кібербезпеки, розробки нормативно-правових актів, підготовки спеціалістів у галузі кібердипломатії.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРДИПЛОМАТІЇ

1.1 Поняття та сутність кібердипломатії

У XXI столітті стрімкий розвиток інформаційно-комунікаційних технологій, зростання обсягів передачі та обробки даних, диджиталізація глобальних суспільств зумовили появу нових викликів у сфері міжнародних відносин. Однією з відповідей на ці виклики стало формування інституційного та концептуального напряму зовнішньої політики – кібердипломатії.

Визначення терміну кібердипломатія

Кібердипломатія — це форма дипломатичної діяльності, що полягає у використанні дипломатичних інструментів для врегулювання відносин між державами у сфері кібербезпеки, регулювання поведінки в кіберпросторі, протидії кіберзагрозам та формування глобальних норм і правил взаємодії в цифровому середовищі [1].

Це поняття охоплює:

- участь держав у міжнародних переговорах щодо кібербезпеки;
- захист національних інтересів у сфері інформаційних технологій;
- просування державних ініціатив у галузі цифрової політики на глобальному рівні;
- взаємодію з міжнародними організаціями та інституціями з метою створення правового режиму в кіберпросторі.

Сутність та зміст

Сутність кібердипломатії полягає у використанні механізмів класичної дипломатії для вирішення конфліктів, пов'язаних із кіберпростором [1]:

- атаками на критичну інфраструктуру;
- поширенням дезінформації;
- втручанням у виборчі процеси;

- кібершпигунством;
- розробкою шкідливого ПЗ тощо.

Цей вид дипломатії функціонує на перетині зовнішньої політики, національної безпеки, цифрової трансформації та міжнародного права. Він передбачає [2]:

- проведення переговорів щодо обмеження кіберозброєнь;
- обговорення принципів державної поведінки у цифровому середовищі;
- координацію реакцій на кібератаки;
- встановлення механізмів атрибуції та відповідальності;
- розвиток міжнародних альянсів (наприклад, через НАТО, ООН, ЄС) для протидії кіберзагрозам.

Основні функції кібердипломатії [2]:

1. Нормативна – формування міжнародних норм поведінки у кіберпросторі.
2. Комунікативна – підтримка каналів обміну між державами у разі інцидентів.
3. Превентивна – запобігання ескалації кіберконфліктів.
4. Інтегративна – об'єднання зусиль держав, НУО, бізнесу та експертного середовища.
5. Репутаційна – просування позитивного іміджу держави як відповідального актора в кіберпросторі.

Основні функції кібердипломатії охоплюють нормативне регулювання, міжнародну комунікацію, запобігання кіберконфліктам, захист державних інтересів у кіберпросторі та формування позитивного іміджу країни як відповідального цифрового актора.

Рисунок 1.1 – Основні функції кібердипломатії

У структурі зовнішньої політики сучасної держави кібердипломатія займає особливе місце як механізм формування цифрового суверенітету та захисту інформаційного простору від зовнішніх втручань. Зокрема, у національних стратегіях країн ЄС, США, Японії, Австралії кібердипломатія вже інтегрована в системи безпеки.

В Україні розвиток кібердипломатії почався з 2014 року як відповідь на масові кібератаки з боку Російської Федерації. Зокрема, створення підрозділів кібербезпеки при МЗС України, участь у міжнародних форумах та співпраця з НАТО стали ключовими кроками.

1.2 Історичні передумови та етапи становлення кібердипломатії

Витоки кібердипломатії: від технічного співробітництва до політичного виміру.

Початкові етапи становлення кібердипломатії сягають кінця XX століття, коли розвиток інформаційно-комунікаційних технологій почав впливати на міжнародні відносини. Зростання залежності держав від цифрових інфраструктур висвітлило необхідність міжнародного співробітництва у сфері кібербезпеки.

Ключові етапи розвитку кібердипломатії [3]:

1. Формування міжнародних ініціатив (2000–2010 роки):
   - 2004 рік: Створення Групи урядових експертів (GGE) при ООН з метою розробки глобальних норм поведінки у кіберпросторі.
   - 2007 рік: Кібератаки на Естонію стали першим масштабним інцидентом, що привернув увагу до кібербезпеки на міжнародному рівні.
   - 2009 рік: США започаткували концепцію "21st Century Statecraft", інтегруючи цифрові технології у дипломатичну практику.
2. Інституціоналізація кібердипломатії (2011–2015 роки):
   - 2011 рік: Ухвалення першої Міжнародної стратегії США щодо кіберпростору.
   - 2012 рік: Створення Центру передового досвіду НАТО з кібероборони (CCDCOE) у Таллінні.
   - 2013 рік: Публікація "Талліннського посібника" щодо застосування міжнародного права до кіберконфліктів.
3. Розширення міжнародного співробітництва (2016–2020 роки):
   - 2017 рік: ЄС впровадив "Cyber Diplomacy Toolbox" для координації дипломатичних заходів у відповідь на кіберзагрози.

- 2018 рік: Ініціатива "Paris Call for Trust and Security in Cyberspace" об'єднала держави, компанії та громадянське суспільство для зміцнення кібербезпеки.

4. Сучасний етап: виклики та перспективи (2021–дотепер):

- 2022 рік: Створення Бюро кіберпростору та цифрової політики (CDP) у Державному департаменті США.
- 2023 рік: Активізація міжнародних зусиль щодо розробки правил поведінки у кіберпросторі, зокрема в рамках ООН та інших міжнародних форумів.

Роль України у формуванні кібердипломатії.

Україна активно долучилася до формування кібердипломатії, особливо після 2014 року. Відповіддю на кібератаки стало створення спеціалізованих підрозділів у сфері кібербезпеки, участь у міжнародних ініціативах та розробка національних стратегій. Зокрема, у 2024 році Україна організувала Міжнародну конференцію з кібердипломатії у Києві, що стало важливим кроком у зміцненні її позицій на міжнародній арені.

1.3 Основні моделі та концепції кібердипломатії в міжнародній практиці

У міжнародній практиці кібердипломатії сформувалися декілька ключових моделей та концепцій, що визначають підходи держав до взаємодії у цифровому середовищі. Зокрема:

- Модель кіберсуверенітету — передбачає право держави контролювати внутрішній кіберпростір і встановлювати власні правила регулювання інтернету. Цей підхід активно просувають Росія та Китай.
- Модель відкритого Інтернету — базується на цінностях свободи слова, децентралізації управління мережею, захисту цифрових прав людини. Прихильниками цієї моделі є США, країни ЄС, Канада, Австралія.

- Багатостороння модель — визнає участь не лише держав, а й приватного сектору, технічних спільнот і громадянського суспільства у формуванні правил кіберпростору (підхід Internet Governance Forum, ICANN).
- Модель кіберстійкості — зосереджена на здатності держав і організацій протистояти кібератакам, швидко відновлювати функціонування та забезпечувати надійний захист цифрової інфраструктури.
- Нормативна модель — акцентує увагу на формуванні глобальних норм і правил поведінки у кіберпросторі (через ООН, ОБСЄ, НАТО).

Для наочності на рисунку 1.1 представлено основні моделі та концепції кібердипломатії, їх ключові характеристики. пр

Рисунок 1.2 – Основні моделі та концепції кібердипломатії в міжнародній практиці

1.3.1 Американська модель: вільний і відкритий кіберпростір

Сполучені Штати Америки розглядають кіберпростір як глобальний публічний ресурс, де пріоритетами є свобода вираження, захист прав людини та інновації. Американська кібердипломатія спрямована на просування принципів відкритого інтернету, сприяння багатосторонньому управлінню мережею та забезпечення безпеки кіберпростору через міжнародне співробітництво.

У 2024 році адміністрація президента Джо Байдена представила нову міжнародну стратегію кібербезпеки, яка фокусується на чотирьох основних напрямках: сприяння безпечному глобальному цифровому екосередовищу, підтримка правозахисних цифрових технологій разом із союзниками, побудова коаліцій для протидії кібератакам та підвищення кіберстійкості партнерських країн.

1.3.2 Європейська модель: баланс між безпекою та правами людини

Європейський Союз дотримується підходу, який поєднує забезпечення кібербезпеки з дотриманням прав людини та основних свобод. ЄС активно працює над розробкою та впровадженням нормативно-правових актів, таких як Загальний регламент захисту даних (GDPR) та Директива про безпеку мережевих та інформаційних систем (NIS Directive), які встановлюють стандарти захисту даних та кібербезпеки.

Крім того, ЄС підтримує багатосторонній підхід до управління інтернетом та сприяє міжнародному діалогу щодо встановлення норм поведінки в кіберпросторі. У 2018 році ЄС підтримав "Паризький заклик до довіри та безпеки в кіберпросторі", який закликає до спільних дій для забезпечення стабільності та безпеки в цифровому середовищі.

1.3.3 Китайсько-російська модель: кіберсуверенітет та державний контроль

Китай та Росія просувають концепцію "кіберсуверенітету", яка передбачає право кожної держави контролювати свій сегмент інтернету, включаючи обмеження доступу до інформації та контроль над цифровими технологіями. Цей підхід акцентує на важливості державного суверенітету в кіберпросторі та відстоює ідею, що кожна країна має право визначати власні правила та політики щодо інтернету.

Китай активно розвиває власну цифрову інфраструктуру та технології, зокрема через ініціативу "Цифровий шовковий шлях", яка спрямована на розширення впливу Китаю в сфері цифрових технологій на глобальному рівні.

Росія, у свою чергу, працює над створенням автономного інтернету та впровадженням законодавства, яке дозволяє обмежувати доступ до певних ресурсів та контролювати інформаційні потоки.

1.3.4 Естонська модель: цифрова держава та кібербезпека

Естонія стала першопроходцем у сфері кібербезпеки серед європейських країн у впровадженні цифрових технологій у державне управління та забезпеченні кібербезпеки. Після масштабної кібератаки у 2007 році Естонія зробила значні інвестиції в розвиток кібербезпеки та стала однією з перших країн, яка запровадила електронне голосування та цифрову ідентифікацію громадян.

У 2008 році в Таллінні було створено Центр передового досвіду НАТО з питань кібероборони (NATO CCDCOE), який займається дослідженнями та навчанням у сфері кібербезпеки. Цей центр також розробив "Талліннський посібник" — керівництво щодо застосування міжнародного права до кіберконфліктів.

1.3.5 Гібридні моделі та багатосторонній підхід

Багато країн, зокрема Німеччина, Франція та Канада, впроваджують гібридні моделі кібердипломатії, які поєднують елементи різних підходів. Ці моделі акцентують на важливості багатостороннього співробітництва, залучення різних стейкхолдерів, включаючи уряди, приватний сектор та громадянське суспільство, до формування політик у сфері кібербезпеки.

Наприклад, Франція активно просуває ініціативу "Паризький заклик до довіри та безпеки в кіберпросторі", яка об'єднує держави, компанії та громадські організації для спільної роботи над забезпеченням стабільності та безпеки в цифровому середовищі.

1.3.6 Основні концепції кібердипломатії

У міжнародній практиці кібердипломатії сформувалися кілька ключових концепцій [4]:

- Кіберсуверенітет — право держави контролювати свій кіберпростір та встановлювати власні правила щодо інтернету.
- Багатостороннє управління інтернетом — залучення різних стейкхолдерів до процесу прийняття рішень щодо управління інтернетом.
- Кіберстійкість — здатність держави протистояти та відновлюватися після кібератак.
- Цифрові права людини — забезпечення прав та свобод людини в цифровому середовищі.
- Норми поведінки в кіберпросторі — встановлення міжнародних правил та стандартів щодо поведінки держав у кіберпросторі.

Ці концепції формують основу для розробки та впровадження політик у сфері кібербезпеки та кібердипломатії на міжнародному рівні.

Висновки до розділу 1

У першому розділі було здійснено комплексне теоретичне дослідження поняття, змісту та еволюції кібердипломатії як нового напряму зовнішньої політики держав у цифрову епоху.

З'ясовано, що кібердипломатія є міждисциплінарним явищем, яке об’єднує традиційні дипломатичні інструменти з сучасними викликами кібербезпеки, управління інтернетом, захисту цифрових прав і побудови міжнародного кіберпорядку.

Розкрито сутність кібердипломатії як форми політичного впливу в інформаційному просторі, спрямованої на формування глобальних норм поведінки у кіберпросторі, протидію транснаціональним кібератакам і забезпечення кіберсуверенітету.

Встановлено, що вона виконує нормативну, комунікативну, превентивну та репутаційну функції, що робить її важливим інструментом у реалізації національних інтересів.

Проаналізовано етапи становлення кібердипломатії на глобальному рівні — від перших ініціатив у рамках ООН і НАТО до сучасних інституційних підходів, зокрема створення CDP (США), CCDCOE (Естонія), механізмів кібервідповідальності ЄС та багатосторонніх ініціатив на кшталт "Паризького заклику".

Узагальнення моделей кібердипломатії дозволило виявити основні геополітичні підходи: ліберальний (США, ЄС), гібридно-інноваційний (Естонія). Ці підходи формують контекст, у якому Україна повинна визначати власну модель кібердипломатичної поведінки.

Таким чином, теоретичні засади кібердипломатії формують ґрунт для аналізу її практичного застосування, зокрема у контексті України, що буде предметом наступного розділу.

РОЗДІЛ 2
СУЧАСНИЙ СТАН КІБЕРДИПЛОМАТІЇ В УКРАЇНІ

2.1 Національні стратегії та нормативно-правове регулювання кібердипломатії в Україні

У відповідь на зростання кіберзагроз та гібридної агресії, Україна поступово формує стратегічну й нормативну основу кібердипломатії. Уряд ухвалив низку ключових документів, що закладають правові, інституційні та міждержавні механізми протидії цифровим загрозам. Ці документи охоплюють аспекти кібербезпеки, інформаційного захисту, цифрової трансформації безпекового сектору та інтеграції у європейський кіберпростір.

На рисунку нижче представлено часову шкалу, яка ілюструє ключові етапи формування політик кібербезпеки та кібердипломатії в Україні у період з 2018 до 2025 року.

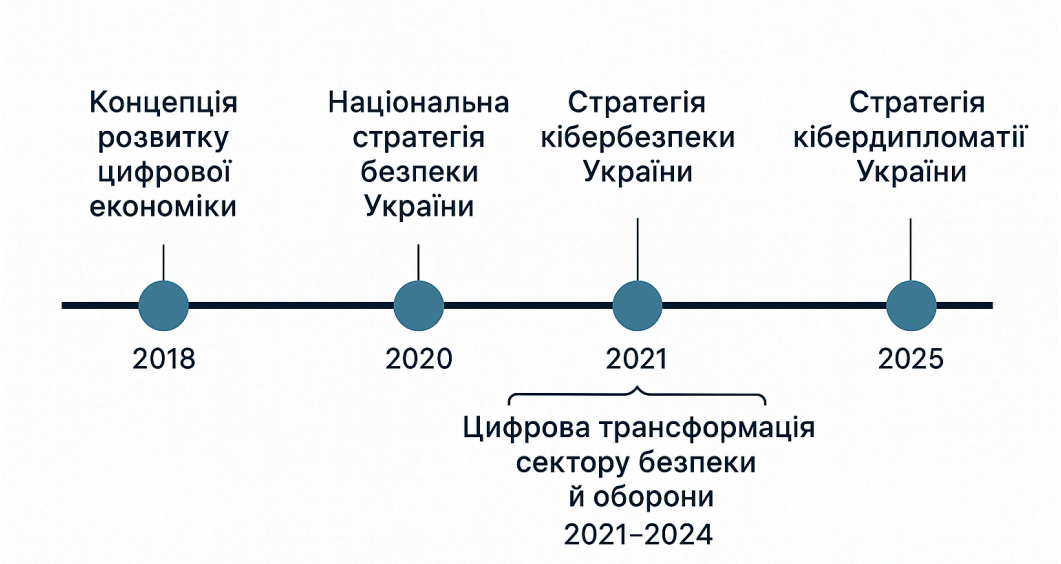


Рисунок 2.1 – Розвиток стратегічних ініціатив України у сфері кібербезпеки та кібердипломатії (2018–2025)

2.1.1 Кібердипломатія як пріоритет національної політики безпеки

З початком збройної агресії Російської Федерації проти України у 2014 році проблема захисту кіберпростору перестала бути суто технічною чи спеціалізованою — вона трансформувалася у комплексне питання, що безпосередньо стосується національного суверенітету, територіальної цілісності та виживання держави. Кібератаки на державні установи, енергетичну інфраструктуру, об’єкти критичної інфраструктури, а також на медіаплатформи й соціальні мережі стали постійною загрозою, що вимагає системної, стратегічної відповіді як на національному, так і на міжнародному рівнях.

Особливо яскраво ця загроза проявилася у випадках масштабних кібератак, зокрема атаки на енергетичну систему у грудні 2015 року, яка призвела до знеструмлення десятків населених пунктів, а також у 2017 році, коли Україну вразила глобальна хвиля кібершкідника Petya/NotPetya. Остання атака паралізувала роботу банків, урядових органів, транспортної інфраструктури та підприємств, завдавши шкоди на сотні мільйонів доларів. Ці події стали не лише технічною проблемою, а й чітким сигналом для всього світу щодо загрози, яку становить кіберагресія як елемент гібридної війни.

На тлі таких викликів кібердипломатія набула надзвичайно важливого значення. Вона перетворилася на один із ключових інструментів зовнішньої політики України, що дозволяє не лише реагувати на інциденти, але й системно формувати партнерства, впливати на формування міжнародних стандартів та норм поведінки в кіберпросторі, долучатися до розробки глобальної цифрової політики.

Участь України в багатосторонніх міжнародних форматах — таких як Організація Об’єднаних Націй, Європейський Союз, Північноатлантичний альянс, IGF (Internet Governance Forum), ITU (Міжнародний союз електрозв’язку) та інші — стала свідченням активного прагнення країни до інтеграції у глобальну систему цифрової безпеки. Через ці формати Україна не лише доносить власну позицію, а й формує союзницькі блоки, залучає

підтримку у протистоянні кіберагресії та розширює коло технічної та політичної допомоги.

Кібердипломатія також стала засобом захисту інформаційного простору країни, у якому ведеться активна боротьба не лише з технічними загрозами, а й з дезінформаційними кампаніями, фейками, пропагандистськими наративами, що поширюються як у межах країни, так і за її межами. Через механізми кібердипломатії Україна вибудовує нову форму цифрової солідарності — систему підтримки, засновану на спільних цінностях відкритості, прозорості, верховенства права та відповідальності.

Важливо підкреслити, що саме після 2014 року українська держава почала активно формувати стратегії кібербезпеки, нормативно-правову базу у сфері захисту інформації та цифрових технологій, а також створювати інституції, відповідальні за міжнародну цифрову політику. Перші спроби формалізувати кібердипломатію як окремий напрям зовнішньої політики відбулися у межах міжвідомчої взаємодії — між Міністерством закордонних справ, Держспецзв'язку, СБУ, РНБО, Мінцифрою та кіберполіцією.

На цьому етапі держава усвідомила, що лише технічних засобів недостатньо — необхідна активна політична й дипломатична діяльність у кіберпросторі, спрямована на створення міжнародних коаліцій, механізмів колективного захисту та нормативного регулювання глобального цифрового середовища. У зв'язку з цим у зовнішньополітичному дискурсі України все частіше почали з'являтися терміни «кібердипломатія», «кіберсуверенітет», «цифрові права людини», «інформаційна гігієна» та інші, що засвідчує перехід до нової парадигми державної безпекової політики.

Отже, кібердипломатія на сучасному етапі національного розвитку стала одним із ключових механізмів реагування на гібридні загрози та інструментом формування стабільних міжнародних відносин, спрямованих на зміцнення національної безпеки держави. Вона дозволяє не лише протидіяти кібератакам, а й впливати на глобальні цифрові процеси, захищаючи інтереси країни в умовах цифрової трансформації світу.

2.1.2 Стратегія кібербезпеки України (2021)

У відповідь на зростаючі кіберзагрози, що стали невід'ємною частиною сучасних збройних конфліктів, у 2021 році в Україні було затверджено нову редакцію Стратегії кібербезпеки — ключового політичного документа, що визначає основні принципи, пріоритети та напрямки дій держави в цифровому просторі. Затверджена Указом Президента України №447/2021, ця Стратегія вперше офіційно закріпила важливість кібердипломатії як невід’ємного інструмента національної безпеки [5].

Один із фундаментальних акцентів документа — необхідність посилення міжнародного співробітництва в галузі кібербезпеки та інтеграції України до євроатлантичного цифрового безпекового простору.

Така постановка питання не є випадковою: саме на тлі триваючої гібридної війни та постійної загрози з боку Російської Федерації українське керівництво усвідомило, що без тісної взаємодії з міжнародними партнерами забезпечення кіберстійкості держави є неможливим.

Стратегія кібербезпеки України 2021 року містить низку важливих положень, які безпосередньо стосуються кібердипломатії [5]:

- Побудова національної системи кібербезпеки на основі стандартів НАТО та ЄС. Це передбачає не лише технічне вдосконалення інфраструктури, а й імплементацію відповідних політик, процедур і протоколів, прийнятих у міжнародних організаціях, до яких Україна прагне інтегруватися.
- Розширення міжнародного співробітництва в межах кіберальянсів. Стратегія підкреслює необхідність активної участі у багатосторонніх ініціативах, програмах кібердопомоги, обміну досвідом та спільного реагування на кібератаки. Йдеться не лише про обмін інформацією, а й про створення механізмів колективної протидії цифровим загрозам.
- Розробка механізмів координації дій державних інституцій у кіберпросторі. Це означає формування ефективної системи управління в умовах кіберінцидентів, коли залучаються одночасно урядові, силові,

військові, дипломатичні та комунікаційні структури. Саме така взаємодія становить базу для розвитку кібердипломатії.

- Протидія використанню кіберпростору для інформаційних атак, дезінформації та гібридного впливу. У цьому контексті кібердипломатія виконує не лише захисну функцію, а й контрнаступальну — спрямовану на викриття агресора, інформування міжнародної спільноти та формування відповідного тиску.
- Посилення ролі України як суб'єкта міжнародного права у сфері цифрової безпеки. Україна декларує своє прагнення не лише захищати себе, а й формувати міжнародні норми, бути учасником глобального процесу врегулювання взаємодії держав у кіберпросторі.

Крім вищенаведеного, Стратегія прямо вказує на необхідність активної участі України у роботі Групи урядових експертів ООН з питань інформаційної безпеки. Це — один із ключових глобальних форумів, де визначаються правила поведінки держав у кіберпросторі, що є основою для формування міжнародного права у цій сфері. Участь у таких процесах є прямим проявом кібердипломатії та свідченням того, що Україна прагне не лише реагувати на загрози, а й впливати на формування глобального порядку денного.

Окрему увагу приділено адаптації національного законодавства до вимог Європейського Союзу, зокрема в контексті імплементації Директиви NIS2 (Network and Information Systems Directive) [6]. Ця директива встановлює обов'язкові вимоги для операторів критичної інфраструктури, провайдерів цифрових послуг і органів влади щодо управління кіберризиками та звітування про інциденти. Її імплементація в українське правове поле є важливим етапом не лише у гармонізації законодавства, але й у зміцненні міжнародної довіри до цифрової політики України.

Таким чином, Стратегія кібербезпеки України (2021) є не просто нормативним документом, а основою для системного впровадження політики кібердипломатії. Вона визначає Україну як активного гравця у сфері глобальної цифрової безпеки, здатного не лише оборонятись, а й брати участь у

формуванні норм, політик та коаліцій, необхідних для забезпечення стабільного, прозорого та безпечного кіберпростору.

2.1.3 Розробка Стратегії кібердипломатії України (2024–2025)

У сучасних умовах посиленої конкуренції в цифровому середовищі, глобального технологічного суперництва та безперервних кіберзагроз Україна усвідомлює необхідність переходу від епізодичних заходів у сфері кібердипломатії до системного, стратегічного підходу. Саме тому у 2024 році Міністерство закордонних справ України офіційно оголосило про початок розробки Стратегії кібердипломатії України — першого в історії держави рамкового політичного документа, який буде повністю присвячений цифровому компоненту зовнішньої політики.

Ця ініціатива є відповіддю на численні виклики сучасного світу, серед яких особливе місце займає транснаціональний характер кібератак, гібридних кампаній, цифрової пропаганди, впливу через соцмережі, кібершпигунства, економічного шантажу тощо. Не менш важливою передумовою для створення цієї стратегії стала міжнародна підтримка, яку Україна отримала після початку повномасштабного вторгнення росії в 2022 році, включно з наданням кібердопомоги, обміном інформацією та доступом до глобальних інфраструктур цифрового захисту.

Підготовкою документу займається Відділ кібердипломатії Міністерства закордонних справ України, створений у 2022 році в межах структурної модернізації зовнішньополітичного відомства. Цей відділ покликаний забезпечити координацію дій МЗС України у сфері кібербезпеки, цифрових прав, інтернет-урядування, а також вибудовувати партнерства з провідними цифровими державами та міжнародними організаціями. Саме його зусиллями ініційовано процес консультацій з міжнародними партнерами, експертами, громадянським суспільством і науковими інституціями з метою вироблення цілісної концепції кібердипломатії України.

Очікується, що стратегія охоплюватиме низку пріоритетних напрямів [7]:

- Визначення ключових міжнародних партнерів України в сфері кібербезпеки. Йдеться про створення переліку стратегічних держав та організацій (НАТО, ЄС, США, Велика Британія, Канада, Естонія, Литва, Японія), з якими Україна підтримуватиме регулярний діалог, обмін інформацією, а також формуватиме спільні політичні позиції.
- Позиціонування України як активного учасника глобального цифрового порядку. У межах цього пункту передбачено участь у міжнародних форумах, таких як OEWG та GGE ООН, IGF, ENISA, а також ініціатива створення українських платформ для міжнародного кібердіалогу.
- Сприяння формуванню прозорих, справедливих і всеохоплюючих міжнародних правил поведінки у кіберпросторі. Україна прагне стати адвокатом відповідального використання кіберзасобів, прозорості державної політики у сфері кіберзахисту, а також дотримання міжнародного гуманітарного права в цифрових конфліктах.
- Розвиток механізмів міжнародного обміну даними про кіберінциденти. Один із найважливіших технічних компонентів стратегії — створення платформ для обміну оперативною інформацією з союзниками, що дозволить своєчасно реагувати на кібератаки та попереджати їхній вплив.
- Дипломатичне реагування на транснаціональні кібератаки. У стратегії буде закріплено механізми «цифрового реагування», зокрема дипломатичні заяви, ініціація розслідувань, санкційні заходи проти агресорів, інформування міжнародної спільноти та мобілізація підтримки.

Варто також наголосити, що в розробці стратегії активно використовується міжнародний досвід, зокрема найкращі практики США, Європейського Союзу та Естонії. Наприклад, у стратегії передбачається створення міжвідомчої системи координації дій у сфері кібердипломатії, куди залучатимуться не лише МЗС України, а й СБУ, Держспецзв’язку, Міністерство внутрішніх справ, Міністерство оборони, Служба зовнішньої розвідки та інші суб’єкти безпекового сектору. Така модель координації має забезпечити

оперативність, гнучкість і цілісність дипломатичних дій у разі загроз або інцидентів у кіберпросторі.

Крім того, в межах стратегії передбачено впровадження системи моніторингу ефективності кібердипломатичних інструментів, що дозволить на основі кількісних та якісних індикаторів оцінювати прогрес у досягненні поставлених цілей.

Таким чином, Стратегія кібердипломатії України (2024–2025) стане не лише важливим внутрішньополітичним документом, а й зовнішньополітичним сигналом для міжнародної спільноти про готовність України брати активну участь у формуванні безпечного, стійкого й справедливого цифрового майбутнього.

2.1.4 Інші стратегічні документи та ініціативи

Крім згаданих, важливими для розуміння державної політики в сфері кібердипломатії є:

- Національна стратегія безпеки України (2020) – в якій інформаційна безпека та кіберзахист визначені як пріоритети [8];
- Концепція розвитку цифрової економіки (2018) – акцент на побудові безпечного цифрового середовища [9];
- Цифрова трансформація безпеки і оборони (2021–2024) – програма Мінцифри щодо захисту державних реєстрів, комунікаційних систем та інфраструктури [10];
- Національна програма інформатизації – де також передбачено формування систем захисту інформаційних ресурсів у міжнародному контексті [11].

Для наочності в таблиці 2.1 наведено порівняльну характеристику основних стратегічних документів, що визначають напрямки розвитку кібердипломатії в Україні.

Таблиця 2.1

Порівняльна характеристика стратегій у контексті кібердипломатії

Документ	Рік	Ключові положення щодо кібердипломатії
Національна стратегія безпеки України	2020	Визначає інформаційну безпеку й кіберзахист як пріоритети національної безпеки.
Концепція розвитку цифрової економіки	2018	Підкреслює необхідність формування безпечного цифрового середовища для сталого економічного розвитку.
Цифрова трансформація сектору безпеки й оборони	2021–2024	Спрямована на захист держреєстрів, комунікацій, інформаційних ресурсів та підвищення кіберстійкості сектору оборони.
Стратегія кібербезпеки України	2021	Офіційно закріплює кібердипломатію як один із ключових інструментів забезпечення нацбезпеки у цифровому просторі.
Національна програма інформатизації	чинна редакція	Містить положення щодо інтеграції України в міжнародний контекст захисту інформації та розвитку нацсистем кіберзахисту.

2.2 Інституційна інфраструктура реалізації кібердипломатії в Україні

Розбудова ефективної кібердипломатії в Україні неможлива без чітко сформованої інституційної архітектури, яка забезпечує координацію між зовнішньополітичними, безпековими, технічними та аналітичними структурами. З огляду на гібридну агресію проти України та постійне зростання кіберзагроз, держава активно формує інститути, здатні реагувати на зовнішні виклики та брати участь у формуванні глобального кіберпорядку.

Рисунок 2.2 – Зовнішньополітичний вимір у сфері кіберпростору

Ключовим органом, що безпосередньо відповідає за зовнішньополітичний вимір у сфері кіберпростору, є Міністерство закордонних справ України. У 2022 році в його структурі було створено Відділ кібердипломатії, який координує участь України у міжнародних переговорах, форумах та проєктах, пов’язаних із цифровою безпекою. Відділ відповідає за міжвідомчу координацію із Держспецзв’язку, СБУ, Мінцифрою, Нацполіцією та іншими органами, а також за просування національних ініціатив на міжнародному рівні. У 2024 році за ініціативи МЗС було розпочато розробку Національної стратегії кібердипломатії України.

Водночас стратегічний нагляд за формуванням політики кібербезпеки та кібердипломатії здійснює Рада національної безпеки і оборони України (РНБО). У 2016 році при РНБО було створено Національний координаційний центр кібербезпеки (НКЦК), що є головною платформою оперативної координації дій

органів державної влади у відповідь на кіберінциденти. Центр також виступає аналітичним майданчиком, що готує пропозиції щодо участі України в міжнародних ініціативах у сфері кібербезпеки.

На технічному рівні одним із центральних виконавчих органів, який забезпечує кіберстійкість державних структур, є Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). В її структурі функціонує Національна команда реагування на комп'ютерні інциденти CERT-UA, яка здійснює моніторинг, аналіз та нейтралізацію кіберзагроз. Через участь CERT-UA у міжнародних ініціативах, як-от FIRST, TF-CSIRT тощо, Україна отримує доступ до глобальної системи обміну інформацією про кіберінциденти.

Окрему роль відіграє Служба безпеки України, яка забезпечує контррозвідувальний захист держави в інформаційній сфері. Її підрозділи проводять розслідування кібершпигунства, шкідливих впливів на державні реєстри, а також взаємодіють з міжнародними правоохоронними органами в частині протидії кібертероризму та транснаціональній кіберзлочинності.

Міністерство цифрової трансформації України (Мінцифра), створене у 2019 році, відіграє важливу роль у формуванні інституційної основи цифрової держави. Міністерство відповідає за впровадження цифрових сервісів, адміністрування державних платформ («Дія», Єдині реєстри тощо) та підтримку проєктів із цифрової безпеки. Мінцифра також ініціює співпрацю з міжнародними технологічними компаніями та платформами (google, Cloudflare, Amazon AWS, Microsoft), що створює для України інструменти кібердипломатичного впливу на приватному рівні.

Практичний вимір забезпечення кібербезпеки, зокрема розслідування кіберзлочинів, покладено на Департамент кіберполіції Національної поліції України. Підрозділ активно залучений до міжнародних операцій Europol, Interpol та спільних слідчих груп, а також бере участь у конференціях, форумах і тренінгах, що мають кібердипломатичну складову.

На рівні законодавчої влади Верховна Рада України забезпечує нормативно-правову базу кібербезпеки та інформаційного захисту. Прийняття Закону України «Про основні засади забезпечення кібербезпеки України» у 2017 році стало фундаментальним кроком у визначенні повноважень та взаємодії між суб'єктами системи кібербезпеки. У 2024 році було зареєстровано законопроєкти, спрямовані на оновлення законодавства про дипломатичну службу з урахуванням кіберспецифіки, зокрема щодо введення інституту кібердипломатів.

Таким чином, інституційна інфраструктура кібердипломатії в Україні є багаторівневою та міжвідомчою. Попри відсутність окремої вертикалі управління, існуюча система дозволяє здійснювати оперативну координацію дій, забезпечувати участь у міжнародних перемовинах, отримувати технічну підтримку від партнерів та формувати імідж України як відповідального і компетентного суб'єкта у сфері кіберпростору.

2.3 Аналіз реалізованих ініціатив та дій України в сфері кібердипломатії

В умовах постійного зростання кіберзагроз та гібридної агресії, що супроводжується інформаційними та кібератаками, Україна активно формує свою політику кібердипломатії.

З 2014 року, коли було зафіксовано перші масштабні кібератаки на критичну інфраструктуру держави, національна безпекова стратегія України набула чіткого кіберкомпонента, що передбачає не лише внутрішній захист, а й участь у міжнародному кіберпросторі як активного суб'єкта.

На рівні зовнішньої політики одним із перших кроків стало налагодження тісного співробітництва з Європейським Союзом у форматі регулярних кібердіалогів. У рамках цього формату Україна і ЄС обговорюють найактуальніші виклики в цифровому середовищі, обмінюються найкращими практиками реагування на інциденти, координують законодавчі ініціативи в

сфері цифрових стандартів та інформаційної безпеки. З 2019 року такі діалоги стали регулярними і охоплюють не лише технічні, але й дипломатичні аспекти.

Паралельно з цим, Україна системно поглиблює співпрацю з НАТО у сфері кібербезпеки. Українські фахівці регулярно беруть участь у навчаннях, тренінгах та спільних кіберсимуляціях за участю НАТО, що дозволяє підвищувати рівень сумісності та адаптувати національні стандарти до норм Альянсу. У 2023 році Україна офіційно розпочала процедуру приєднання до Центру передового досвіду НАТО з кібероборони (CCDCOE) в Таллінні, що стало важливим сигналом про зростання ролі України у євроатлантичній системі цифрової безпеки.

Активну участь Україна бере у роботі Групи урядових експертів ООН (GGE) та відкритої робочої групи (OEWG), які займаються виробленням міжнародних норм поведінки у кіберпросторі. Українські представники неодноразово виступали із пропозиціями щодо посилення міжнародного правового режиму у сфері кібербезпеки, зокрема щодо відповідальності держав за кібератаки, обміну інформацією про інциденти та прозорості кіберозброєння.

У контексті боротьби з кіберагресією Україна активно підтримує глобальні ініціативи, спрямовані на зміцнення довіри та безпеки в кіберпросторі. Було укладено низку двосторонніх меморандумів про співпрацю у сфері кібербезпеки з країнами ЄС, США, Ізраїлем, Естонією, Литвою та іншими державами. Ці домовленості передбачають не лише обмін інформацією, а й проведення спільних навчань, координацію політики в ООН, підтримку України в кіберінцидентах, технічну допомогу в модернізації державних захисних систем.

Особливо важливою стала ініціатива із створення національного сегменту глобальної платформи реагування на кібератаки, який передбачає миттєве залучення міжнародних партнерів у випадку масштабних загроз. Після початку повномасштабного вторгнення російської федерації у 2022 році Україна отримала суттєву міжнародну підтримку в кіберсфері: провідні західні

IT-компанії надали Україні інфраструктуру для хмарного збереження даних, кіберзахист урядових сайтів та кіберрозвідку щодо загроз.

У межах публічної кібердипломатії Україна бере участь у великих міжнародних форумах: Munich Security Conference, GLOBSEC, IGF (Internet Governance Forum), CYBERSEC Europe та ін. Під час цих заходів українські представники порушують питання відповідальності держав за кібератаки, необхідності формування міжнародного трибуналу з розслідування кіберагресії та створення інструментів санкційного впливу на держави-порушники.

Окремий вектор співпраці — це залучення до глобальних кібернавчань. Українські структури регулярно беруть участь у навчаннях типу Cyber Flag, Locked Shields, Cyber Europe, які моделюють реальні кіберінциденти і дають змогу перевірити оперативну готовність держави. У таких навчаннях залучені представники як збройних сил, так і цивільних установ — кіберполіції, CERT-UA, Держспецзв’язку.

Також Україна формує мережу кібердипломатичних партнерств через дипломатичні місії та консульства. В окремих українських посольствах за кордоном уже діють цифрові аташе, які відповідають за підтримку зв'язків з національними кіберцентрами країн перебування. Це дозволяє оперативно реагувати на інциденти, сприяти притягненню до відповідальності правопорушників, а також посилює взаємну підтримку в рамках ООН, ОБСЄ, Ради Європи.

З освітнього боку, важливим елементом розвитку кібердипломатії стали ініціативи Міністерства закордонних справ України та Дипломатичної академії щодо підготовки кадрів нового типу.

Впроваджуються спеціалізовані програми з кібердипломатії, цифрового управління, інформаційної безпеки у зовнішній політиці. До навчання залучаються іноземні експерти, представники НАТО, Європейського агентства з кібербезпеки (ENISA), а також науковці з університетів Естонії, Німеччини, США.

Таким чином, Україна вже реалізувала значну кількість ініціатив, які можна віднести до сфери кібердипломатії. Вони охоплюють як традиційну міжурядову взаємодію, так і нетрадиційні форми — участь у глобальних платформах, кіберальянсах, цифровій допомозі, створенні репутаційного образу країни як надійного партнера в боротьбі з кіберзлочинністю та кіберагресією. Це формує цілісну модель кібердипломатичної діяльності, яка все більше інтегрується у зовнішню політику України.

Висновки до розділу 2

У другому розділі було проаналізовано сучасний стан кібердипломатії в Україні через призму стратегічних документів, інституційної інфраструктури та реалізованих міжнародних ініціатив. Дослідження показало, що, попри відсутність окремої нормативно визначеної політики кібердипломатії на законодавчому рівні, Україна вже фактично реалізує її елементи у сфері зовнішньої політики та національної безпеки.

Зокрема, національні стратегії — такі як Стратегія кібербезпеки України, Національна стратегія безпеки та програми цифрової трансформації — містять чіткі орієнтири на активну участь України в глобальних кіберпроцесах, формування партнерств та адаптацію до міжнародних стандартів. Паралельно відбувається формування окремої Стратегії кібердипломатії, яка має закріпити механізми координації та визначити зовнішньополітичні пріоритети у цифровій сфері.

Інституційна система кібердипломатії в Україні є багатокомпонентною і включає МЗС, РНБО, Держспецзв’язку, СБУ, Мінцифру, кіберполіцію, а також представництва України за кордоном. Незважаючи на відсутність централізованої вертикалі, взаємодія між цими структурами забезпечує гнучкість та оперативність у реагуванні на цифрові виклики.

Реалізовані ініціативи свідчать про активну інтеграцію України у світовий кіберпростір: участь у форумах, кібердіалогах з ЄС, співпраця з НАТО, ООН,

укладення меморандумів із країнами-партнерами, розвиток публічної кібердипломатії, залучення міжнародної технічної допомоги, створення навчальних програм — усе це формує потужний базис для розвитку повноцінної кібердипломатичної політики.

Таким чином, Україна перебуває на етапі формування власної моделі кібердипломатії, яка спирається як на національні безпекові інтереси, так і на спільні цінності міжнародної спільноти. В умовах кіберконфлікту, що супроводжує збройну агресію, кібердипломатія перетворюється для України з допоміжного інструмента на ключовий елемент зовнішньополітичної стратегії.

РОЗДІЛ 3
МЕХАНІЗМИ КІБЕРДИПЛОМАТІЇ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

3.1 Формування партнерських зв'язків і участь у міжнародних організаціях

В умовах зростаючої міждержавної конкуренції у цифровому просторі та загроз національній безпеці з боку зловмисних кібердій, Україна змушена розглядати кібердипломатію як один із ключових напрямів зовнішньої політики. Одним з найважливіших механізмів кібердипломатії є формування стійких міжнародних партнерств і активна участь у роботі профільних міждержавних організацій. Через ці інструменти Україна інтегрується у глобальну систему кібербезпеки, розвиває інституційний діалог із ключовими акторами та формує власну суб'єктність у цифровій сфері.

Участь України в діяльності міжнародних організацій

Одним з важливих напрямів діяльності України у сфері кібердипломатії є її активна участь у міжнародних міжурядових форматах:

- Організація Об'єднаних Націй (ООН) — зокрема у діяльності Групи урядових експертів (GGE) та Відкритої робочої групи з кібербезпеки (OEWG). Участь у цих органах дозволяє Україні формувати позицію щодо норм поведінки держав у кіберпросторі, протидіяти ініціативам, які суперечать інтересам відкритого Інтернету, та доносити до світової спільноти інформацію про цифрову агресію з боку РФ [12].
- Організація з безпеки і співробітництва в Європі (ОБСЄ) — майданчик для обговорення заходів довіри у кіберпросторі. Україна бере участь у відповідних робочих групах і ініціативах, спрямованих на зниження ризиків міждержавної ескалації внаслідок кібератак [13].

- НАТО та Програма «Партнерство заради миру» — НАТО визнає кіберпростір як окрему операційну сферу, і Україна активно співпрацює з Альянсом у межах програм кіберзахисту, тренувань, симуляцій (наприклад, Locked Shields), а також бере участь у проєктах Центру передового досвіду з кібероборони у Таллінні (CCDCOE) [14].
- Європейський Союз — через виконання Угоди про асоціацію та імплементацію відповідних директив у сфері кібербезпеки (зокрема NIS2), Україна наближає своє законодавство до європейських стандартів. Крім того, налагоджено співпрацю з Європейським агентством з кібербезпеки (ENISA) та іншими структурами [15].
- Міжнародний форум з управління Інтернетом (IGF) — участь у багатосторонніх майданчиках з управління Інтернетом дозволяє Україні підтримувати відкриту архітектуру глобальної мережі, відстоювати свободу слова в цифровому просторі, а також протидіяти політиці цифрової ізоляції, яку просуває російська федерація та деякі інші авторитарні режими.

Партнерства на двосторонньому рівні

Окрім участі у глобальних форумах, Україна активно розвиває двосторонню співпрацю у сфері кібербезпеки та цифрової дипломатії:

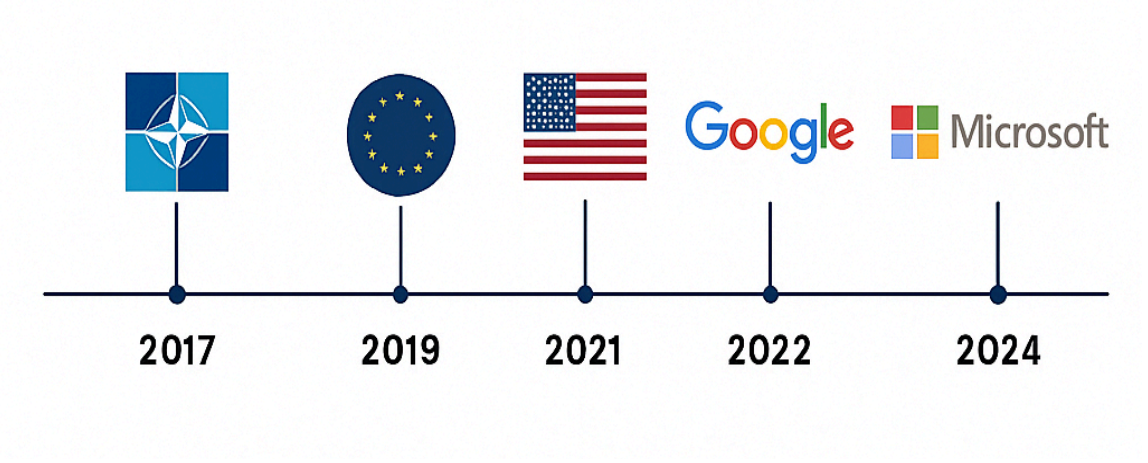
- Україна – США: співпраця з Державним департаментом США, Агентством з кібербезпеки та інфраструктурної безпеки (CISA), а також з USAID, яке реалізує проєкти з посилення кіберстійкості державного сектору в Україні. США також надали підтримку у створенні навчальних центрів та оперативного реагування на інциденти [16].
- Україна – Естонія: стратегічне партнерство у сфері цифрового урядування, кібербезпеки та навчання кадрів. Естонія передає експертизу у створенні систем електронного управління, захисту критичної інфраструктури та взаємодії з громадянами через цифрові канали [17].
- Україна – Великобританія, Канада, Литва, Польща: налагоджена співпраця у сфері обміну кіберінформацією, проведення спільних

навчань, розвитку CERT-структур, впровадження систем моніторингу загроз [18].

- Україна – Ізраїль: партнерство у сфері кіберрозвідки, аналізу атак, впровадження технологій захисту та оцінки кіберризиків [19].

У період з 2017 по 2024 рік Україна поступово нарощувала обсяги міжнародної співпраці в сфері кібербезпеки, беручи участь у спільних навчаннях, ініціативах, програмах технічної допомоги та обміну інформацією. На рисунку 3.1 візуалізовано ключові проєкти, за роками та відповідними організаціями-партнерами.

Рисунок 3.1 – Основні міжнародні ініціативи України у сфері кібердипломатії



(2017–2024)

Ці двосторонні механізми дозволяють Україні швидко реагувати на кіберінциденти, отримувати експертну допомогу, формувати кадровий резерв і розширювати технічну базу для забезпечення цифрового суверенітету.

Кібердипломатія як механізм підвищення довіри

Формування партнерств не обмежується лише безпековими питаннями. Кібердипломатія дозволяє також [1]:

- підвищити міжнародну довіру до цифрової політики України;
- залучити міжнародну технічну допомогу;
- розбудовувати імідж України як держави-інноватора у сфері кібербезпеки;

- використовувати дипломатичні механізми для ідентифікації джерел атак та мобілізації міжнародної підтримки.

Кібердипломатія в Україні — це вже не лише «реакція на загрози», а проактивний інструмент формування середовища міжнародної підтримки, цифрової довіри та колективної кіберстійкості. У контексті повномасштабної агресії росії це стало не лише зовнішньополітичним, а й екзистенційним завданням державної безпеки.

3.2. Протидія гібридним загрозам та цифрова дипломатія в умовах збройного конфлікту

Сучасні воєнні конфлікти давно вийшли за межі класичного озброєння, перетворившись на гібридні протистояння, де кіберпростір відіграє центральну роль. Україна є одним із найяскравіших прикладів держави, яка з 2014 року постійно перебуває під дією гібридної агресії з боку російської федерації. Цей тиск включає не лише збройне вторгнення, а й масштабні кібероперації, дезінформаційні кампанії, втручання у комунікаційну інфраструктуру, атаки на критичні об’єкти, інформаційний тероризм та спроби маніпулювання міжнародною думкою.

У таких умовах кібердипломатія стала одним із ключових інструментів протидії гібридним загрозам, оскільки саме через дипломатичні канали Україна мобілізує міжнародну підтримку, формує коаліції для кіберзахисту, привертає увагу до кіберзлочинів та добивається реагування з боку міжнародних організацій.

Виявлення та документування кіберзагроз

Після 2022 року українські державні органи значно активізували зусилля щодо ідентифікації, документування та публічного розкриття інформації про кібератаки, здійснені росією. Особливу роль у цьому відіграють [20]:

- СБУ та Держспецзв’язку, які через CERT-UA та Кіберцентр забезпечують фіксацію інцидентів;

- МЗС України, що дипломатичними каналами передає докази іноземної агресії до міжнародних інституцій;
- Цифрові слідчі центри та ІТ-волонтери, які досліджують походження атак, аналізують зразки шкідливого ПЗ, визначають інфраструктури атакувальників.

Оприлюднення таких даних на міжнародних платформах — важливий елемент інформаційної протидії та публічної відповідальності агресора.

Цифрова дипломатія під час повномасштабної війни

Після початку повномасштабного вторгнення росії в Україну у лютому 2022 року цифрова дипломатія набула нової, небаченої ваги [20]:

- Україна змогла мобілізувати глобальну ІТ-спільноту, сформувавши ініціативу IT Army of Ukraine, що координується, у тому числі, на міждержавному рівні.
- Завдяки дипломатичному втручанню, міжнародні ІТ-компанії (Google, Microsoft, Amazon, Meta, Cloudflare) надали допомогу у захисті української інфраструктури, переміщенні даних до хмар, фільтрації контенту, блокуванні російських пропагандистських ресурсів.
- Через дипломатичні інструменти Україна домоглася санкційного відключення росії від деяких цифрових послуг, сервісів та технологій.
- Була налагоджена оперативна координація з європейськими та північноамериканськими партнерами, що дозволило здійснювати обмін технічною інформацією про атаки майже в реальному часі.

Таким чином, цифрова дипломатія стала фактично фронтом — інструментом інформаційної оборони, мобілізації ресурсів та блокування каналів цифрової агресії супротивника.

Дипломатичне реагування на кіберінциденти

Суттєво зросла й важливість реактивних дипломатичних дій, спрямованих на міжнародне визнання фактів кіберзлочинів [20]:

- Україна ініціює розгляд кіберзагроз у Раді Безпеки ООН.

- Офіційно апелює до іноземних урядів із закликами до розслідування кібератак та притягнення винних до відповідальності.
- Через міжнародні форуми просуває ідею створення механізмів кібервідповідальності держав, які порушують міжнародні норми у цифровому просторі.
- Долучається до міжнародних санкційних ініціатив, спрямованих на цифрових виконавців, розробників шкідливого ПЗ, підконтрольні державі хакерські групи.

Ці заходи дозволяють не лише стримувати агресора, а й формувати міжнародну правову практику щодо державної відповідальності за кіберзлочини.

Таким чином, у контексті гібридної війни, цифрова дипломатія та кібердипломатичні механізми не просто посилюють зовнішньополітичний вплив України — вони є невід'ємною частиною її оборонної стратегії.

Участь у кіберкоаліціях, міжнародне оприлюднення фактів атак, дипломатичні заяви, цифрові санкції — все це є елементами комплексної відповіді на багаторівневу загрозу, що виходить за межі звичайної військової агресії.

3.3 Перспективи розвитку кібердипломатії: напрями вдосконалення державної політики

У XXI столітті кіберпростір став не лише ареною економічного та інформаційного розвитку, а й стратегічною зоною національної безпеки. Для України, яка перебуває під постійною загрозою гібридної війни, кібердипломатія є критично важливим механізмом інтеграції у міжнародну систему безпеки та захисту державного суверенітету. Проте, для ефективного функціонування цієї сфери необхідне системне вдосконалення державної політики — як у нормативному, так і в інституційному вимірах.

3.3.1 Інституційне укріплення кібердипломатії

Ефективна реалізація кібердипломатії потребує чіткої та інтегрованої інституційної інфраструктури, яка б забезпечувала координацію дій між ключовими органами державної влади, прозорість прийняття рішень та оперативне реагування на загрози в цифровому середовищі.

В умовах зростаючих кіберзагроз, а також активного використання інформаційних технологій у міжнародній політиці, інституційне укріплення кібердипломатії стає критично важливим елементом державної безпеки. Передусім, доцільним є створення постійно діючої міжвідомчої координаційної платформи з питань кібердипломатії, до складу якої входили б представники Міністерства закордонних справ України, Державної служби спеціального зв'язку та захисту інформації, Служби безпеки України, Ради національної безпеки і оборони, Міністерства цифрової трансформації, а також профільних аналітичних центрів. Такий орган дозволив би сформувати єдину політику в галузі кібердипломатії та забезпечити інтеграцію технічного, політичного й правового компонентів у спільну систему реагування.

На рисунку 3.2 показано алгоритм створення постійно діючої міжвідомчої координаційної платформи з питань кібердипломатії.

Після створення міжвідомчої координаційної платформи важливим завданням є чітке визначення ролей та взаємозв'язків між основними державними структурами, які залучаються до реалізації кібердипломатії. Це дозволяє досягти ефективної синхронізації дій у сфері зовнішньої та інформаційної безпеки.

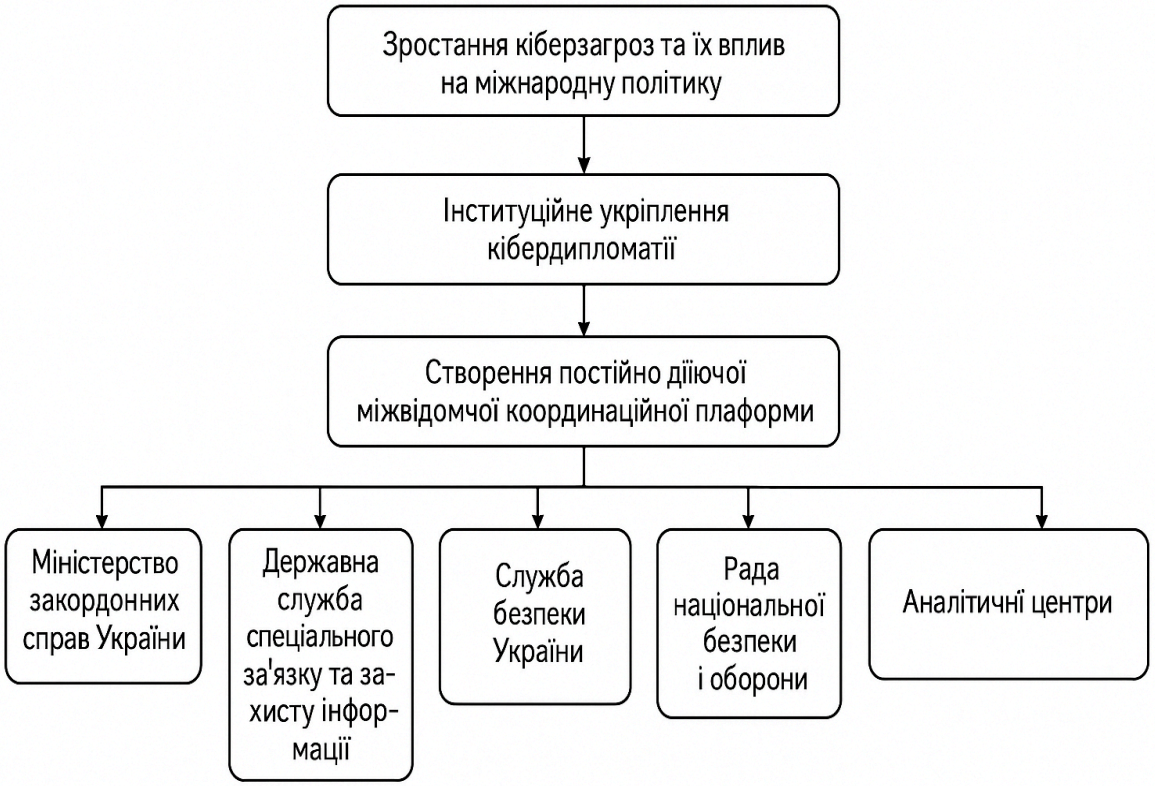


Рисунок 3.2 – Алгоритм створення постійно діючої міжвідомчої координаційної платформи з питань кібердипломатії

Рисунок 3.3 – Структура інституційної взаємодії у сфері кібердипломатії України

Наступним важливим кроком є впровадження інституту цифрових аташе у складі закордонних дипломатичних установ України. Ці фахівці мали б відповідати за координацію міжнародного співробітництва в цифровій сфері, моніторинг регіональних кіберзагроз, забезпечення обміну інформацією з місцевими урядами, міжнародними організаціями та провідними IT-компаніями. Подібна практика вже довела свою ефективність у зовнішній політиці низки країн, зокрема Сполучених Штатів Америки, Великобританії, Німеччини та Естонії.

Також варто приділити увагу поглибленню співпраці з міжнародними цифровими дипломатичними структурами. Мова йде, зокрема, про Департамент кіберполітики Державного департаменту США, підрозділи Європейської служби зовнішньої дії, Центр передового досвіду НАТО з кібербезпеки у Таллінні (CCDCOE) та інші відповідні установи. Налагодження постійного двостороннього та багатостороннього діалогу з цими структурами дозволить Україні брати участь у формуванні глобальної цифрової політики, вчасно адаптувати національне законодавство та зміцнювати власну кіберстійкість.

Зміцнення інституційної основи кібердипломатії має розглядатися як пріоритет державної політики. Воно не лише сприятиме ефективному представництву інтересів України у міжнародному цифровому просторі, але й забезпечить швидке реагування на зовнішні виклики, підвищить рівень довіри до української кіберполітики та зміцнить репутацію держави як надійного партнера у сфері міжнародної цифрової безпеки.

3.3.2 Формування кадрового потенціалу та системи освіти

Однією з ключових умов успішного розвитку кібердипломатії є наявність кваліфікованих кадрів, здатних ефективно працювати на перетині зовнішньої політики, інформаційної безпеки, міжнародного права та цифрових технологій. Враховуючи новизну цієї сфери, Україна стикається з проблемою нестачі підготовлених фахівців, здатних реалізовувати завдання кібердипломатії на

міжнародному рівні. Тому розвиток кадрового потенціалу та створення сучасної системи освіти у цій галузі є невід'ємним елементом вдосконалення державної політики.

Насамперед, важливо ініціювати впровадження спеціалізованих освітніх програм і курсів з кібердипломатії. Такі програми мають охоплювати як теоретичні основи — міжнародне право, цифрову геополітику, етику кіберпростору, так і практичні навички — ведення переговорів у сфері ІТ-безпеки, аналіз кіберзагроз, взаємодію з міжнародними організаціями. Освіта має бути міждисциплінарною, здійснюватися на базі провідних вишів України, зокрема дипломатичних академій, технічних університетів і закладів, що готують фахівців у сфері безпеки.

Водночас варто передбачити створення системи післядипломної освіти та підвищення кваліфікації для державних службовців, дипломатів і представників безпекових структур. Ідеться про короткострокові програми, тренінги, стажування, розроблені за участі національних та іноземних експертів. Особливу увагу слід приділити адаптації таких програм до динамічних змін у сфері кібербезпеки, новітніх міжнародних стандартів і практик цифрового врегулювання конфліктів.

Крім формального навчання, ефективним інструментом стане розширення міжнародного освітнього співробітництва. Необхідно активно залучати Україну до міжнародних проєктів і стипендій з кібербезпеки й кібердипломатії, таких як програми ЄС (Horizon Europe, Erasmus+), ініціативи НАТО, Центру передового досвіду CCDCOE, програм ОБСЄ тощо. Це дозволить українським спеціалістам переймати кращі практики, налагоджувати міжнародні зв'язки й підвищувати власний рівень експертизи.

Також до формування кадрового потенціалу доцільно залучати експертів з приватного сектору та громадянського суспільства. В умовах, коли ІТ-компанії володіють передовими технологіями й досвідом реагування на кіберінциденти, їх участь у підготовці фахівців для державного сектору виглядає

обґрунтованою. Налагодження такої співпраці допоможе створити гнучку й адаптивну систему, що відповідатиме вимогам часу.

Таким чином, формування висококваліфікованого людського ресурсу для сфери кібердипломатії є не просто освітнім завданням, а стратегічним чинником забезпечення цифрового суверенітету держави, її міжнародної суб'єктності та здатності реагувати на складні виклики кіберепохи.

3.3.3 Удосконалення нормативно-правової бази

Нормативно-правове забезпечення є фундаментом будь-якої державної політики, особливо у сфері безпеки та міжнародного співробітництва. Кібердипломатія, як напрям державної діяльності, що охоплює цифрові процеси, міжнародні відносини, протидію кібератакам та формування цифрових норм поведінки, потребує чіткої, сучасної й адаптивної правової основи. Станом на сьогодні Україна має базові документи, що регламентують діяльність у сфері кібербезпеки, однак вони лише частково охоплюють аспекти міжнародної взаємодії в цифровому просторі.

Першочерговим завданням є адаптація національного законодавства до європейських стандартів у сфері цифрової безпеки, зокрема до положень Директиви ЄС NIS2 (Network and Information Security). Ця директива передбачає створення ефективних механізмів координації дій між державами-членами ЄС, обмін інформацією про кіберінциденти, обов'язкову звітність критичної інфраструктури про кібератаки. Для України це означає необхідність гармонізації законодавства, зокрема в частині обов'язків державних і приватних суб'єктів щодо реагування на інциденти, формування механізмів нагляду та контролю.

Крім цього, доцільним є розроблення й впровадження комплексного закону про кібердипломатію, який би визначав статус, завдання, інструменти та суб'єкти цього напряму державної політики. Такий документ має враховувати міжнародно-правові підходи, які закладені в роботі Групи урядових експертів

ООН (GGE), Відкритої робочої групи ООН (OEWG), практику Європейського Союзу, а також положення Будапештської конвенції про кіберзлочинність.

Особливої уваги потребує врегулювання правового статусу цифрової агресії, що особливо актуально для України в контексті гібридної війни. Необхідно закріпити на рівні законодавства визначення кібератак як елементу збройного конфлікту або актів міжнародної агресії, що відкриє можливості для міжнародного юридичного переслідування агресора та використання механізмів колективної безпеки.

Також важливим завданням є створення правових механізмів реагування на міжнародні кіберінциденти. Це стосується як оперативного обміну інформацією з партнерами, так і процедури дипломатичного протесту, санкційного реагування, звернень до міжнародних судових інстанцій, документування порушень. Така практика має стати стандартною частиною зовнішньополітичної діяльності держави у сфері кібербезпеки.

Удосконалення нормативної бази дозволить не лише структурувати діяльність державних органів у сфері кібердипломатії, а й зміцнити позиції України на міжнародній арені, продемонструвати її відповідність міжнародним стандартам і готовність до конструктивного діалогу щодо безпеки у цифровому просторі.

3.3.4 Розширення міжнародної присутності та суб'єктності України

У сучасному глобалізованому світі кіберпростір став одним із ключових елементів міжнародної взаємодії, а присутність держави в глобальних цифрових ініціативах — показником її політичної активності, спроможності до кооперації та суб'єктності у сфері безпеки. Для України, яка перебуває в умовах постійної кіберзагрози з боку російської федерації, важливо не лише реагувати на виклики, але й формувати проактивну позицію на міжнародній арені.

Першочерговим завданням є активізація участі України в міжнародних міжурядових платформах, які займаються формуванням глобальної політики у

сфері кібербезпеки. Йдеться, зокрема, про роботу у Групі урядових експертів ООН (GGE), Відкритій робочій групі з питань кібербезпеки (OEWG), Форумі з управління інтернетом (IGF), а також взаємодію з НАТО та ЄС у рамках відповідних програм цифрової дипломатії. Повноцінна участь у цих структурах дозволяє Україні впливати на формування норм поведінки в кіберпросторі та просувати власні національні інтереси.

Особливе значення має поглиблення співпраці з Центром передового досвіду НАТО з кібербезпеки (CCDCOE) в Таллінні. Україна вже є приєднаною стороною до низки ініціатив Центру, проте варто активніше використовувати цей майданчик для розбудови експертних контактів, отримання аналітичної підтримки, участі в навчаннях та спільних проєктах. Розширення співпраці з CCDCOE також сприятиме гармонізації національної політики з підходами країн-членів Альянсу.

Наступним важливим напрямом є ініціювання нових двосторонніх та багатосторонніх цифрових партнерств. Україна має потенціал для поглиблення співпраці з такими лідерами кібердипломатії як Естонія, США, Франція, Польща, Канада, Австралія. Ідеться не лише про підписання декларацій і меморандумів, а й про запуск спільних дослідницьких центрів, програм обміну, спільних навчань та платформ для обміну інформацією про кіберінциденти.

Водночас важливо просувати ініціативу створення міжнародного механізму відповідальності за кібератаки, включаючи створення незалежного арбітражного органу або спеціалізованого цифрового трибуналу. Це дозволило б закріпити юридичні підстави для притягнення до відповідальності акторів, які вчиняють агресію в цифровому середовищі.

Розширення міжнародної присутності в сфері кібердипломатії дозволить Україні не лише убезпечити себе від зовнішніх загроз, а й стати повноправним гравцем у формуванні нової архітектури глобальної кібербезпеки. Системна участь у міжнародних ініціативах, налагодження партнерств і розбудова дипломатичних механізмів дозволяють перетворити виклики цифрової епохи на інструменти стратегічного посилення держави.

Висновки до розділу 3

У третьому розділі було проаналізовано механізми кібердипломатії як інструментів забезпечення національної безпеки та формування міжнародних відносин у цифрову епоху. Дослідження показало, що кібердипломатія перестає бути вузькопрофільним напрямом і набуває ознак повноцінного складника державної політики у сфері безпеки, міжнародного співробітництва та цифрового розвитку.

Насамперед, виявлено, що інституційне укріплення кібердипломатії є ключовою умовою її ефективності. Україна має всі передумови для створення дієвої системи координації в межах державних органів, зокрема шляхом формалізації міжвідомчої платформи та впровадження інституту цифрових аташе. Водночас, існує потреба у налагодженні сталих контактів з міжнародними цифровими дипломатичними структурами.

У сфері кадрового забезпечення необхідно впроваджувати спеціалізовані програми вищої освіти та підвищення кваліфікації, які охоплюють як технічні, так і дипломатичні компетенції. Співпраця з іноземними партнерами, приватним сектором та аналітичними центрами має стати постійною складовою процесу формування людського потенціалу.

Аналіз також вказує на нагальну потребу в удосконаленні нормативно-правової бази, зокрема гармонізації з європейськими стандартами, розробці законодавства про кібердипломатію та правового визначення цифрової агресії. Законодавче закріплення статусу кіберінцидентів як факторів, що впливають на національну безпеку, дозволить державі ефективно захищати свої інтереси на міжнародному рівні.

Крім того, розширення міжнародної присутності України в цифрових дипломатичних ініціативах є не лише інструментом зовнішньополітичного впливу, а й механізмом побудови довіри до держави як суб’єкта глобальної кібербезпеки. Активна участь у міжнародних форумах, ініціювання нових

партнерств, а також просування ідеї відповідальності за кібератаки є пріоритетними напрямами на найближчу перспективу.

Таким чином, реалізація запропонованих механізмів кібердипломатії створює основу для побудови цілісної стратегії цифрової зовнішньої політики України, сприяє її інтеграції до євроатлантичного простору та зміцнює її здатність протистояти сучасним загрозам у кіберсфері.

ВИСНОВКИ

Проведене дослідження на тему «Механізми кібердипломатії як засоби формування міжнародних відносин для національної безпеки держави» дозволило всебічно проаналізувати природу, функціональні характеристики та перспективи розвитку кібердипломатії як складника зовнішньої політики України.

У роботі було охоплено як теоретичні засади становлення цього явища, так і практичні аспекти національної політики в умовах сучасного геополітичного та кіберпросторового контексту.

У першому розділі роботи розглянуто базові підходи до визначення поняття кібердипломатії, її сутнісні риси та історичну еволюцію. Показано, що кібердипломатія є мультидисциплінарним напрямом, що виник на перетині міжнародного права, кібербезпеки та політичної комунікації. Встановлено, що в умовах цифрової трансформації вона перетворюється на стратегічний інструмент впливу на міжнародну політику, сприяє просуванню національних інтересів у глобальному інформаційному просторі, формуванню правил поведінки держав у кіберсередовищі та зміцненню цифрового суверенітету.

Порівняльний аналіз міжнародних моделей кібердипломатії (американської, європейської, китайсько-російської, естонської) дав змогу визначити потенціал для створення адаптованої гібридної моделі для України, яка б поєднувала технологічну відкритість, правозахисний підхід та високий рівень кіберзахисту.

У другому розділі здійснено поглиблений аналіз сучасного стану кібердипломатії в Україні. Встановлено, що за останнє десятиліття, з початку агресії російської федерації, держава зробила суттєвий прогрес у нормативному та стратегічному забезпеченні цифрової безпеки. Зокрема, визначено, що Стратегія кібербезпеки (2021) і розроблювана Стратегія кібердипломатії

(2024–2025) стали важливими рамковими документами, які зафіксували пріоритетність міжнародної цифрової взаємодії як елементу національної безпеки.

Проаналізовано інституційну архітектуру реалізації цієї політики, яка включає МЗС України, ДССЗЗІ, СБУ, Міністерство цифрової трансформації та інші органи, однак наголошено на потребі посилення координації між ними. Оцінено практичні кроки України на міжнародній арені: участь у кіберформатах ООН, партнерство з CCDCOE, активну співпрацю з ЄС і НАТО.

У третьому розділі визначено ключові механізми вдосконалення національної політики у сфері кібердипломатії, зокрема:

- інституційне укріплення, що передбачає створення міжвідомчого органу координації, запровадження інституту цифрових аташе та посилення взаємодії з міжнародними структурами;
- кадрове забезпечення, через розробку освітніх програм, професійної перепідготовки та співпраці з ІТ-сектором;
- нормативно-правову адаптацію, включаючи гармонізацію з директивами ЄС (NIS2), розробку спеціального закону про кібердипломатію та правове врегулювання поняття цифрової агресії;
- розширення міжнародної присутності України, через поглиблення співпраці з міжнародними організаціями, просування національних ініціатив, участь у формуванні глобальних правил поведінки в кіберпросторі.

Загалом, дослідження підтвердило, що кібердипломатія стає необхідним інструментом для забезпечення цифрової безпеки та зовнішньополітичної суб’єктності держави в XXI столітті. В умовах гібридної війни та зростаючої кількості транснаціональних кіберзагроз її ефективний розвиток є не лише актуальним, але й життєво важливим для збереження державного суверенітету та формування позитивного міжнародного іміджу України.

На основі результатів дослідження теми «Механізми кібердипломатії як засоби формування міжнародних відносин для національної безпеки держави»

сформульовано комплекс практичних заходів, реалізація яких дозволить підвищити ефективність державної політики України в цій сфері, посилити її міжнародну суб'єктність та стійкість до сучасних кіберзагроз.

1. Інституціалізація кібердипломатії на рівні державної стратегії
    - Рекомендовано завершити розробку та затвердити Стратегію кібердипломатії України на 2025–2030 роки, ініційовану Міністерством закордонних справ. Вона має стати рамковим документом, що закріплює пріоритети держави в цифровому вимірі зовнішньої політики.
    - До структури документа варто включити: оцінку загроз, стратегічні цілі, ключових партнерів, індикатори ефективності, механізми реалізації.
    - За зразок можна взяти Стратегію цифрової зовнішньої політики ЄС (2021), Cyber Diplomacy Toolbox Європейської ради, Стратегію США в сфері кібербезпеки (2023).
2. Створення міжвідомчого координаційного органу
    - Запропоновано створити Раду з питань кібердипломатії при РНБО України з чітко визначеними повноваженнями.
    - Такий орган має забезпечувати координацію між МЗС, СБУ, ДССЗЗІ, Мінцифри, СЗРУ, НАБУ, ГУР МО та представниками ІТ-сектору.
    - Функції: аналіз кіберінцидентів, формування міжнародної позиції, підготовка до переговорів, розробка рішень щодо дипломатичних відповідей на цифрову агресію.
3. Впровадження інституту цифрових аташе
    - Впровадити посади аташе з питань кібербезпеки та цифрової дипломатії у ключових дипломатичних місіях України (США, Естонія, Бельгія, Канада, Польща, штаб-квартира НАТО в Брюсселі).

- Такі аташе можуть стати каналом оперативного обміну інформацією про кібератаки, забезпечувати двосторонню експертну взаємодію, організовувати міжнародну допомогу (аналогічну до програми EU Cyber Rapid Response Teams).

4. Розвиток системи підготовки кадрів
   - На базі Дипломатичної академії України, КПІ, НТУ «ХПІ», Львівської політехніки, Харківського університету внутрішніх справ розробити освітньо-професійні програми за напрямом “Кібердипломатія”.
   - Програма має включати модулі з міжнародного права, кібербезпеки, аналізу даних, цифрових технологій, практики багатосторонніх переговорів.
   - Організувати стажування в CCDCOE (НАТО), ENISA (ЄС), EU CyberNet, а також у Департаменті кіберсправ МЗС Естонії — одного з лідерів у цій сфері.
5. Законодавче закріплення інструментів кібердипломатії
   - Підготувати проєкт закону «Про кібердипломатію», в якому:
     - визначити основні поняття (цифрова агресія, кіберзлочин, дипломатична відповідь у кіберпросторі),
     - закріпити повноваження органів,
     - передбачити механізм реагування на міжнародні інциденти,
     - запровадити статус цифрового інциденту як приводу для міжнародно-правових дій (аналог статті 51 Статуту ООН щодо самооборони).
   - Закон має бути узгоджений із Законом України «Про основи національної безпеки», Стратегією кібербезпеки України (Указ Президента №447/2021), а також актами міжнародного права.
6. Активізація участі в глобальних кіберініціативах

- Забезпечити системну участь делегацій України у GGE та OEWG ООН, IGF, CCDCOE, EU Cyber Forum, що дозволяє впливати на формування глобальних норм.
- Ініціювати розробку міжнародного механізму притягнення до відповідальності за кіберзлочини, зокрема створення трибуналу або арбітражного органу у справах цифрової агресії.

7. Публічно-приватне партнерство

- Створити Національний цифровий консорціум за участі держави, ключових українських та міжнародних IT-компаній (Google, Microsoft, Cisco, Cloudflare, SoftServe, EPAM, Ajax Systems).
- Його завдання: спільне вироблення політик реагування на кіберзагрози, експертна допомога, аналітична підтримка МЗС, розробка проєктів у сфері цифрової стійкості, зокрема кіберштучного інтелекту (AI for Diplomacy).
- Загальний практичний результат
- Упровадження зазначених рекомендацій дозволить Україні:
- забезпечити комплексний захист національних інтересів у цифровому середовищі;
- підвищити дипломатичну присутність у глобальних кіберпроцесах;
- розбудувати внутрішній потенціал реагування на кіберзагрози;
- перейти від реактивного до проактивного формату кібердипломатії.

У довгостроковій перспективі це сприятиме формуванню інституційної спроможності України як цифрової держави з чітко визначеним міжнародним статусом у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Український дипломатичний огляд. Кібердипломатія: виклики та перспективи розвитку // Український дипломатичний огляд. – № 68, 2023. – [Електронний ресурс]. – Режим доступу: https://ud.gdip.com.ua/wp-content/uploads/2023/12/68_2023.pdf

2. Christou, G. Cyber Diplomacy: From Concept to Practice. – Tallinn Paper No. 14, NATO CCDCOE, 2023. – [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

3. Klimburg, A. (Ed.). Confidence-Building Measures in Cyberspace: Current Debates and Trends // International Cyber Norms: Legal, Policy & Industry Perspectives. – NATO CCDCOE, 2017. – Chapter 7. – [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch7.pdf

4. Salvi, A., Tiirmaa-Klaar, H., & Lewis, J. A. (Eds.). A Handbook for the Practice of Cyber Diplomacy. – Luxembourg: Publications Office of the European Union, 2024. – [Електронний ресурс]. – Режим доступу: https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/APafQ4IV/a-handbook-for-the-practice-of-cyber-diplomacy.pdf

5. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26 серпня 2021 року. – [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/4472021-40013

6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). – [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

7. Міністерство закордонних справ України. Відділ кібердипломатії. – [Електронний ресурс]. – Режим доступу: https://mfa.gov.ua/pro-ministerstvo/struktura/strukturni-pidrozdili/viddil-kiberdiplomatiyi

8. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"» від 14 вересня 2020 року. – [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/3922020-35037

9. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки, схвалена розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. – [Електронний ресурс]. – Режим доступу: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi

10. Міністерство цифрової трансформації України. Цифрова трансформація сектору безпеки і оборони України (2021–2024). – [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/news/cifrova-transformatsiya-sektoru-bezpeki-i-oboroni-ukraini-prezentatsiya-programi

11. Закон України «Про Національну програму інформатизації» від 1 грудня 2022 р. № 2807-IX. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/2807-20

12. United Nations Office for Disarmament Affairs (UNODA). Developments in the field of information and telecommunications in the context of international security – GGE and OEWG reports. – [Електронний ресурс]. – Режим доступу: https://www.un.org/disarmament/ict-security/

13. Organization for Security and Co-operation in Europe (OSCE). Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the

Use of ICTs. – [Електронний ресурс]. – Режим доступу: https://www.osce.org/cyber-ict-security

14. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Locked Shields, Cyber Defence Exercises, and Ukraine's Partnership. – [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/

15. European Union Agency for Cybersecurity (ENISA). EU-Ukraine Cybersecurity Cooperation and NIS2 Directive Implementation. – [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/

16. U.S. Department of State – Bureau of Cyberspace and Digital Policy. The 2024 U.S.-Ukraine Cyber Dialogue. – [Електронний ресурс]. – Режим доступу: https://2021-2025.state.gov/the-2024-u-s-ukraine-cyber-dialogue/

17. e-Governance Academy. Digital Transformation for Ukraine (DT4UA). – [Електронний ресурс]. – Режим доступу: https://ega.ee/project/dt4ua/

18. National Cyber Security Centre (UK). The NCSC, working with... – [Електронний ресурс]. – Режим доступу: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/overview/the-ncsc-working-with

19. Israel National Cyber Directorate (INCD). Ukraine-Israel Cybersecurity Collaboration. – [Електронний ресурс]. – Режим доступу: https://www.gov.il/en/departments/israel_national_cyber_directorate

20. CyberPeace Institute. Cyber Dimensions of the Armed Conflict in Ukraine – Q3 2023. – [Електронний ресурс]. – Режим доступу: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2023/

21. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

22. Стратегія кібербезпеки України, затверджена Указом Президента України № 447/2021 від 26.08.2021. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021

23. Статут Організації Об’єднаних Націй. – [Електронний ресурс]. – Режим доступу: https://www.un.org

24. Cybersecurity Strategy of the European Union. The EU’s Cybersecurity Strategy for the Digital Decade. – Brussels, 2020. – [Електронний ресурс]. – Режим доступу: https://digital-strategy.ec.europa.eu

25. NATO CCDCOE – Cooperative Cyber Defence Centre of Excellence. – [Електронний ресурс]. – Режим доступу: https://ccdcoe.org

26. European External Action Service (EEAS). EU Cyber Diplomacy Toolbox. – [Електронний ресурс]. – Режим доступу: https://www.eeas.europa.eu

27. Ministry of Foreign Affairs of Estonia. Cyber Diplomacy Unit. – [Електронний ресурс]. – Режим доступу: https://vm.ee/en

28. Cyber Diplomacy: Managing Security and Governance Online / Ed. by N. Choucri. – Cambridge, MA: MIT Press, 2018. – 298 p.

29. Українська школа урядування. Аналітична записка «Цифрова дипломатія: виклики та перспективи». – Київ, 2022.

30. Український інститут майбутнього. Звіт «Кібердипломатія як інструмент безпеки». – Київ, 2023. – [Електронний ресурс]. – Режим доступу: https://uifuture.org

31. Official Journal of the European Union. Directive (EU) 2022/2555 (NIS2 Directive). – [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu

32. United Nations Office for Disarmament Affairs (UNODA). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. – [Електронний ресурс]. – Режим доступу: https://www.un.org/disarmament

33. Міністерство цифрової трансформації України. Дорожня карта цифрової безпеки. – Київ, 2023. – [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua