Харківський національний університет імені В. Н. Каразіна
ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу» Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «ЦИФРОВА ДИПЛОМАТІЯ НІМЕЧЧИНИ ЯК ІНСТРУМЕНТ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Виконала:
студентка 2 курсу, групи УМІБ-61
другого (магістерського) рівня вищої освіти,
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Гадючко Тетяна Євгенівна
(прізвище, ім'я по батькові)

Керівник:
д.п.н, професор Шамраєва В.М.
(науковий ступінь, вчене звання, прізвище, ім'я по батькові)

Рецензент:
д.держ.упр., проф. Дзюндзюк В.Б.
(науковий ступінь, вчене звання, прізвище, ім'я по батькові)

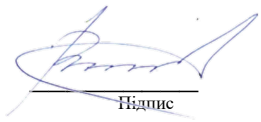
ХАРКІВ – 2025 рік

Харківський національний університет імені В. Н. Каразіна

ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ

Завідувач кафедри



Підпис

Наталія ВІННИКОВА

ініціали, прізвище

«2» червня 2025року

(зі змінами від 10.09.2025, 06.10.2025)

ЗАВДАННЯ

на кваліфікаційну роботу магістра

Гадючко Тетяни Євгенівни

(прізвище, ім'я та по батькові)

1. Тема роботи «Цифрова дипломатія Німеччини як інструмент формування інформаційної безпеки»

керівник роботи Шамраєва Валентина Михайлівна, д.п.н., професор

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 (зі змінами від «10» вересня 2025 року № 4001-5/3049; «6» жовтня 2025 року № 4001-5/3656.

2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 року

3. Перелік питань, які потрібно розробити:

з’ясувати концептуальні засади цифрової дипломатії та інформаційної безпеки у сучасній системі міжнародних відносин; виявити специфіку формування німецької цифрової дипломатії; розкрити інституційну структуру забезпечення цифрової дипломатії та інформаційної безпеки Німеччини; визначити практичні інструменти німецької цифрової дипломатії у сфері інформаційної безпеки; встановити вплив німецької цифрової дипломатії на формування європейського інформаційного порядку; обґрунтувати рекомендації щодо використання німецького досвіду для зміцнення інформаційної безпеки України.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	12.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	22.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання здобувачем завершеної КРМ науковому керівнику для перевірки та оформлення відгуку	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-29.11.2025
8	Доопрацювання роботи, прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Підготовка до захисту та захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання: 02 червня 2025 року (10.09.2025; 06.10.2025)

Студент (підпис) Тетяна ГАДЮЧКО (ініціали, прізвище)

Керівник роботи (підпис) Валентина ШАМРАЄВА (ініціали, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Трансформація глобального комунікаційного середовища внаслідок стрімкої цифровізації кардинально змінила характер міжнародних відносин та створила принципово нові виклики для національної безпеки держав, де інформаційний простір перетворився на арену стратегічної конкуренції між державами та недержавними акторами, а здатність ефективно використовувати цифрові технології для просування національних інтересів стала критично важливою складовою зовнішньої політики сучасних держав. Цифрова дипломатія як новий феномен міжнародних відносин органічно поєднує традиційні дипломатичні практики з можливостями інформаційно-комунікаційних технологій для досягнення зовнішньополітичних цілей, формування сприятливого міжнародного іміджу та забезпечення інформаційної безпеки держави в умовах глобалізованого цифрового простору. Особливої актуальності дослідження цифрової дипломатії як інструменту забезпечення інформаційної безпеки набуває в контексті масштабних дезінформаційних кампаній, кібератак на критичну інфраструктуру та спроб іноземного втручання у демократичні процеси, які стали характерними рисами сучасного міжнародного безпекового середовища та загрожують стабільності демократичних інститутів і соціальній згуртованості суспільств.

Ступінь наукової розробленості проблеми. Теоретичні засади цифрової дипломатії досліджували зарубіжні науковці, зокрема Корнеліу Бйола та Ілан Манор, які концептуалізували цифрову дипломатію як стратегічне використання цифрових технологій для досягнення дипломатичних цілей, Філіпп Сейб, який проаналізував трансформацію дипломатії в епоху соціальних медіа, а також Аманда Сандре, яка дослідила інноваційні практики цифрової дипломатії провідних держав світу. Питання інформаційної безпеки в контексті міжнародних відносин вивчали Александер Клімбург, який запропонував комплексну концепцію кібербезпеки та інформаційної війни, Майкл Шмітт, редактор Талліннського керівництва з міжнародного права, застосовного до кібероперацій, а також Пітер Сінгер та Аллан Фрідман, які дослідили феномен кібервійни та її наслідки для міжнародної безпеки. Німецький досвід цифрової

політики та кібербезпеки аналізували Аннеґрет Бендієк, Мартін Ремер та Свен Херпіг, які вивчали еволюцію німецької стратегії кібербезпеки та інституційні механізми її реалізації.

Українські науковці також зробили вагомий внесок у дослідження цифрової дипломатії та інформаційної безпеки, зокрема Володимир Горбулін розробив концептуальні засади інформаційної безпеки України в умовах гібридної війни, Дмитро Дубов проаналізував проблеми концептуалізації та практичної реалізації стратегічних комунікацій, Георгій Почепцов дослідив феномен сучасних інформаційних воєн, а Олена Тимошенко вивчала цифрову дипломатію як інструмент зовнішньої політики сучасних держав. Водночас варто зазначити, що в українській науці бракує комплексних досліджень, присвячених саме німецькому досвіду використання цифрової дипломатії для забезпечення інформаційної безпеки, а також аналізу можливостей адаптації цього досвіду для потреб України в умовах російської інформаційної агресії. Існуючі дослідження або зосереджуються на окремих аспектах цифрової дипломатії без достатньої уваги до питань інформаційної безпеки, або аналізують інформаційну безпеку без систематичного розгляду ролі цифрової дипломатії як інструменту її забезпечення, що зумовлює необхідність комплексного дослідження взаємозв'язку між цими двома феноменами на прикладі німецької практики.

Мета дослідження полягає у з'ясуванні ролі цифрової дипломатії Німеччини як інструменту забезпечення інформаційної безпеки та обґрунтуванні напрямів адаптації німецького досвіду для зміцнення інформаційної стійкості України.

Завдання дослідження визначено відповідно до мети та структури роботи і включають:

- з'ясувати концептуальні засади цифрової дипломатії та інформаційної безпеки у сучасній системі міжнародних відносин;
- виявити специфіку формування німецької цифрової дипломатії;
- розкрити інституційну структуру забезпечення цифрової дипломатії та інформаційної безпеки Німеччини;

- визначити практичні інструменти німецької цифрової дипломатії у сфері інформаційної безпеки;
- встановити вплив німецької цифрової дипломатії на формування європейського інформаційного порядку;
- обґрунтувати рекомендації щодо використання німецького досвіду для зміцнення інформаційної безпеки України.

Об'єктом дослідження є цифрова дипломатія як інструмент зовнішньої політики держав у сучасній системі міжнародних відносин.

Предметом дослідження виступає цифрова дипломатія Німеччини у її взаємозв'язку з формуванням інформаційної безпеки держави та європейського інформаційного порядку.

Методи дослідження сформована на основі комплексного використання теорій міжнародних відносин та спеціалізованих методів політичної науки для всебічного аналізу досліджуваної проблеми. Теоретичну основу роботи становлять неореалізм, який використано для аналізу конкурентного характеру інформаційного простору та ролі держав у забезпеченні власної інформаційної безпеки через розвиток національних спроможностей, неолібералізм, що дозволив виявити потенціал міжнародної кооперації та роль інституцій у формуванні режимів співробітництва у сфері інформаційної безпеки, конструктивізм, застосований для розуміння процесів формування норм та ідентичностей у цифровому просторі через дипломатичні практики, а також комунікативна теорія міжнародних відносин, яка забезпечила концептуальні рамки для аналізу раціональної комунікації у цифровій дипломатії. Додатково використано концепції інформаційної стійкості та стратегічних комунікацій для операційного аналізу практичних механізмів використання цифрової дипломатії в цілях зміцнення інформаційної безпеки.

Методологічну основу дослідження становлять загальнонаукові та спеціалізовані методи політичної науки, застосовані відповідно до специфіки завдань кожного розділу роботи. Системний метод використано для аналізу цифрової дипломатії та інформаційної безпеки як взаємопов'язаних елементів єдиної системи національної безпеки держави та для виявлення структурних

зв’язків між різними компонентами німецької системи забезпечення інформаційної безпеки. Історичний метод застосовано для дослідження еволюції німецької цифрової дипломатії та виявлення ключових етапів її формування під впливом технологічних змін та зростаючих інформаційних загроз. Порівняльний метод використано для зіставлення німецької моделі цифрової дипломатії з практиками інших провідних держав та виявлення унікальних характеристик німецького підходу. Інституційний метод дозволив проаналізувати організаційну структуру німецької системи забезпечення цифрової дипломатії та інформаційної безпеки, розподіл повноважень між різними відомствами та механізми міжвідомчої координації. Метод контент-аналізу застосовано для вивчення офіційних стратегічних документів Німеччини та Європейського Союзу у сфері цифрової політики, кібербезпеки та протидії дезінформації з метою виявлення ключових концептуальних підходів та пріоритетів. Метод кейс-стаді використано для детального аналізу конкретних випадків застосування Німеччиною інструментів цифрової дипломатії для протидії інформаційним загрозам та формування європейської політики у сфері інформаційної безпеки.

Інформаційну базу дослідження становлять різноманітні типи джерел, що забезпечують емпіричне підґрунтя для аналізу. До нормативно-правових джерел належать стратегії кібербезпеки Німеччини, законодавчі акти Європейського Союзу у сфері цифрової політики та захисту даних, включно з Загальним регламентом захисту даних, Актом про цифрові послуги, Директивою про мережеву та інформаційну безпеку, а також міжнародні документи з питань кібербезпеки та інформаційної безпеки, розроблені в рамках ООН, ОБСЄ та НАТО. Аналітичні та статистичні матеріали включають звіти провідних аналітичних центрів, таких як Німецький інститут міжнародної політики та безпеки, Європейський центр досліджень і документації з безпеки та оборони, аналітичні доповіді Європейської комісії та Європейської служби зовнішніх дій про стан інформаційної безпеки ЄС, звіти Федерального відомства з інформаційної безпеки Німеччини та Агенції Європейського Союзу з кібербезпеки про кіберзагрози, а також дані моніторингу дезінформаційних

кампаній, проведеного Групою стратегічних комунікацій ЄС. Наукові джерела охоплюють монографії провідних зарубіжних та вітчизняних дослідників цифрової дипломатії та інформаційної безпеки, статті у високорейтингових наукових журналах, дисертаційні дослідження з відповідної проблематики, а також матеріали міжнародних конференцій з питань кібербезпеки та цифрової дипломатії. Емпіричну базу доповнюють офіційні веб-сайти Федерального міністерства закордонних справ Німеччини, Європейської служби зовнішніх дій, акаунти німецьких дипломатичних представництв у соціальних мережах, публікації у німецьких та європейських медіа про інформаційну безпеку, а також експертні інтерв'ю та публічні виступи німецьких політиків і дипломатів з питань цифрової зовнішньої політики та кібербезпеки.

Практичне значення результатів дослідження полягає у можливості їх використання у кількох напрямах професійної діяльності та освітнього процесу. Результати дослідження можуть бути застосовані у практиці української публічної дипломатії для розробки стратегій цифрової комунікації з міжнародними аудиторіями, удосконалення механізмів протидії російській дезінформації та зміцнення інформаційної стійкості українського суспільства на основі адаптації німецького та європейського досвіду до специфіки українського контексту. Матеріали роботи можуть бути використані у діяльності Міністерства закордонних справ України, Міністерства цифрової трансформації, Служби безпеки України та інших державних органів, відповідальних за інформаційну безпеку держави, для розробки відповідних стратегічних документів, навчальних програм підготовки фахівців та механізмів міжвідомчої координації у сфері цифрової дипломатії. Висновки та рекомендації дослідження можуть бути враховані органами державної влади, що відповідають за євроінтеграційні процеси, для гармонізації українського законодавства з європейськими стандартами у сфері цифрової політики, кібербезпеки та захисту даних, а також для поглиблення співпраці з європейськими партнерами у протидії спільним інформаційним загрозам. Результати роботи можуть бути використані у розробленні освітніх курсів та навчальних програм з цифрової дипломатії, міжнародної інформаційної безпеки, стратегічних комунікацій та публічної

дипломатії для підготовки фахівців у галузі міжнародних відносин та національної безпеки у вищих навчальних закладах України.

Апробація результатів дослідження відбувалася на всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу», до якого були підготовлені тези за темою «Цифрова дипломатія Німеччини як інструмент зміцнення інформаційної безпеки України».

Структура роботи зумовлена метою, завданнями та логікою дослідження. Магістерська кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел. Загальний обсяг роботи становить 112 сторінок, з них основного тексту 105 сторінок. Список використаних джерел складає 73 найменування.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЦИФРОВОЇ ДИПЛОМАТІЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття та еволюція цифрової дипломатії у сучасній системі міжнародних відносин

Трансформація глобального комунікаційного простору в останні два десятиліття кардинально змінила характер взаємодії держав на міжнародній арені, що зумовило виникнення принципово нових форм дипломатичної практики, котрі органічно поєднують традиційні інструменти зовнішньої політики із можливостями цифрових технологій. Цифрова дипломатія як феномен сучасних міжнародних відносин постала результатом конвергенції технологічного прогресу та еволюції дипломатичних практик, внаслідок чого виникла якісно нова парадигма міждержавної комунікації, яка передбачає використання інформаційно-комунікаційних технологій для досягнення зовнішньополітичних цілей держави та формування сприятливого міжнародного іміджу.

Концептуалізація цифрової дипломатії як самостійного напряму наукових досліджень розпочалася на межі XX та XXI століть, коли дослідники почали фіксувати якісні зміни у способах здійснення дипломатичної діяльності під впливом інтернет-технологій та соціальних мереж [40]. У науковому дискурсі склалося кілька підходів до визначення сутності цього явища, які варіюються від вузького трактування цифрової дипломатії як використання соціальних медіа у зовнішній політиці до широкого розуміння її як комплексної системи цифрових інструментів та стратегій, спрямованих на реалізацію національних інтересів у глобальному інформаційному просторі. Британський дослідник Корнеліу Бйола визначає цифрову дипломатію як стратегічне використання цифрових технологій для досягнення дипломатичних цілей, підкреслюючи при цьому, що ефективність такої діяльності залежить від здатності держави адаптувати традиційні дипломатичні практики до специфіки цифрового середовища [59, с. 34]. Натомість німецькі дослідники схильні розглядати цифрову дипломатію як інтегральну частину публічної дипломатії, що передбачає не лише комунікацію з зарубіжними аудиторіями через цифрові канали, а й формування стійких мереж

взаємодії між державними та недержавними акторами міжнародних відносин.

Еволюційний розвиток цифрової дипломатії можна умовно поділити на кілька етапів, кожен з яких характеризується специфічними технологічними можливостями та дипломатичними практиками, що відображають загальні тенденції цифровізації суспільства та трансформації міжнародного порядку. Перший етап, що охоплює період з середини 1990-х до початку 2000-х років, позначився створенням офіційних веб-сайтів міністерств закордонних справ та дипломатичних представництв, які слугували переважно інформаційними платформами для одностороннього поширення офіційної позиції держави без можливості інтерактивної взаємодії з аудиторією [73, с. 78]. Другий етап, що розпочався приблизно з 2008 року та тривав до середини 2010-х років, характеризувався активним освоєнням дипломатичними відомствами соціальних мереж, насамперед Twitter та Facebook, які дозволили перейти від односторонньої трансляції інформації до діалогу з міжнародною спільнотою та формування прямих каналів комунікації з зарубіжними громадянами. Сучасний, третій етап розвитку цифрової дипломатії відзначається комплексним використанням різноманітних цифрових платформ, включно з відеохостингами, месенджерами та спеціалізованими застосунками, а також застосуванням технологій штучного інтелекту, великих даних та алгоритмічної аналітики для таргетованого впливу на цільові аудиторії та моніторингу міжнародного інформаційного простору [50].

Функціональне призначення цифрової дипломатії виходить за межі простої технологічної модернізації традиційних дипломатичних практик і передбачає якісну трансформацію способів реалізації зовнішньої політики держави в умовах інформаційного суспільства, де швидкість поширення інформації та можливість прямого доступу до глобальних аудиторій створюють нові можливості й виклики для державних акторів. Дослідники виділяють кілька ключових функцій цифрової дипломатії, серед яких особливе значення мають інформаційна функція, що передбачає оперативне донесення офіційної позиції держави до міжнародної спільноти та формування порядку денного у публічному просторі, комунікативна функція, яка забезпечує діалог з

іноземними громадянами та недержавними акторами, та репутаційна функція, спрямована на формування позитивного іміджу держави на міжнародній арені [39, с. 112]. Окрім цього, дедалі важливішого значення набуває функція раннього попередження та кризового реагування, коли цифрові платформи використовуються для оперативного інформування про загрози, координації дій під час надзвичайних ситуацій та спростування дезінформації, що особливо актуально в контексті гібридних війн та інформаційних конфліктів сучасності.

Теоретичне осмислення цифрової дипломатії вимагає звернення до різноманітних концептуальних рамок, які дозволяють проаналізувати це явище з різних методологічних позицій та виявити його багатовимірну природу у системі міжнародних відносин. Представники неореалістичної школи схильні розглядати цифрову дипломатію як новий інструмент у боротьбі за владу та вплив у міжнародній системі, де держави використовують цифрові технології для максимізації свого відносного могутності та забезпечення національної безпеки в умовах анархічного міжнародного середовища, при цьому особлива увага приділяється асиметріям у доступі до цифрових технологій та можливостям їх використання для зміни балансу сил [62, с. 45]. Неоліберальстський підхід акцентує увагу на кооперативному потенціалі цифрової дипломатії, підкреслюючи її роль у формуванні міжнародних режимів, стимулюванні транснаціональних мереж взаємодії та зниженні трансакційних витрат міжнародної комунікації, що сприяє зміцненню міжнародної кооперації навіть в умовах конфліктності інтересів окремих держав. Конструктивістська перспектива пропонує розглядати цифрову дипломатію як механізм формування ідентичностей та нормативних структур у міжнародних відносинах, де через цифрові комунікації конструюються смисли, транслюються цінності та формуються спільні уявлення про легітимні форми міжнародної взаємодії.

Місце цифрової дипломатії у загальній архітектурі зовнішньої політики сучасних держав визначається її здатністю доповнювати та підсилювати традиційні дипломатичні інструменти, створюючи синергетичний ефект від поєднання класичних методів міждержавної взаємодії з можливостями цифрових технологій для досягнення стратегічних національних інтересів. У структурі

зовнішньополітичного механізму провідних держав світу цифрова дипломатія інституціоналізується через створення спеціалізованих підрозділів у міністерствах закордонних справ, призначення цифрових послів та амбасадорів у соціальних мережах, розробку комплексних стратегій цифрової комунікації та виділення значних бюджетних ресурсів на розвиток цифрових дипломатичних можливостей [72]. Німеччина як одна з провідних європейських держав демонструє системний підхід до інтеграції цифрової дипломатії у свою зовнішню політику, що виявляється у створенні спеціалізованих структур у Федеральному міністерстві закордонних справ, розробці стратегічних документів з цифрової політики та активному використанні соціальних мереж для просування німецьких інтересів на міжнародній арені. При цьому німецький підхід характеризується особливою увагою до питань цифрової етики, захисту персональних даних та забезпечення демократичної легітимності цифрових дипломатичних практик, що відображає загальноєвропейські цінності та принципи регулювання цифрового простору.

Ефективність цифрової дипломатії як інструменту зовнішньої політики залежить від множини факторів, серед яких ключове значення мають технологічні можливості держави, рівень цифрової грамотності населення, якість цифрової інфраструктури та здатність дипломатичного відомства адаптуватися до швидкозмінного цифрового середовища [52, с. 156]. Водночас варто враховувати, що цифрова дипломатія породжує і специфічні виклики для держав, включно з необхідністю забезпечення кібербезпеки дипломатичних комунікацій, протидії дезінформації та маніпуляціям у цифровому просторі, збалансування між відкритістю цифрової комунікації та збереженням конфіденційності дипломатичної діяльності, а також управління репутаційними ризиками в умовах миттєвого поширення інформації та вірусності контенту. Сучасні дослідження свідчать, що успішна цифрова дипломатія вимагає не лише технологічної оснащеності, а й глибокого розуміння специфіки цифрового середовища, культурних особливостей різних онлайн-спільнот та здатності до швидкого реагування на динамічні зміни в інформаційному просторі, що потребує постійного навчання дипломатичних кадрів та розвитку нових

компетенцій у сфері цифрових комунікацій.

Аналіз сучасних тенденцій розвитку цифрової дипломатії дозволяє стверджувати, що вона поступово трансформується від тактичного інструменту комунікації до стратегічного компоненту національної безпеки та зовнішньої політики, що вимагає системної інтеграції цифрового виміру в усі напрями дипломатичної діяльності держави [55]. Провідні держави світу дедалі більше усвідомлюють важливість цифрової присутності та впливу у глобальному інформаційному просторі, що знаходить відображення у значних інвестиціях у розвиток цифрових дипломатичних можливостей, створенні спеціалізованих навчальних програм для дипломатів та розробці довгострокових стратегій цифрової зовнішньої політики. Особливістю сучасного етапу є також зростання значення багатосторонньої цифрової дипломатії, коли держави координують свої зусилля у цифровому просторі для просування спільних інтересів та цінностей, що особливо характерно для Європейського Союзу, члени якого прагнуть сформувати єдиний європейський підхід до цифрової дипломатії та забезпечити узгоджене просування європейських цінностей у глобальному цифровому просторі.

Перспективи подальшого розвитку цифрової дипломатії пов’язані з впровадженням нових технологій, зокрема штучного інтелекту для аналізу великих масивів даних та прогнозування розвитку ситуації, використанням віртуальної та доповненої реальності для створення інноваційних форматів дипломатичної взаємодії, а також застосуванням блокчейн-технологій для забезпечення безпеки та прозорості цифрових дипломатичних комунікацій, що створює якісно нові можливості для реалізації зовнішньої політики держав у цифрову епоху [68, с. 203]. Водночас технологічний прогрес породжує і нові етичні дилеми та виклики, пов’язані з використанням алгоритмів для впливу на громадську думку, захистом приватності громадян у процесі цифрових дипломатичних взаємодій та забезпеченням демократичного контролю над діяльністю автоматизованих систем у сфері зовнішньої політики, що вимагає розробки відповідних нормативних рамок та етичних стандартів цифрової дипломатії.

Отже, цифрова дипломатія являє собою складний та багатовимірний феномен сучасних міжнародних відносин, який органічно поєднує традиційні дипломатичні практики з інноваційними можливостями цифрових технологій для досягнення зовнішньополітичних цілей держави, формування сприятливого міжнародного іміджу та забезпечення національних інтересів у глобальному інформаційному просторі. Еволюція цифрової дипломатії від простих веб-сайтів до комплексних цифрових екосистем відображає загальні процеси цифровізації суспільства та трансформації міжнародного порядку, внаслідок чого цифровий вимір стає невід'ємною складовою зовнішньої політики провідних держав світу. Німеччина як одна з найбільш технологічно розвинених країн Європи демонструє послідовний підхід до розбудови власних цифрових дипломатичних можливостей, поєднуючи технологічні інновації з традиційними європейськими цінностями демократії, верховенства права та захисту прав людини, що робить німецький досвід цифрової дипломатії особливо цікавим для дослідження у контексті формування інформаційної безпеки. Розуміння сутності, функцій та еволюції цифрової дипломатії створює необхідне теоретичне підґрунтя для подальшого аналізу її ролі як інструменту забезпечення інформаційної безпеки, що потребує звернення до концептуальних засад самої категорії інформаційної безпеки та її місця в системі національної та міжнародної безпеки.

1.2. Інформаційна безпека як складова національної та міжнародної безпеки

Трансформація глобального безпекового середовища в умовах стрімкої цифровізації всіх сфер суспільного життя зумовила виникнення принципово нових загроз та викликів, які виходять за межі традиційного розуміння національної безпеки та вимагають переосмислення самої сутності безпеки в контексті інформаційного суспільства, де інформація та контроль над нею стають стратегічним ресурсом, а інформаційний простір перетворюється на арену міждержавного суперництва та конфлікту. Інформаційна безпека як відносно новий концепт у теорії та практиці міжнародних відносин поступово

кристалізувалася протягом останніх трьох десятиліть у відповідь на зростаючу залежність держав від інформаційно-комунікаційних технологій та усвідомлення вразливості критичної інфраструктури перед кібератаками, дезінформаційними кампаніями та іншими формами інформаційної агресії, що здатні завдати державі збитків, порівнянних з наслідками традиційних воєнних операцій.

Концептуалізація інформаційної безпеки у науковому дискурсі відбувалася паралельно з розвитком інформаційних технологій та усвідомленням їхнього впливу на міжнародну та національну безпеку, внаслідок чого сформувалися різні підходи до визначення цього поняття, які відображають національні особливості сприйняття інформаційних загроз та культурно-історичні традиції різних держав [57, с. 67]. Західний підхід до інформаційної безпеки, який домінує в документах Європейського Союзу та країн НАТО, традиційно акцентує увагу на захисті інформаційно-комунікаційних систем від несанкціонованого доступу, кібератак та технічних збоїв, розглядаючи інформаційну безпеку переважно через призму технологічної захищеності цифрової інфраструктури та забезпечення конфіденційності, цілісності й доступності інформації. Натомість у пострадянському просторі, включно з Україною, інформаційна безпека традиційно розумілася ширше та охоплювала не лише технічні аспекти захисту інформаційних систем, а й питання збереження національного інформаційного суверенітету, протидії інформаційній агресії та забезпечення інформаційно-психологічної стійкості суспільства перед зовнішніми впливами. Сучасне розуміння інформаційної безпеки в німецькому контексті органічно поєднує технічні аспекти кібербезпеки з питаннями захисту демократичних інститутів від дезінформації та зовнішнього втручання, що відображає комплексний характер інформаційних загроз у сучасному світі та необхідність багатовимірної відповіді на них [67].

Структура інформаційної безпеки характеризується складністю та багаторівневістю, оскільки охоплює різноманітні виміри захисту інформаційного простору від потенційних загроз та забезпечення стійкого функціонування інформаційно-комунікаційних систем в умовах деструктивних

впливів різної природи та інтенсивності. Технічний вимір інформаційної безпеки передбачає забезпечення захисту апаратних та програмних компонентів інформаційних систем від кібератак, зловмисного програмного забезпечення та технічних несправностей, що вимагає впровадження сучасних технологій захисту інформації, регулярного оновлення програмного забезпечення та навчання персоналу основам кібергігієни [45, с. 89]. Юридичний вимір охоплює створення нормативно-правової бази для регулювання відносин в інформаційній сфері, встановлення відповідальності за порушення інформаційної безпеки та забезпечення міжнародної співпраці у боротьбі з кіберзлочинністю, при цьому особливої актуальності набувають питання гармонізації національних законодавств різних держав та формування міжнародних правових режимів регулювання кіберпростору. Організаційний вимір стосується створення інституційних структур та механізмів забезпечення інформаційної безпеки на національному, регіональному та міжнародному рівнях, включно зі спеціалізованими державними агенціями, координаційними центрами реагування на кіберінциденти та багатосторонніми платформами співробітництва у сфері інформаційної безпеки.

Особливої уваги заслуговує змістовий вимір інформаційної безпеки, який пов’язаний з якістю та достовірністю інформації, що циркулює в суспільстві, а також із захистом громадян від маніпулятивних впливів, дезінформації та пропаганди, котрі здатні підірвати соціальну стабільність та демократичні інститути держави [40, с. 134]. Цей вимір набуває особливої актуальності в контексті гібридних війн сучасності, коли інформаційні операції стають невід’ємною складовою воєнно-політичного протистояння між державами, а соціальні мережі перетворюються на поле битви за свідомість мільйонів людей та інструмент дестабілізації політичної ситуації в країнах-противниках. Німеччина як країна з трагічним історичним досвідом тоталітарної пропаганди приділяє особливу увагу змістовому виміру інформаційної безпеки, прагнучи при цьому знайти баланс між захистом суспільства від деструктивних інформаційних впливів та збереженням фундаментальних демократичних свобод, насамперед свободи слова та свободи преси, що робить німецький підхід

до регулювання інформаційного простору об’єктом пильної уваги міжнародної спільноти.

Інформаційна безпека тісно інтегрована в загальну систему національної безпеки держави і становить її невід’ємну складову, оскільки стабільне функціонування практично всіх критичних секторів національної економіки та державного управління залежить від безперебійної роботи інформаційно-комунікаційних систем, а вразливість інформаційної інфраструктури може призвести до каскадних ефектів у різних сферах життєдіяльності суспільства [69]. Енергетичний сектор, транспортна інфраструктура, фінансова система, охорона здоров’я та система державного управління сьогодні критично залежать від цифрових технологій, внаслідок чого кібератака на інформаційні системи однієї з цих сфер може спричинити масштабні збої в роботі інших секторів та створити загрозу для національної безпеки загалом. Дослідження сучасних інцидентів інформаційної безпеки, зокрема кібератак на енергетичну інфраструктуру України у 2015 та 2016 роках, атаки вірусу-шифрувальника WannaCry у 2017 році та численних випадків втручання в виборчі процеси демократичних країн, переконливо демонструють, що інформаційна безпека перестала бути суто технічною проблемою та перетворилася на стратегічне питання національної та міжнародної безпеки, яке вимагає скоординованих зусиль держав та міжнародних організацій.

Міжнародний вимір інформаційної безпеки набуває дедалі більшого значення в умовах глобалізації та взаємозалежності національних інформаційних інфраструктур, коли кіберінциденти в одній країні можуть миттєво поширитися на інші держави завдяки транскордонному характеру кіберпростору та глобальній інтеграції інформаційних систем [47, с. 178]. Транснаціональна природа інформаційних загроз зумовлює необхідність міжнародної співпраці у сфері інформаційної безпеки, оскільки жодна держава не спроможна самостійно забезпечити повноцінний захист свого інформаційного простору від зовнішніх загроз та ефективно протидіяти транснаціональній кіберзлочинності без координації зусиль з іншими країнами. Європейський Союз послідовно розбудовує багатосторонню архітектуру інформаційної безпеки

через прийняття загальноєвропейських директив та регламентів, створення спільних центрів реагування на кіберінциденти та розвиток механізмів обміну інформацією про кіберзагрози між державами-членами, демонструючи тим самим можливість ефективної регіональної інтеграції у сфері інформаційної безпеки навіть за умови збереження національного суверенітету окремих держав.

Глобалізація інформаційного простору породжує специфічні виклики для забезпечення інформаційної безпеки, серед яких особливе місце посідають асиметричність інформаційних загроз, коли навіть невеликі групи або окремі індивіди здатні завдати значної шкоди державним інформаційним системам, а також проблематика атрибуції кібератак, яка ускладнює притягнення винних до відповідальності та стримування потенційних агресорів у кіберпросторі [65]. Технічні можливості приховування справжнього джерела кібератак через використання проксі-серверів, мереж анонімізації та підробки цифрових слідів створюють сприятливе середовище для діяльності як недержавних кіберзлочинців, так і державних акторів, які використовують кібероперації як інструмент зовнішньої політики, прагнучи при цьому зберегти можливість правдоподібного заперечення своєї причетності до інцидентів. Саме тому питання розробки міжнародних норм відповідальної поведінки держав у кіберпросторі та створення механізмів контролю за дотриманням цих норм залишається одним з найбільш актуальних викликів сучасної міжнародної безпеки, попри численні зусилля ООН, ОБСЄ та інших міжнародних організацій з формування консенсусу щодо правил гри в цифровому середовищі.

Загрози інформаційному простору в умовах глобалізації характеризуються різноманітністю форм, масштабів та потенційних наслідків для національної безпеки держав, що вимагає комплексного підходу до їх класифікації та розуміння специфіки кожного типу загроз для розробки адекватних механізмів протидії [63, с. 201]. Технічні загрози охоплюють широкий спектр кібератак на інформаційні системи, включно з DDoS-атаками, спрямованими на порушення доступності онлайн-ресурсів через їх перевантаження штучно створеним трафіком, зловмисним програмним забезпеченням, що здатне викрадати конфіденційну інформацію або блокувати роботу комп’ютерних систем, та

таргетованими атаками на критичну інфраструктуру, які можуть призвести до масштабних збоїв у роботі життєво важливих систем держави. Змістовні загрози пов'язані з поширенням дезінформації, маніпулятивного контенту та пропаганди, що спрямовані на підрив довіри громадян до демократичних інститутів, розпалювання соціальних конфліктів та дестабілізацію політичної ситуації в країні, при цьому особливу небезпеку становлять coordinated inauthentic behavior у соціальних мережах, коли мережі ботів та фейкових акаунтів використовуються для штучної ампліфікації певних наративів та маніпулювання громадською думкою.

Особливістю сучасного етапу є конвергенція технічних та змістовних загроз у рамках комплексних гібридних операцій, коли кібератаки поєднуються з дезінформаційними кампаніями для досягнення максимального дестабілізуючого ефекту та підриву стійкості демократичних суспільств перед зовнішніми викликами [59, с. 156]. Досвід протистояння російській агресії демонструє, що сучасні інформаційні загрози не обмежуються виключно кіберпростором, а органічно інтегруються в загальну стратегію гібридної війни, де інформаційні операції доповнюють військові дії, економічний тиск та дипломатичні маневри, створюючи синергетичний ефект впливу на державу-ціль. Німеччина як одна з провідних європейських держав неодноразово ставала об'єктом російських інформаційних операцій, спрямованих на підрив єдності Європейського Союзу, послаблення трансатлантичних зв'язків та дискредитацію німецького політичного керівництва, що зумовило активізацію німецьких зусиль з розбудови власних можливостей забезпечення інформаційної безпеки та розвитку механізмів протидії іноземному інформаційному втручанню.

Аналіз сучасних тенденцій у сфері інформаційних загроз свідчить про зростання їх складності та витонченості, оскільки зловмисники активно використовують досягнення в галузі штучного інтелекту, машинного навчання та обробки великих даних для створення більш ефективних інструментів кібератак та маніпулювання громадською думкою [58]. Технологія дипфейків, яка дозволяє створювати гіперреалістичні відео та аудіозаписи з підробленим змістом, становить принципово нову загрозу для інформаційної безпеки,

оскільки підриває можливість відрізнити справжню інформацію від фальшивої та створює сприятливе середовище для дезінформації на якісно новому рівні достовірності фальсифікованого контенту. Алгоритми штучного інтелекту використовуються також для автоматизації створення та поширення дезінформаційного контенту, ідентифікації вразливостей в інформаційних системах та проведення таргетованих фішингових атак, що значно підвищує ефективність злочинних дій та ускладнює завдання захисників інформаційної безпеки.

Інституційна відповідь на інформаційні загрози на національному та міжнародному рівнях передбачає створення комплексної системи забезпечення інформаційної безпеки, яка охоплює нормативно-правове регулювання, організаційні структури, технічні засоби захисту та механізми міжнародної співпраці [38, с. 234]. Німеччина розбудувала розгалужену систему забезпечення інформаційної безпеки, ключовими елементами якої є Федеральне відомство з інформаційної безпеки, котре відповідає за технічний захист урядових інформаційних систем та координацію національних зусиль у сфері кібербезпеки, Федеральна служба захисту конституції, яка займається виявленням та протидією іноземному шпигунству в кіберпросторі, та спеціалізовані підрозділи в Міністерстві оборони, що забезпечують кіберзахист військової інфраструктури та розвивають наступальні кібероперативні можливості. На європейському рівні Німеччина активно підтримує ініціативи щодо зміцнення спільної кіберстійкості Європейського Союзу через імплементацію Директиви про мережеву та інформаційну безпеку, створення Європейського центру компетенції з кібербезпеки та розвиток механізмів спільного реагування на масштабні кіберінциденти, що загрожують безпеці кількох держав-членів одночасно.

Виклики забезпечення інформаційної безпеки в демократичних суспільствах пов’язані з необхідністю балансування між ефективним захистом від інформаційних загроз та збереженням фундаментальних громадянських свобод, насамперед права на приватність та свободу вираження поглядів, що становить складну етичну та політичну дилему для урядів західних демократій

[73, с. 267]. Авторитарні режими мають значно більше можливостей для контролю над інформаційним простором та обмеження інформаційних потоків на своїй території, тоді як демократичні держави мусять шукати більш витончені механізми захисту, які не порушують базових прав громадян та не створюють прецедентів для зловживань державною владою. Німецький досвід регулювання інформаційного простору, зокрема впровадження закону про покращення забезпечення правопорядку в соціальних мережах, який зобов'язує платформи оперативно видаляти незаконний контент, викликав інтенсивні дебати щодо меж допустимого державного втручання в цифрове середовище та ризиків надмірної цензури, що підкреслює складність знаходження оптимального балансу між безпекою та свободою в інформаційному суспільстві.

Перспективи розвитку системи забезпечення інформаційної безпеки пов'язані з подальшим удосконаленням технічних засобів захисту інформаційних систем, розвитком штучного інтелекту для виявлення та попередження кібератак, зміцненням міжнародної співпраці у боротьбі з транснаціональними кіберзагрозами та формуванням загальносвітового консенсусу щодо норм відповідальної поведінки держав у кіберпросторі [71]. Водночас технологічні рішення самі по собі не здатні забезпечити надійний захист від інформаційних загроз без розвитку цифрової грамотності населення, формування критичного мислення та стійкості громадян перед маніпулятивними впливами, а також без створення ефективних механізмів співпраці між державою, приватним сектором та громадянським суспільством у забезпеченні інформаційної безпеки. Особливої актуальності набуває питання підготовки кваліфікованих фахівців у сфері інформаційної безпеки, оскільки дефіцит експертів у цій галузі залишається однією з найбільших перешкод для ефективного захисту від кіберзагроз, а конкуренція за таланти між державним сектором та приватним бізнесом ускладнює формування державних кіберспроможностей.

Таким чином, інформаційна безпека становить критично важливу складову національної та міжнародної безпеки в сучасному світі, оскільки цифровізація всіх сфер життєдіяльності суспільства створює нові вразливості та загрози, які

можуть бути експлуатовані як недержавними злочинцями, так і ворожими державами для завдання шкоди національним інтересам та дестабілізації демократичних суспільств. Багатовимірна структура інформаційної безпеки охоплює технічні, юридичні, організаційні та змістовні аспекти захисту інформаційного простору, при цьому ефективне забезпечення інформаційної безпеки вимагає комплексного підходу, який поєднує технологічні рішення з розвитком інституційних спроможностей, міжнародною співпрацею та підвищенням інформаційної грамотності населення. Німеччина як провідна європейська держава розробила системний підхід до забезпечення інформаційної безпеки, який органічно поєднує захист від технічних кіберзагроз з протидією дезінформації та збереженням демократичних цінностей, що робить німецький досвід особливо цінним для розуміння можливостей використання цифрової дипломатії як інструменту зміцнення інформаційної безпеки, що потребує детального розгляду теоретичних підходів до аналізу взаємозв'язку між цими двома феноменами сучасних міжнародних відносин.

1.3. Теоретичні підходи до аналізу цифрової дипломатії як інструменту інформаційної безпеки

Осмислення цифрової дипломатії як інструменту забезпечення інформаційної безпеки вимагає звернення до різноманітних теоретичних парадигм міжнародних відносин, які пропонують відмінні концептуальні рамки для аналізу ролі інформації, комунікації та технологій у формуванні безпекового середовища сучасності, при цьому жодна з існуючих теорій не здатна повністю пояснити складність взаємозв'язків між цифровою дипломатією та інформаційною безпекою, що зумовлює необхідність комплементарного використання кількох методологічних підходів для отримання цілісного розуміння цього феномену. Теоретичний аналіз цифрової дипломатії через призму інформаційної безпеки дозволяє не лише зрозуміти механізми впливу цифрових дипломатичних практик на стан захищеності інформаційного простору держави, а й виявити потенціал різних стратегій цифрової дипломатії

для нейтралізації інформаційних загроз, зміцнення інформаційної стійкості суспільства та формування сприятливого міжнародного інформаційного середовища, що сприяє реалізації національних інтересів у глобальному цифровому просторі.

Неореалістична парадигма міжнародних відносин пропонує специфічний погляд на цифрову дипломатію та інформаційну безпеку, розглядаючи їх крізь призму боротьби за владу та відносне могутність в анархічній міжнародній системі, де держави прагнуть максимізувати свою безпеку через накопичення різноманітних ресурсів впливу, серед яких інформаційні та технологічні можливості набувають дедалі більшого значення [50, с. 89]. З неореалістичної перспективи інформаційний простір являє собою нову арену міждержавного суперництва, де відбувається боротьба за контроль над інформаційними потоками, формування порядку денного міжнародної спільноти та здатність впливати на громадську думку як у власній країні, так і в інших державах, при цьому цифрова дипломатія розглядається як інструмент силової політики, спрямований на зміцнення позицій держави у глобальній ієрархії могутності та забезпечення переваг у інформаційному протиборстві з геополітичними конкурентами. Неореалісти підкреслюють, що в умовах анархії міжнародної системи держави не можуть покладатися на міжнародні інституції чи норми для забезпечення своєї інформаційної безпеки, а мусять розвивати власні кіберспроможності та цифрові дипломатичні інструменти для самодопомоги та стримування потенційних агресорів у кіберпросторі [57, с. 134]. Саме тому провідні держави світу інвестують значні ресурси у розбудову наступальних кіберспроможностей та розвиток цифрової дипломатії не лише як засобу комунікації, а й як інструменту демонстрації сили та сигналізування своїх можливостей у інформаційній сфері потенційним противникам.

Неореалістичний аналіз цифрової дипломатії Німеччини через призму інформаційної безпеки виявляє напругу між традиційною німецькою схильністю до багатосторонності та кооперації, з одного боку, та необхідністю розвитку автономних національних спроможностей забезпечення кібербезпеки в умовах загострення геополітичної конкуренції, з іншого боку, що особливо яскраво

проявилося після серії російських кібератак на німецькі урядові структури та втручання у виборчі процеси [40, с. 178]. Німеччина поступово усвідомлює обмеженість виключно кооперативних підходів до забезпечення інформаційної безпеки та необхідність розвитку власних можливостей стримування та відплати за кібератаки, що знаходить відображення у створенні кіберкомандування Бундесверу та розширенні повноважень спецслужб у кіберпросторі, водночас німецький уряд прагне поєднувати зміцнення національних кіберспроможностей з підтримкою європейської інтеграції у сфері інформаційної безпеки, розглядаючи Європейський Союз як засіб колективного посилення позицій європейських держав у глобальній інформаційній конкуренції з такими потужними гравцями як США, Китай та росія.

Неолібералістський підхід до аналізу цифрової дипломатії та інформаційної безпеки акцентує увагу на можливостях міжнародної кооперації, ролі міжнародних інституцій та значенні взаємозалежності для формування режимів співробітництва навіть у такій чутливій сфері як інформаційна безпека, де держави мають сильні стимули до конкурентної поведінки [67, с. 201]. Представники неолібералізму вказують на те, що транснаціональний характер інформаційних загроз створює спільні інтереси держав у співпраці для протидії кіберзлочинності, тероризму в кіберпросторі та іншим формам зловживань цифровими технологіями, при цьому міжнародні інституції можуть відігравати важливу роль у зниженні трансакційних витрат такої співпраці, забезпеченні обміну інформацією про загрози та формуванні спільних стандартів кібербезпеки. Цифрова дипломатія з неолібералістичної перспективи розглядається насамперед як інструмент формування міжнародних режимів у сфері інформаційної безпеки, просування універсальних норм відповідальної поведінки держав у кіберпросторі та розбудови транснаціональних мереж співробітництва між урядовими та неурядовими акторами для спільного вирішення проблем цифрової епохи. Неоліберали підкреслюють значення довіри та репутації у міжнародних відносинах, вказуючи на те, що держави, які послідовно демонструють відповідальну поведінку в кіберпросторі та активно використовують цифрову дипломатію для транспарентної комунікації своїх

намірів, здатні формувати коаліції однодумців та ізолювати держави-порушники міжнародних норм [59, с. 223].

Німеччина як послідовний прихильник мультилатералізму активно використовує цифрову дипломатію для просування ініціатив щодо зміцнення міжнародної співпраці у сфері інформаційної безпеки, підтримуючи роботу Групи урядових експертів ООН з питань інформаційної безпеки, активно беручи участь у діяльності ОБСЄ з формування заходів довіри у кіберпросторі та ініціюючи створення європейських механізмів спільного реагування на кіберінциденти [45]. Німецька цифрова дипломатія послідовно просуває ідею застосування міжнародного гуманітарного права до кібероперацій під час збройних конфліктів, виступає за розробку додаткових міжнародних норм поведінки держав у кіберпросторі та підтримує ініціативи щодо заборони використання шкідливих інформаційно-комунікаційних технологій проти критичної інфраструктури інших держав у мирний час, демонструючи тим самим прагнення до формування передбачуваного та правозаснованого міжнародного порядку в цифровій сфері. Водночас неоліберальний підхід має певні обмеження у поясненні цифрової дипломатії як інструменту інформаційної безпеки, оскільки надмірно оптимістично оцінює готовність держав до співпраці та недооцінює структурні перешкоди для формування ефективних міжнародних режимів у ситуації глибоких розбіжностей між провідними державами світу щодо базових принципів регулювання кіберпростору та конкуруючих моделей цифрового суверенітету.

Конструктивістська парадигма пропонує принципово відмінний погляд на взаємозв’язок цифрової дипломатії та інформаційної безпеки, зосереджуючи увагу на ролі ідей, ідентичностей та соціальних практик у формуванні інтересів держав та конструюванні безпекового середовища, при цьому конструктивісти наголошують, що загрози національній безпеці не є об’єктивно даними, а соціально конструюються через дискурсивні практики та інтерсуб’єктивні значення, які приписуються певним явищам [69, с. 267]. З конструктивістської перспективи цифрова дипломатія являє собою потужний інструмент формування колективних уявлень про характер інформаційних загроз, легітимні способи

забезпечення інформаційної безпеки та норми прийнятної поведінки держав у кіберпросторі, оскільки через цифрові комунікаційні канали держави транслюють певні наративи, які впливають на те, як міжнародна спільнота сприймає ті чи інші дії в інформаційній сфері та які відповіді на інформаційні виклики вважаються легітимними. Конструктивісти звертають увагу на те, що сама концепція інформаційної безпеки по-різному розуміється в різних культурних та політичних контекстах, при цьому ці відмінності у розумінні не є просто технічними розбіжностями у термінології, а відображають глибші розбіжності у цінностях, ідентичності та уявленнях про роль держави в інформаційному просторі [73, с. 156].

Аналіз німецької цифрової дипломатії через конструктивістську призму виявляє, що Німеччина активно використовує цифрові комунікаційні канали для просування своєї нормативної програми у сфері інформаційної безпеки, яка базується на ліберально-демократичних цінностях, верховенстві права та захисті прав людини в цифровому середовищі, прагнучи при цьому сформувати міжнародний консенсус навколо європейського бачення регулювання кіберпростору як альтернативи китайській моделі цифрового суверенітету та американському ринковому підходу [47]. Німецькі дипломати систематично використовують міжнародні форуми, соціальні мережі та цифрові платформи для артикуляції німецької позиції щодо неприйнятності державного шпигунства в кіберпросторі, необхідності захисту критичної інфраструктури від кібератак та важливості збереження відкритого характеру інтернету при одночасному забезпеченні захисту від його зловживань, намагаючись через такі дискурсивні практики вплинути на формування глобальних норм поведінки в цифровому середовищі. Конструктивістський підхід дозволяє також зрозуміти, чому питання інформаційної безпеки набуло такого високого пріоритету в німецькій зовнішній політиці після 2014 року, оскільки російська агресія проти України та виявлення фактів втручання Росії у німецькі виборчі процеси призвели до переосмислення німецькою політичною елітою природи російської загрози та конструювання інформаційної безпеки як критично важливого виміру національної безпеки Німеччини [50, с. 298].

Комунікативна теорія міжнародних відносин, розроблена німецьким дослідником Томасом Ріссе та його колегами, пропонує додатковий теоретичний інструментарій для аналізу цифрової дипломатії як механізму формування інформаційної безпеки через раціональну комунікацію та переконання на міжнародній арені [65, с. 334]. Комунікативний підхід виходить з того, що держави та інші міжнародні актори можуть не лише торгуватися, погрожувати чи маніпулювати один одним, а й вступати в раціональний дискурс, спрямований на досягнення взаєморозуміння та формування консенсусу навколо спільних норм та правил поведінки, при цьому ефективність такої аргументативної взаємодії залежить від дотримання певних комунікативних умов, включно з щирістю учасників, відкритістю для аргументів іншої сторони та орієнтацією на досягнення справедливого рішення, а не просто просування власних інтересів будь-якою ціною. Цифрова дипломатія створює нові можливості для аргументативної взаємодії між державами та недержавними акторами у сфері інформаційної безпеки, оскільки цифрові платформи забезпечують прямий доступ до глобальних аудиторій, можливість оперативного реагування на аргументи опонентів та формування транснаціональних дискусійних спільнот навколо питань регулювання кіберпростору та протидії інформаційним загрозам [63].

Водночас застосування комунікативної теорії до аналізу цифрової дипломатії виявляє і серйозні проблеми, пов’язані з тим, що в реальній практиці цифрової комунікації далеко не завжди дотримуються ідеальні умови раціонального дискурсу, оскільки держави часто використовують цифрові канали не для щирого діалогу та пошуку консенсусу, а для стратегічної маніпуляції, дезінформації та символічної легітимації заздалегідь прийнятих рішень [40, с. 201]. Німецька цифрова дипломатія у сфері інформаційної безпеки балансує між щирим прагненням до формування міжнародного консенсусу через раціональну аргументацію та необхідністю використовувати цифрові комунікації як інструмент просування німецьких національних інтересів та протидії дезінформаційним кампаніям ворожих держав, що іноді вимагає відступу від ідеальних стандартів комунікативної раціональності заради

ефективності та оперативності реагування на інформаційні загрози. Особливо складним виявляється застосування комунікативного підходу у відносинах з авторитарними режимами, які систематично порушують базові принципи раціонального дискурсу через використання дезінформації, відмову визнавати очевидні факти та інструментальне ставлення до міжнародних переговорних процесів як до платформи для пропаганди власної позиції без справжньої відкритості до аргументів інших учасників.

Модель інформаційної стійкості являє собою відносно новий концептуальний підхід до осмислення інформаційної безпеки, який акцентує увагу не стільки на запобіганні інформаційним загрозам через технічні засоби захисту, скільки на формуванні здатності суспільства витримувати інформаційні удари, швидко відновлюватися після інформаційних криз та адаптуватися до постійно мінливого ландшафту інформаційних загроз [58, с. 112]. Концепція стійкості запозичена з екології та психології, де вона означає здатність системи зберігати свої ключові функції під впливом зовнішніх шоків та адаптуватися до нових умов без втрати ідентичності, при цьому застосування цієї концепції до інформаційної сфери передбачає розгляд інформаційної безпеки не як статичного стану захищеності, а як динамічного процесу формування адаптивних можливостей суспільства протистояти різноманітним інформаційним викликам. Інформаційна стійкість охоплює кілька вимірів, включно з технічною стійкістю інформаційних систем до кібератак, когнітивною стійкістю громадян до маніпулятивних впливів та дезінформації, соціальною стійкістю суспільства до спроб розпалювання конфліктів через інформаційні кампанії та інституційною стійкістю демократичних інститутів до іноземного інформаційного втручання [57, с. 156].

Цифрова дипломатія може відігравати важливу роль у формуванні інформаційної стійкості через кілька механізмів, серед яких особливе значення мають підвищення медіаграмотності та критичного мислення населення через освітні кампанії в цифровому просторі, формування довіри до офіційних джерел інформації через транспарентну та послідовну комунікацію державних органів, оперативне спростування дезінформації та маніпулятивних наративів через

цифрові канали, а також координація зусиль різних суспільних акторів у протидії інформаційним загрозам через цифрові платформи співробітництва [38]. Німеччина розробила комплексний підхід до формування інформаційної стійкості суспільства, який передбачає не лише технічне зміцнення кіберзахисту критичної інфраструктури, а й інвестиції у розвиток медіаграмотності населення, підтримку незалежної журналістики та фактчекінгу, зміцнення довіри між державою та громадянами через прозору цифрову комунікацію урядових органів, при цьому німецька цифрова дипломатія активно просуває концепцію інформаційної стійкості на міжнародному рівні як альтернативу авторитарним підходам до забезпечення інформаційної безпеки через жорсткий державний контроль над інформаційним простором [59, с. 178].

Модель стратегічних комунікацій доповнює концепцію інформаційної стійкості та пропонує операційну рамку для розуміння того, як держави можуть використовувати цифрову дипломатію для активного формування інформаційного середовища у спосіб, що сприяє реалізації їхніх національних інтересів та нейтралізації інформаційних загроз [71, с. 234]. Стратегічні комунікації розглядаються не просто як поширення інформації чи пропаганда, а як цілеспрямована координація слів та дій для досягнення певних стратегічних цілей через вплив на ставлення, сприйняття та поведінку цільових аудиторій, при цьому ефективні стратегічні комунікації вимагають глибокого розуміння аудиторії, послідовності між риторикою та реальними діями, а також здатності адаптувати повідомлення до специфіки різних комунікаційних каналів та культурних контекстів. У контексті інформаційної безпеки стратегічні комунікації виконують кілька важливих функцій, включно з формуванням порядку денного та рамок інтерпретації подій, що ускладнює просування ворожих наративів, демонстрацією рішучості та спроможностей держави для стримування потенційних агресорів у інформаційному просторі, мобілізацією внутрішньої підтримки політики інформаційної безпеки та залученням міжнародних партнерів до спільних зусиль з протидії інформаційним загрозам [67, с. 267].

Німецька цифрова дипломатія інтегрує елементи стратегічних комунікацій

через координацію повідомлень різних урядових відомств у цифровому просторі, розробку наративів, що просувають німецьке бачення інформаційної безпеки та протидіють ворожим інформаційним кампаніям, а також через таргетоване використання різних цифрових платформ для досягнення специфічних комунікаційних цілей з різними аудиторіями [45, с. 298]. Федеральне міністерство закордонних справ Німеччини створило спеціалізовані підрозділи стратегічних комунікацій, які відповідають за координацію німецької цифрової дипломатії у сфері інформаційної безпеки, моніторинг інформаційного простору для виявлення дезінформаційних кампаній та оперативне реагування на інформаційні виклики через цифрові канали, демонструючи тим самим усвідомлення німецьким урядом важливості проактивного формування інформаційного середовища для захисту національних інтересів. Водночас німецький підхід до стратегічних комунікацій відрізняється від практик деяких інших держав через його чітку прив'язку до демократичних цінностей та відмову від використання дезінформації чи маніпуляцій навіть у боротьбі з ворожими інформаційними кампаніями, що іноді обмежує ефективність німецьких стратегічних комунікацій у протистоянні з авторитарними режимами, які не обтяжують себе етичними обмеженнями у інформаційному протиборстві.

Інтеграція різних теоретичних підходів дозволяє сформувати багатовимірне розуміння цифрової дипломатії як інструменту інформаційної безпеки, яке враховує як структурні фактори міжнародної системи, що створюють стимули для конкуренції та співробітництва держав у інформаційній сфері, так і агентні можливості держав формувати норми, ідентичності та комунікаційні практики через цифрову дипломатію для конструювання сприятливого безпекового середовища [69]. Неореалістична перспектива нагадує про те, що цифрова дипломатія функціонує в умовах постійної конкуренції між державами за вплив у інформаційному просторі та необхідності розвитку власних спроможностей для забезпечення інформаційної безпеки, неоліберальстський підхід вказує на можливості міжнародної кооперації та роль інституцій у формуванні режимів співробітництва у сфері інформаційної безпеки, конструктивізм звертає увагу на значення ідей та норм у визначенні

того, що вважається загрозою інформаційній безпеці та які відповіді є легітимними, комунікативна теорія підкреслює потенціал раціонального дискурсу для досягнення взаєморозуміння, а концепції інформаційної стійкості та стратегічних комунікацій пропонують операційні рамки для розуміння практичних механізмів використання цифрової дипломатії для зміцнення інформаційної безпеки. Комплементарне використання цих теоретичних підходів дозволяє уникнути однобічності в аналізі та врахувати різні аспекти складного взаємозв'язку між цифровою дипломатією та інформаційною безпекою [47, с. 189].

Емпіричний аналіз німецької цифрової дипломатії у сфері інформаційної безпеки підтверджує корисність мультитеоретичного підходу, оскільки німецька практика демонструє елементи всіх розглянутих теоретичних парадигм, поєднуючи розвиток національних кіберспроможностей для стримування потенційних агресорів з активною участю у багатосторонніх ініціативах щодо формування міжнародних норм кіберповедінки, просуванням нормативної програми, заснованої на ліберально-демократичних цінностях, з прагматичним використанням стратегічних комунікацій для захисту німецьких інтересів у конкурентному інформаційному середовищі [73, с. 223]. Німеччина намагається знайти баланс між різними логіками поведінки у інформаційній сфері, що відображає складність завдання забезпечення інформаційної безпеки в умовах глобалізованого та взаємозалежного світу, де держави одночасно конкурують і співпрацюють, формують норми і порушують їх, використовують силу переконання та загрозу примусу для досягнення своїх цілей в інформаційному просторі. Теоретичне осмислення цього балансування між різними стратегіями та підходами до використання цифрової дипломатії для забезпечення інформаційної безпеки становить важливе завдання для подальших досліджень у цій галузі, оскільки успішні практики потребують не лише емпіричного опису, а й теоретичного обґрунтування умов їхньої ефективності та можливостей адаптації в інших контекстах.

Перспективи розвитку теоретичних підходів до аналізу цифрової дипломатії як інструменту інформаційної безпеки пов'язані з необхідністю

більш глибокого осмислення впливу технологічних змін на трансформацію дипломатичних практик та безпекового середовища, зокрема наслідків впровадження штучного інтелекту, автономних систем та квантових технологій для майбутнього інформаційної безпеки [65]. Існуючі теоретичні рамки були розроблені переважно до масового впровадження цих нових технологій, тому потребують адаптації та розширення для врахування якісно нових можливостей та загроз, які створюються технологічним прогресом у цифровій сфері, при цьому особливої уваги заслуговує питання про те, як цифрова дипломатія може сприяти формуванню міжнародних норм відповідального використання нових технологій та запобігання їхньому застосуванню у шкідливих цілях проти інформаційної безпеки держав та прав людини. Також важливим напрямом теоретичного розвитку є поглиблене дослідження взаємозв'язків між цифровою дипломатією, інформаційною безпекою та більш широкими процесами демократизації і авторитаризації в сучасному світі, оскільки накопичуються свідчення того, що цифрові технології можуть використовуватися як для зміцнення демократичних інститутів та захисту прав людини, так і для їхнього підриву через масове стеження, цензуру та маніпуляцію громадською думкою [63, с. 267].

Таким чином, теоретичне осмислення цифрової дипломатії як інструменту забезпечення інформаційної безпеки вимагає звернення до різноманітних концептуальних рамок, які пропонують відмінні, але комплементарні перспективи для аналізу цього складного феномену сучасних міжнародних відносин. Неореалістична парадигма підкреслює конкурентний характер інформаційного простору та необхідність розвитку національних спроможностей для забезпечення інформаційної безпеки в умовах анархії міжнародної системи, неолібералізм акцентує можливості міжнародної кооперації та ролі інституцій у формуванні режимів співробітництва, конструктивізм звертає увагу на значення ідей та норм у конструюванні безпекового середовища, комунікативна теорія вказує на потенціал раціонального дискурсу для досягнення консенсусу, а концепції інформаційної стійкості та стратегічних комунікацій пропонують операційні рамки для

практичного використання цифрової дипломатії в цілях інформаційної безпеки. Німецький досвід цифрової дипломатії у сфері інформаційної безпеки демонструє практичну реалізацію елементів усіх цих теоретичних підходів, що підтверджує необхідність мультитеоретичної перспективи для повноцінного розуміння ролі цифрової дипломатії у формуванні інформаційної безпеки сучасних держав. Розглянуті теоретичні підходи створюють необхідну концептуальну основу для подальшого емпіричного аналізу конкретних практик німецької цифрової дипломатії та оцінки їхньої ефективності у забезпеченні інформаційної безпеки Німеччини та європейського регіону в цілому.

Висновки до розділу 1

Теоретичний аналіз цифрової дипломатії та інформаційної безпеки, здійснений у першому розділі дослідження, дозволяє сформулювати низку концептуальних висновків, які створюють необхідну методологічну основу для подальшого емпіричного вивчення німецького досвіду використання цифрової дипломатії як інструменту формування інформаційної безпеки та визначають ключові теоретичні рамки для аналізу взаємозв'язків між цифровою трансформацією дипломатичної практики і забезпеченням захищеності національного інформаційного простору в умовах сучасних викликів глобального безпекового середовища. Осмислення еволюції цифрової дипломатії від простих веб-сайтів до складних цифрових екосистем, концептуалізація інформаційної безпеки як багатовимірного феномену, що охоплює технічні, юридичні, організаційні та змістовні аспекти захисту інформаційного простору, а також критичний розгляд різноманітних теоретичних підходів до аналізу цифрової дипломатії як інструменту інформаційної безпеки засвідчують складність досліджуваного об'єкта та необхідність комплексного міждисциплінарного підходу до його вивчення.

Цифрова дипломатія як феномен сучасних міжнародних відносин являє собою результат конвергенції технологічного прогресу та еволюції дипломатичних практик, внаслідок чого виникла якісно нова парадигма

міждержавної комунікації, яка органічно поєднує традиційні інструменти зовнішньої політики з можливостями інформаційно-комунікаційних технологій для досягнення зовнішньополітичних цілей держави. Еволюційний розвиток цифрової дипломатії демонструє поступове ускладнення форм та методів цифрової взаємодії у міжнародних відносинах, починаючи від односторонньої трансляції інформації через офіційні веб-сайти до багатовимірного діалогу з глобальними аудиторіями через соціальні мережі та використання передових технологій штучного інтелекту для таргетованого впливу на цільові аудиторії.

Функціональне призначення цифрової дипломатії виходить за межі технологічної модернізації традиційних дипломатичних практик і передбачає якісну трансформацію способів реалізації зовнішньої політики, включно з оперативним інформуванням міжнародної спільноти про офіційну позицію держави, налагодженням діалогу з іноземними громадянами та недержавними акторами, формуванням позитивного міжнародного іміджу та забезпеченням раннього попередження про загрози і кризове реагування в умовах інформаційних конфліктів сучасності.

Інформаційна безпека як відносно новий концепт у теорії та практиці міжнародних відносин поступово кристалізувалася у відповідь на зростаючу залежність держав від інформаційно-комунікаційних технологій та усвідомлення вразливості критичної інфраструктури перед різноманітними формами інформаційної агресії, що здатні завдати державі збитків, порівнянних з наслідками традиційних воєнних операцій. Багатовимірна структура інформаційної безпеки охоплює технічний вимір захисту інформаційних систем від кібератак, юридичний вимір створення нормативно-правової бази регулювання інформаційної сфери, організаційний вимір формування інституційних механізмів забезпечення інформаційної безпеки, а також змістовий вимір захисту громадян від маніпулятивних впливів та дезінформації. Інформаційна безпека тісно інтегрована в загальну систему національної безпеки держави, оскільки стабільне функціонування критичних секторів економіки та державного управління залежить від безперебійної роботи інформаційно-комунікаційних систем, при цьому транснаціональна природа інформаційних

загроз зумовлює об’єктивну необхідність міжнародної співпраці, адже жодна держава не спроможна самостійно забезпечити повноцінний захист свого інформаційного простору без координації зусиль з іншими країнами.

Теоретичне осмислення цифрової дипломатії як інструменту забезпечення інформаційної безпеки вимагає мультипарадигмального підходу, оскільки кожна з розглянутих теоретичних перспектив виявляє специфічні аспекти взаємозв’язку між цифровою дипломатією та інформаційною безпекою, що в сукупності створює цілісну картину досліджуваного феномену. Неореалістична парадигма акцентує конкурентний характер інформаційного простору та розглядає цифрову дипломатію як інструмент боротьби за вплив у глобальному інформаційному середовищі, підкреслюючи необхідність розвитку автономних національних спроможностей для забезпечення інформаційної безпеки. Неолібералістський підхід виявляє потенціал міжнародної кооперації у сфері інформаційної безпеки, вказуючи на роль міжнародних інституцій у формуванні режимів співробітництва та спільних стандартів кібербезпеки, при цьому цифрова дипломатія розглядається як інструмент просування універсальних норм відповідальної поведінки держав у кіберпросторі. Конструктивістська перспектива привертає увагу до ролі ідей та дискурсивних практик у формуванні уявлень про інформаційні загрози та легітимні способи забезпечення інформаційної безпеки, підкреслюючи значення цифрової дипломатії як інструменту конструювання безпекового середовища через трансляцію певних наративів. Комунікативна теорія доповнює це розуміння через акцентування потенціалу раціональної аргументативної взаємодії для досягнення взаєморозуміння та формування консенсусу, хоча її застосування виявляє і серйозні обмеження, пов’язані з реальною практикою цифрової комунікації, де держави часто використовують маніпуляцію замість щирого діалогу.

Концепції інформаційної стійкості та стратегічних комунікацій пропонують операційні рамки для практичного використання цифрової дипломатії в цілях зміцнення інформаційної безпеки, при цьому модель інформаційної стійкості акцентує увагу на формуванні адаптивних можливостей суспільства протистояти різноманітним інформаційним викликам через технічне

зміцнення систем, розвиток медіаграмотності населення та формування довіри між державою та громадянами, тоді як підхід стратегічних комунікацій зосереджується на цілеспрямованій координації повідомлень для досягнення стратегічних цілей через вплив на сприйняття та поведінку цільових аудиторій. Інтеграція різних теоретичних підходів дозволяє сформувати багатовимірне розуміння цифрової дипломатії як інструменту інформаційної безпеки, яке враховує як структурні фактори міжнародної системи, що створюють стимули для конкуренції та співробітництва держав, так і агентні можливості держав формувати норми та комунікаційні практики для конструювання сприятливого безпекового середовища.

Німеччина як одна з провідних європейських держав демонструє системний підхід до інтеграції цифрової дипломатії у свою зовнішню політику та використання її як інструменту забезпечення інформаційної безпеки, при цьому німецький підхід характеризується прагненням поєднувати технологічні інновації з традиційними європейськими цінностями демократії, верховенства права та захисту прав людини. Німецька практика демонструє елементи всіх розглянутих теоретичних підходів, балансуючи між розвитком національних кіберспроможностей та участю у багатосторонніх ініціативах, між просуванням нормативної програми та прагматичним використанням стратегічних комунікацій, що свідчить про складність завдання забезпечення інформаційної безпеки в умовах глобалізованого світу. Розроблені теоретичні рамки створюють необхідну концептуальну основу для подальшого емпіричного аналізу конкретних практик німецької цифрової дипломатії у сфері інформаційної безпеки, який дозволить виявити специфіку німецького підходу, оцінити його ефективність та визначити можливості адаптації німецького досвіду в інших національних контекстах.

РОЗДІЛ 2. СТРАТЕГІЯ ТА ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ДИПЛОМАТІЇ НІМЕЧЧИНИ

2.1. Формування цифрової дипломатії Німеччини

Формування цифрової дипломатії Німеччини як самостійного напряму зовнішньої політики відбувалося поступово протягом останніх двох десятиліть у відповідь на технологічні зміни глобального комунікаційного середовища та усвідомлення німецькою політичною елітою стратегічного значення інформаційного простору для реалізації національних інтересів і забезпечення безпеки держави в умовах цифрової трансформації міжнародних відносин. Еволюція німецької зовнішньої інформаційної політики відображає загальні тенденції адаптації традиційної дипломатії до викликів інформаційної епохи, водночас демонструючи специфічні риси, зумовлені історичним досвідом Німеччини, її роллю у європейській інтеграції та прагненням поєднувати технологічні інновації з фундаментальними демократичними цінностями, що відрізняє німецький підхід від практик як авторитарних режимів, так і деяких інших західних демократій. Аналіз історичного розвитку німецької цифрової дипломатії дозволяє виявити ключові етапи її становлення, ідентифікувати чинники, що впливали на формування стратегічних пріоритетів у цій сфері, та зрозуміти логіку трансформації німецького підходу до використання цифрових технологій у зовнішній політиці загалом і в забезпеченні інформаційної безпеки зокрема.

Початковий етап формування цифрової дипломатії Німеччини охоплює період з середини 1990-х до кінця 2000-х років і характеризувався переважно технічною модернізацією комунікаційної інфраструктури Федерального міністерства закордонних справ без стратегічного переосмислення самої сутності дипломатичної діяльності в цифрову епоху [40, с. 45]. У цей період Міністерство закордонних справ Німеччини зосередилося на створенні офіційного веб-сайту відомства та веб-представництв німецьких посольств у різних країнах світу, які слугували насамперед інформаційними платформами для односторонньої трансляції офіційних повідомлень та надання консульських послуг німецьким громадянам за кордоном, при цьому інтерактивна взаємодія з

іноземними аудиторіями залишалася мінімальною, а стратегічне бачення ролі цифрових технологій у зовнішній політиці фактично було відсутнім. Німецька дипломатична служба в цей період демонструвала певний консерватизм у підході до цифрових інновацій, що частково пояснювалося традиційною культурою німецької бюрократії з її акцентом на формальних процедурах та ієрархічних структурах прийняття рішень, які не завжди сприяли швидкій адаптації до динамічного цифрового середовища та експериментуванню з новими формами комунікації.

Якісна трансформація німецького підходу до цифрової дипломатії розпочалася приблизно з 2010 року, коли Федеральне міністерство закордонних справ під керівництвом міністра Гідо Вестервеллеініціювало масштабну програму модернізації зовнішньої комунікації з активним використанням соціальних мереж та цифрових платформ для прямого діалогу з глобальними аудиторіями [66]. Цей період позначився створенням офіційних акаунтів Міністерства закордонних справ у Twitter, Facebook та інших соціальних мережах, призначенням спеціальних співробітників, відповідальних за цифрову комунікацію у дипломатичних представництвах, та розробкою перших стратегічних документів, що визначали принципи та цілі німецької присутності в цифровому просторі, при цьому особлива увага приділялася можливостям соціальних мереж для публічної дипломатії, просування німецької культури та цінностей, а також налагодження прямих контактів з молодими аудиторіями в різних регіонах світу. Водночас на цьому етапі цифрова дипломатія ще не розглядалася як інструмент забезпечення національної безпеки, а сприймалася переважно через призму культурної дипломатії та м’якої сили, що відображало загальне недооцінювання потенційних загроз, пов’язаних з цифровізацією міжнародних відносин.

Радикальна переоцінка ролі цифрової дипломатії у німецькій зовнішній політиці відбулася після 2013 року внаслідок розголосу про масове стеження американських спецслужб, включно із прослуховуванням мобільного телефону канцлера Ангели Меркель, що викликало широкий резонанс у німецькому суспільстві та змусило політичну еліту усвідомити вразливість національного

інформаційного простору перед зовнішніми загрозами [40, с. 112]. Ця подія стала каталізатором переосмислення німецького підходу до цифрових технологій у контексті національної безпеки та зовнішньої політики, внаслідок чого розпочався активний процес формування комплексної стратегії кібербезпеки та цифрової зовнішньої політики, яка б враховувала не лише можливості, а й ризики цифровізації для німецьких національних інтересів. Німеччина почала активно просувати на європейському рівні ініціативи щодо захисту персональних даних, обмеження масового стеження та забезпечення цифрового суверенітету Європейського Союзу, при цьому цифрова дипломатія поступово перетворювалася з інструменту публічної дипломатії на важливий компонент стратегії національної безпеки, що вимагало створення нових інституційних структур та механізмів координації між різними відомствами, відповідальними за кібербезпеку та зовнішню політику.

Наступний етап еволюції німецької цифрової дипломатії розпочався після 2014 року в контексті російської агресії проти України та виявлення масштабних російських кампаній з дезінформації та втручання у виборчі процеси західних демократій, що остаточно утвердило розуміння інформаційної безпеки як критично важливого виміру національної безпеки Німеччини [48, с. 78]. Німецький уряд почав систематично інвестувати у розбудову спроможностей протидії дезінформації, створення центрів стратегічних комунікацій та розвиток цифрової дипломатії як інструменту захисту демократичних інститутів від іноземного інформаційного втручання, при цьому особлива увага приділялася підготовці до федеральних виборів 2017 року, під час яких очікувалися спроби зовнішнього втручання через кібератаки та дезінформаційні кампанії у соціальних мережах. Федеральне міністерство закордонних справ під керівництвом Франка-Вальтера Штайнмаєра, а згодом Зігмара Габріеля та Гайко Мааса послідовно розширювало мандат цифрової дипломатії, включаючи до нього не лише комунікацію з зарубіжними аудиторіями, а й активну протидію дезінформації, просування міжнародних норм відповідальної поведінки держав у кіберпросторі та формування коаліцій однодумців для спільного захисту демократичних цінностей в інформаційному просторі.

Концептуалізація німецької цифрової дипломатії відбувалася через формування двох взаємопов'язаних, але частково автономних концепцій, а саме Digitale Außenpolitik та Cyber-Außenpolitik, які відображають різні аспекти використання цифрових технологій у зовнішній політиці та специфічні виклики, що постають перед німецькою дипломатією в цифрову епоху [70]. Концепція Digitale Außenpolitik охоплює широкий спектр питань, пов'язаних з цифровою трансформацією дипломатичної практики, включно з використанням соціальних мереж для комунікації з глобальними аудиторіями, застосуванням цифрових технологій для модернізації внутрішніх процесів дипломатичної служби, просуванням німецьких інтересів у міжнародних дискусіях про регулювання цифрового простору, а також формуванням стратегічних партнерств з технологічними компаніями та дослідницькими центрами для забезпечення технологічного лідерства Німеччини у ключових сферах цифрової економіки. Натомість концепція Cyber-Außenpolitik зосереджується більш вузько на питаннях кібербезпеки у міжнародних відносинах, включно з протидією кібератакам на німецькі державні та приватні інформаційні системи, розробкою міжнародних норм відповідальної поведінки держав у кіберпросторі, формуванням режимів контролю за кіберзброєю та застосуванням міжнародного права до кібероперацій у контексті збройних конфліктів.

Стратегічні пріоритети німецької цифрової дипломатії сформувалися як результат усвідомлення множинних викликів та можливостей, що виникають у зв'язку з цифровізацією міжнародних відносин, і відображають прагнення Німеччини зайняти лідируючі позиції у формуванні глобального цифрового порядку, заснованого на демократичних цінностях, верховенстві права та захисті прав людини [59, с. 134]. Першим стратегічним пріоритетом є просування концепції відкритого, безпечного та мирного кіберпростору, що передбачає активну участь німецької дипломатії у міжнародних дискусіях про застосування міжнародного права до кіберпростору, підтримку ініціатив щодо розробки норм відповідальної поведінки держав у цифровому середовищі та протидію спробам авторитарних режимів легітимізувати жорсткий державний контроль над інтернетом під прикриттям концепції цифрового суверенітету. Другим

пріоритетом є зміцнення кіберстійкості Європейського Союзу та його держав-членів через розвиток спільних механізмів реагування на кіберінциденти, обмін інформацією про загрози, координацію дипломатичних відповідей на масштабні кібератаки та формування європейського технологічного суверенітету у критичних сферах цифрової інфраструктури, що дозволило б зменшити залежність від технологічних гігантів з інших регіонів світу.

Третім стратегічним пріоритетом німецької цифрової дипломатії є активна протидія дезінформації та захист демократичних процесів від іноземного інформаційного втручання, що передбачає не лише технічні заходи із забезпечення безпеки виборчої інфраструктури, а й системну роботу з підвищення медіаграмотності населення, підтримку незалежної журналістики та фактчекінгу, розвиток стратегічних комунікацій для оперативного спростування дезінформаційних наративів, а також міжнародну співпрацю у виявленні та атрибуції скоординованих дезінформаційних кампаній [42, с. 167]. Четвертим пріоритетом є забезпечення захисту прав людини в цифровому просторі, включно з правом на приватність, свободою вираження поглядів в інтернеті, захистом персональних даних від несанкціонованого збору та використання, а також протидією використанню цифрових технологій для масового стеження, цензури та придушення дисидентства авторитарними режимами, при цьому Німеччина активно використовує цифрову дипломатію для просування європейських стандартів захисту даних як глобального еталону та критикує практики держав, які систематично порушують цифрові права своїх громадян.

П’ятим стратегічним пріоритетом є розвиток цифрової публічної дипломатії для просування позитивного іміджу Німеччини у світі, залучення талановитої молоді до співпраці з німецькими інституціями та формування глобальних мереж підтримки німецьких ініціатив у різних сферах міжнародної політики через активне використання соціальних мереж, цифрових платформ обміну та віртуальних форматів культурної дипломатії [73, с. 201]. Реалізація цих стратегічних пріоритетів вимагає не лише розвитку технічних спроможностей німецької дипломатичної служби, а й формування нової культури цифрової комунікації у середовищі німецьких дипломатів, що передбачає готовність до

експериментування з новими форматами взаємодії, здатність швидко реагувати на динамічні зміни в інформаційному просторі та розуміння специфіки різних цифрових платформ і онлайн-спільнот, з якими взаємодіє німецька дипломатія. Федеральне міністерство закордонних справ інвестувало значні ресурси у навчання дипломатичних кадрів цифровим компетенціям, створення спеціалізованих підрозділів цифрової дипломатії та розробку внутрішніх керівництв і протоколів для роботи в соціальних мережах, що засвідчує усвідомлення німецьким керівництвом стратегічної важливості цифрового виміру зовнішньої політики для забезпечення національних інтересів у довгостроковій перспективі.

Аналіз еволюції стратегічних документів німецького уряду, присвячених цифровій політиці та кібербезпеці, дозволяє простежити трансформацію німецького підходу від переважно технократичного розуміння цифровізації як процесу впровадження нових технологій до комплексного стратегічного бачення цифрової трансформації як фундаментального виклику для національної безпеки, економічної конкурентоспроможності та соціальної стабільності, що вимагає скоординованих зусиль різних державних відомств, приватного сектору та громадянського суспільства [56]. Перша Стратегія кібербезпеки Німеччини, прийнята у 2011 році, мала переважно оборонний характер і зосереджувалася на технічному захисті критичної інфраструктури від кібератак, тоді як друга редакція цієї стратегії, представлена у 2016 році, вже включала ширше розуміння кіберзагроз, охоплюючи питання дезінформації, гібридних загроз та необхідності міжнародної співпраці у забезпеченні кібербезпеки. Третя Стратегія кібербезпеки, оприлюднена у 2021 році, ознаменувала перехід до проактивного підходу, що передбачає не лише захист від кіберзагроз, а й розвиток наступальних кіберспроможностей для стримування потенційних агресорів та формування стратегічної автономії Німеччини і Європейського Союзу у цифровій сфері, при цьому особлива увага приділяється ролі цифрової дипломатії у просуванні німецьких інтересів та цінностей у глобальних дискусіях про майбутнє кіберпростору.

Формування стратегічних пріоритетів німецької цифрової дипломатії

відбувалося під впливом кількох ключових факторів, серед яких особливе значення мали загострення російської інформаційної агресії проти західних демократій, зростання геополітичної конкуренції між США і Китаєм за технологічне лідерство та контроль над глобальними цифровими стандартами, а також внутрішньоєвропейські дебати про баланс між інноваціями та регулюванням у цифровій сфері [50, с. 223]. Російські інформаційні операції, включно з кібератаками на Бундестаг у 2015 році, спробами вплинути на федеральні вибори 2017 року та систематичними дезінформаційними кампаніями, спрямованими на підрив довіри до німецьких політичних інститутів, переконливо продемонстрували німецькому керівництву реальність інформаційних загроз та необхідність розвитку адекватних інструментів протидії, що стало потужним стимулом для активізації роботи над формуванням комплексної стратегії інформаційної безпеки з важливою роллю цифрової дипломатії у її реалізації. Водночас Німеччина прагне уникати надмірної мілітаризації кіберпростору та зберігає прихильність багатосторонньому підходу до вирішення проблем цифрової епохи, що відображає глибоко вкорінену у німецькій політичній культурі традицію пошуку компромісних рішень через діалог та інституційне співробітництво.

Особливістю німецького підходу до формування цифрової дипломатії є його тісний зв’язок із загальноєвропейськими ініціативами у сфері цифрової політики та кібербезпеки, оскільки Німеччина розглядає Європейський Союз як критично важливу платформу для консолідації зусиль європейських держав у протистоянні глобальним викликам цифрової епохи та формування європейської альтернативи американській і китайській моделям цифрового розвитку [37, с. 256]. Німецька цифрова дипломатія активно підтримує європейські ініціативи у сфері регулювання цифрових платформ, захисту персональних даних, розвитку європейської цифрової інфраструктури та створення спільних механізмів реагування на кіберзагрози, при цьому Німеччина часто виступає посередником між різними групами держав-членів Європейського Союзу, що мають відмінні погляди на оптимальний баланс між державним регулюванням та ринковими механізмами у цифровій сфері, а також на відносини з США і Китаєм у

технологічній сфері. Прагнення поєднувати національні інтереси Німеччини з просуванням загальноєвропейських підходів до цифрової політики іноді створює напругу та вимагає складних політичних компромісів, однак німецьке керівництво послідовно наголошує на тому, що лише через європейську інтеграцію Німеччина та інші середні європейські держави можуть зберегти достатній вплив на формування глобальних правил гри в цифровому просторі та захистити свої інтереси від домінування наддержав.

Таким чином, формування цифрової дипломатії Німеччини відбувалося поетапно протягом останніх двох десятиліть у відповідь на технологічні зміни та зростаючі загрози інформаційній безпеці, при цьому німецький підхід еволюціонував від технічної модернізації комунікаційної інфраструктури до комплексного стратегічного бачення цифрової дипломатії як важливого інструменту забезпечення національної безпеки та просування німецьких інтересів у глобальному інформаційному просторі. Концептуалізація німецької цифрової дипломатії через поняття Digitale Außenpolitik та Cyber-Außenpolitik відображає багатовимірний характер цього феномену, що охоплює як широкі питання цифрової трансформації зовнішньої політики, так і специфічні виклики кібербезпеки у міжнародних відносинах, при цьому стратегічні пріоритети німецької цифрової дипломатії включають просування відкритого та безпечного кіберпростору, зміцнення кіберстійкості ЄС, протидію дезінформації, захист прав людини в цифровому середовищі та розвиток цифрової публічної дипломатії. Розуміння історичної еволюції та стратегічних пріоритетів німецької цифрової дипломатії створює необхідне підґрунтя для аналізу інституційних структур та механізмів, через які реалізується німецька політика у сфері цифрової дипломатії та інформаційної безпеки.

2.2. Інституційна структура забезпечення цифрової дипломатії та інформаційної безпеки Німеччини

Реалізація стратегічних пріоритетів німецької цифрової дипломатії та забезпечення інформаційної безпеки держави вимагає складної інституційної архітектури, яка охоплює численні державні відомства, спеціалізовані агенції та механізми міжвідомчої координації, при цьому ефективність німецького підходу значною мірою залежить від здатності різних інституцій узгоджувати свої дії, обмінюватися інформацією та формувати єдину стратегію реагування на інформаційні виклики, що постають перед Німеччиною у глобалізованому цифровому середовищі. Інституційна структура німецької системи забезпечення цифрової дипломатії та інформаційної безпеки характеризується певною фрагментацією повноважень між різними відомствами, що відображає федеральний устрій Німеччини та традиційний німецький підхід до розподілу влади, спрямований на запобігання надмірній концентрації повноважень у руках однієї інституції, водночас ця фрагментація іноді створює виклики для швидкого прийняття рішень та координації дій у динамічному інформаційному просторі, що вимагає розвитку ефективних механізмів міжвідомчої співпраці та чіткого визначення сфер відповідальності різних акторів у забезпеченні інформаційної безпеки держави.

Центральну роль у формуванні та реалізації німецької цифрової дипломатії відіграє Федеральне міністерство закордонних справ, яке є головним координатором німецької зовнішньої політики і несе первинну відповідальність за комунікацію з іноземними урядами, міжнародними організаціями та зарубіжними громадськостями через традиційні та цифрові канали дипломатичної взаємодії [40, с. 89]. У структурі Міністерства закордонних справ протягом останнього десятиліття були створені спеціалізовані підрозділи, відповідальні за різні аспекти цифрової дипломатії, включно з відділом цифрової та кіберзовнішньої політики, який розробляє стратегічні документи та координує німецьку позицію у міжнародних дискусіях про регулювання кіберпростору, відділом стратегічних комунікацій, що займається протидією дезінформації та формуванням наративів для просування німецьких інтересів, а також

численними офіцерами цифрової дипломатії у німецьких посольствах та консульствах по всьому світу, які відповідають за присутність Німеччини в соціальних мережах та взаємодію з локальними онлайн-спільнотами. Міністерство закордонних справ активно інвестує у підготовку дипломатичних кадрів для роботи в цифровому середовищі через спеціальні навчальні програми, що охоплюють як технічні аспекти використання цифрових платформ, так і стратегічні питання цифрової комунікації, управління репутаційними ризиками в онлайн-просторі та протидії дезінформаційним кампаніям, при цьому особлива увага приділяється формуванню розуміння культурних особливостей різних цифрових спільнот та специфіки комунікації в різних соціальних мережах, що є критично важливим для ефективної цифрової дипломатії.

Координація міжнародних аспектів німецької політики у сфері кібербезпеки також покладена на Федеральне міністерство закордонних справ, яке представляє німецьку позицію у багатосторонніх форматах обговорення питань інформаційної безпеки, включно з Групою урядових експертів ООН з питань інформаційної безпеки, дискусіями в рамках ОБСЄ про заходи довіри у кіберпросторі та переговорами про застосування міжнародного права до кібероперацій [67, с. 112]. Міністерство закордонних справ відіграє ключову роль у формуванні коаліцій держав-однодумців для просування німецького бачення відкритого, безпечного та заснованого на правилах кіберпростору, при цьому німецькі дипломати активно використовують двосторонні та багатосторонні канали для консультацій з партнерами про спільні підходи до реагування на кіберінциденти, атрибуції кібератак та застосування дипломатичних санкцій проти держав або недержавних акторів, відповідальних за шкідливі кіберактивності. Водночас Міністерство закордонних справ не володіє технічними спроможностями для моніторингу кіберзагроз, розслідування кіберінцидентів чи здійснення активних заходів кіберзахисту, що зумовлює необхідність тісної співпраці з іншими відомствами, які мають відповідні технічні можливості та експертизу у сфері кібербезпеки.

Федеральне відомство з інформаційної безпеки є головною технічною інституцією Німеччини у сфері кібербезпеки і відіграє центральну роль у

забезпеченні захисту урядових інформаційних систем, моніторингу кіберзагроз, координації національного реагування на кіберінциденти та наданні рекомендацій щодо безпечного використання інформаційних технологій державним і приватним секторам [38]. Відомство, створене ще у 1991 році як наступник структур, відповідальних за криптографічний захист урядових комунікацій, поступово розширило свій мандат відповідно до еволюції кіберзагроз та цифровізації критичної інфраструктури, перетворившись на комплексний центр компетенції з питань кібербезпеки, який надає технічну підтримку всім федеральним відомствам, координує обмін інформацією про кіберзагрози між державним і приватним секторами через Національний центр реагування на кіберінциденти та веде просвітницьку роботу серед населення щодо безпечної поведінки в цифровому просторі. Федеральне відомство з інформаційної безпеки не має повноважень правоохоронного або розвідувального характеру, його діяльність зосереджена виключно на превентивних технічних заходах захисту інформаційних систем та координації реагування на кіберінциденти, що відрізняє німецьку модель від практик деяких інших держав, де функції кібербезпеки часто концентруються у спецслужбах або військових відомствах, при цьому німецький підхід відображає прагнення забезпечити прозорість діяльності у сфері кібербезпеки та чітке розмежування між технічним захистом інформаційних систем, з одного боку, та розвідувальною чи правоохоронною діяльністю, з іншого боку.

Співпраця між Федеральним міністерством закордонних справ та Федеральним відомством з інформаційної безпеки здійснюється через регулярні консультації, обмін інформацією про міжнародні тенденції у сфері кіберзагроз та спільну участь у підготовці стратегічних документів з питань кібербезпеки, при цьому Відомство з інформаційної безпеки надає технічну експертизу для формування позицій німецької дипломатії у міжнародних переговорах про технічні стандарти кібербезпеки, тоді як Міністерство закордонних справ забезпечує просування німецьких ініціатив на міжнародній арені та формування сприятливого політичного контексту для реалізації технічних рекомендацій Відомства [59, с. 167]. Федеральне відомство з інформаційної безпеки також

активно співпрацює з аналогічними інституціями інших європейських держав та з Агенцією Європейського Союзу з кібербезпеки у рамках обміну інформацією про кіберзагрози, спільних навчань з реагування на кіберінциденти та гармонізації технічних стандартів кібербезпеки у межах Європейського Союзу, що сприяє зміцненню колективної кіберстійкості європейського регіону та формуванню спільних підходів до захисту критичної інфраструктури від транснаціональних кіберзагроз.

Федеральна служба захисту конституції, яка є внутрішньою контррозвідувальною службою Німеччини, відіграє важливу роль у виявленні та протидії іноземному кібершпигунству, інформаційним операціям іноземних спецслужб на німецькій території та спробам впливу на німецькі політичні процеси через дезінформаційні кампанії та маніпуляції в соціальних мережах [44, с. 201]. Служба захисту конституції має повноваження проводити розслідування діяльності іноземних агентів впливу в Німеччині, моніторити підозрілі кіберактивності, що можуть становити загрозу національній безпеці, та надавати попередження державним і приватним структурам про потенційні ризики, пов’язані з іноземним кібершпигунством або інформаційним втручанням, при цьому діяльність Служби регулюється суворими правовими обмеженнями, спрямованими на захист конституційних прав громадян та запобігання зловживанням повноваженнями спецслужб. Служба захисту конституції регулярно оприлюднює звіти про стан загроз національній безпеці Німеччини, у яких дедалі більше уваги приділяється кіберзагрозам та інформаційним операціям іноземних держав, зокрема Росії, Китаю та Ірану, що спрямовані на викрадення промислових секретів, збір розвідувальної інформації про німецькі урядові структури та дестабілізацію політичної ситуації через розпалювання соціальних конфліктів та підрив довіри до демократичних інститутів.

Координація між Федеральною службою захисту конституції та Федеральним міністерством закордонних справ відбувається насамперед у контексті атрибуції кібератак та підготовки дипломатичних відповідей на випадки встановленого іноземного втручання, коли Служба надає розвідувальну

інформацію, що дозволяє ідентифікувати державних акторів, відповідальних за шкідливі кіберактивності, а Міністерство використовує цю інформацію для формулювання офіційних протестів, координації спільних заяв з партнерами та застосування дипломатичних санкцій [73, с. 234]. Водночас існують певні напруги між потребою Міністерства закордонних справ у швидкому отриманні інформації для дипломатичного реагування та обережністю спецслужб у розголошенні розвідувальних даних, що можуть компрометувати джерела інформації або методи роботи, внаслідок чого процес прийняття рішень про публічну атрибуцію кібератак іноді затягується, що зменшує ефективність дипломатичної відповіді та дозволяє агресорам уникати швидких наслідків за свої дії.

Бундесвер, збройні сили Німеччини, також відіграє зростаючу роль у забезпеченні кібербезпеки держави через Кіберкомандування Бундесверу, створене у 2017 році як окремий вид збройних сил, відповідальний за захист військових інформаційних систем, проведення кібероперацій у підтримку військових місій та розвиток наступальних кіберспроможностей для стримування потенційних агресорів [51]. Створення Кіберкомандування ознаменувало важливий поворот у німецькому підході до кібербезпеки, оскільки вперше Німеччина офіційно визнала можливість використання наступальних кіберспроможностей у військових цілях, що викликало інтенсивні дебати у німецькому суспільстві про етичні та правові межі кібервійни та ризики ескалації конфліктів у кіберпросторі. Кіберкомандування Бундесверу тісно співпрацює з Федеральним відомством з інформаційної безпеки у технічних питаннях захисту інформаційних систем, з Федеральною службою захисту конституції у виявленні іноземного кібершпигунства проти військових об’єктів, а також з розвідувальними службами союзників по НАТО у рамках обміну інформацією про кіберзагрози та координації кібероборони Альянсу, при цьому діяльність Кіберкомандування регулюється як національним законодавством Німеччини, так і зобов’язаннями у рамках міжнародного гуманітарного права, що накладають суворі обмеження на застосування кіберзброї під час збройних конфліктів.

Роль Кіберкомандування Бундесверу у німецькій цифровій дипломатії є специфічною і зосереджена переважно на забезпеченні технічних спроможностей для стримування агресії в кіберпросторі та демонстрації рішучості Німеччини захищати свої інтереси всіма доступними засобами, включно з військовими кіберспроможностями, що має сигналізуючий ефект для потенційних противників [50, с. 267]. Водночас Федеральне міністерство закордонних справ дотримується обережної позиції щодо публічної комунікації про військові кіберспроможності Німеччини, прагнучи уникати надмірної мілітаризації дискусій про кіберпростір та зберігаючи акцент на дипломатичних і правових механізмах регулювання кіберактивностей держав, що відображає загальну філософію німецької зовнішньої політики з її традиційним скептицизмом щодо силових рішень та перевагою, що надається багатостороннім дипломатичним підходам. Координація між військовими та цивільними відомствами у сфері кібербезпеки здійснюється через Раду національної кібербезпеки, міжвідомчий орган, що об’єднує представників усіх ключових інституцій, відповідальних за різні аспекти цифрової політики та інформаційної безпеки, і забезпечує узгодження стратегічних підходів та координацію оперативних дій у відповідь на масштабні кіберінциденти чи інформаційні кризи.

Інститут Гете як головна інституція німецької культурної дипломатії відіграє специфічну, але важливу роль у німецькій цифровій дипломатії через просування німецької мови та культури у цифровому просторі, організацію онлайн-програм культурного обміну та формування мереж молодих лідерів думок у різних країнах світу, які можуть стати провідниками німецьких цінностей та інтересів у своїх локальних онлайн-спільнотах [49, с. 298]. Інститут Гете активно використовує соціальні мережі, цифрові платформи навчання та віртуальні культурні події для досягнення глобальних аудиторій, при цьому особлива увага приділяється молоді та цифровим активістам у країнах, що розвиваються, де німецька присутність у традиційних медіа може бути обмеженою, а цифрові канали дозволяють встановити прямий контакт з потенційними прихильниками німецької моделі суспільного розвитку. Цифрова

культурна дипломатія Інституту Гете доповнює більш політичні аспекти німецької цифрової дипломатії, створюючи позитивний фон для сприйняття Німеччини у світі та формуючи довгострокові зв'язки, що можуть бути мобілізовані для підтримки німецьких ініціатив у міжнародній політиці, при цьому Інститут Гете ретельно уникає відкритої політичної ангажованості та прагне зберігати імідж аполітичної культурної організації, що сприяє довірі до його діяльності та дозволяє працювати навіть у країнах з авторитарними режимами, де відкрита політична діяльність іноземних акторів є неможливою.

Європейський вимір інституційної структури німецької цифрової дипломатії та забезпечення інформаційної безпеки має критичне значення, оскільки Німеччина розглядає європейську інтеграцію як ключовий механізм посилення своїх позицій у глобальному цифровому просторі та формування єдиного європейського підходу до регулювання інформаційної сфери [40, с. 156]. Німеччина активно підтримує розвиток інституційних спроможностей Європейського Союзу у сфері кібербезпеки та цифрової дипломатії, включно з Європейською службою зовнішніх дій, яка координує цифрову публічну дипломатію ЄС та керує Групою стратегічних комунікацій Європейського Союзу, що займається моніторингом та протидією дезінформації, Агенцією ЄС з кібербезпеки, яка забезпечує технічну підтримку держав-членів у зміцненні їхньої кіберстійкості, а також новоствореним Європейським центром компетенції з кібербезпеки, розташованим у Бухаресті, який координує дослідження та розробки у сфері кібербезпекових технологій на рівні ЄС. Німецькі представники займають активні позиції у всіх цих європейських структурах та послідовно просувають німецьке бачення пріоритетів європейської політики у сфері цифрової дипломатії та інформаційної безпеки, при цьому Німеччина інвестує значні фінансові ресурси у підтримку європейських ініціатив та надає технічну експертизу для розробки загальноєвропейських стандартів та процедур у цій сфері.

Співпраця Німеччини з НАТО у сфері кібербезпеки здійснюється через участь у роботі Центру передового досвіду НАТО з кібероборони у Таллінні, регулярні консультації у рамках Кіберкомітету Альянсу та участь у спільних

навчаннях з реагування на масштабні кіберінциденти, що можуть загрожувати колективній безпеці держав-членів НАТО [48, с. 178]. Німеччина підтримала визнання кіберпростору п'ятою оперативною сферою НАТО поряд із сухопутною, морською, повітряною та космічною сферами, а також активно бере участь у дискусіях про умови застосування статті 5 Вашингтонського договору про колективну оборону у відповідь на кібератаки, при цьому німецька позиція підкреслює необхідність високого порогу для визнання кібератаки актом агресії, що тригерує колективну відповідь Альянсу, щоб уникнути ризиків ескалації конфліктів через помилкову атрибуцію чи непропорційне реагування на кіберінциденти. Водночас Німеччина усвідомлює важливість трансатлантичної солідарності у протистоянні кіберзагрозам з боку авторитарних держав та підтримує розвиток натівських механізмів обміну інформацією про кіберзагрози, спільної підготовки фахівців з кібербезпеки та координації кібероборони критичної інфраструктури Альянсу.

Багатостороння співпраця Німеччини у сфері цифрової дипломатії та інформаційної безпеки також охоплює участь у роботі Організації з безпеки і співробітництва в Європі, яка розробила унікальний набір заходів довіри у кіберпросторі, спрямованих на зниження ризиків конфліктів через непорозуміння або випадкову ескалацію кіберінцидентів між державами-учасницями [70, с. 223]. Німеччина активно підтримує розвиток механізмів ОБСЄ з обміну інформацією про кіберінциденти, створення каналів екстреного зв'язку між урядами для оперативного з'ясування обставин підозрілих кіберактивностей та формування спільного розуміння застосування міжнародного права до кіберпростору, при цьому німецькі дипломати наголошують на особливій цінності обсєвської платформи для діалогу з Росією про норми поведінки у кіберпросторі, незважаючи на всі складнощі у відносинах після російської агресії проти України. Німеччина також активно співпрацює з ООН у рамках роботи Групи урядових експертів з питань інформаційної безпеки та Відкритої робочої групи з того ж питання, просуваючи ідею універсального застосування міжнародного права, включно з Статутом ООН та міжнародним гуманітарним правом, до кіберактивностей держав та виступаючи за розробку

додаткових норм відповідальної поведінки держав у кіберпросторі, що доповнювали б існуючі правові зобов'язання та забезпечували більшу передбачуваність поведінки держав у цифровому середовищі.

Таким чином, інституційна структура забезпечення цифрової дипломатії та інформаційної безпеки Німеччини характеризується розподілом повноважень між численними державними відомствами та агенціями, кожна з яких має специфічні функції у загальній архітектурі національної кібербезпеки, при цьому Федеральне міністерство закордонних справ відіграє центральну координуючу роль у формуванні зовнішніх аспектів німецької політики у цій сфері, Федеральне відомство з інформаційної безпеки забезпечує технічний захист урядових систем та координацію національного реагування на кіберінциденти, Федеральна служба захисту конституції займається виявленням іноземного кібершпигунства та інформаційного втручання, Кіберкомандування Бундесверу розвиває військові кіберспроможності, а Інститут Гете просуває німецьку культуру у цифровому просторі як елемент м'якої сили. Ефективність цієї складної інституційної системи залежить від якості міжвідомчої координації та здатності різних акторів узгоджувати свої дії у відповідь на динамічні виклики інформаційного простору, при цьому європейський та трансатлантичний виміри німецької інституційної архітектури у сфері цифрової дипломатії та інформаційної безпеки відображають стратегічний вибір Німеччини на користь багатосторонності та колективних підходів до вирішення проблем цифрової епохи. Розуміння інституційної структури німецької системи забезпечення цифрової дипломатії створює необхідне підґрунтя для аналізу конкретних практичних інструментів, які використовує Німеччина для реалізації своїх стратегічних пріоритетів у сфері інформаційної безпеки.

2.3. Практичні інструменти цифрової дипломатії Німеччини у сфері інформаційної безпеки

Реалізація стратегічних пріоритетів німецької цифрової дипломатії у сфері інформаційної безпеки здійснюється через комплексний набір практичних

інструментів, які охоплюють як технологічні рішення для захисту інформаційних систем, так і комунікаційні стратегії для протидії дезінформації, формування сприятливих наративів та взаємодії з різноманітними аудиторіями через цифрові платформи, при цьому ефективність німецького підходу значною мірою залежить від здатності інтегрувати ці різноманітні інструменти у когерентну стратегію, яка б враховувала специфіку різних типів загроз, особливості різних комунікаційних каналів та культурні відмінності цільових аудиторій у різних регіонах світу. Німецька практика використання цифрової дипломатії для забезпечення інформаційної безпеки демонструє поступовий перехід від реактивних підходів, зосереджених на захисті від конкретних загроз, до проактивних стратегій формування інформаційного середовища у спосіб, що сприяє реалізації німецьких національних інтересів та ускладнює просування ворожих наративів, водночас німецький уряд прагне дотримуватися демократичних принципів та уникати використання маніпулятивних технік чи дезінформації навіть у протистоянні з противниками, які не обтяжують себе такими етичними обмеженнями, що іноді створює асиметрію у можливостях впливу на інформаційний простір порівняно з авторитарними режимами.

Протидія дезінформації становить один з найважливіших практичних напрямів німецької цифрової дипломатії у сфері інформаційної безпеки, оскільки німецьке керівництво усвідомлює серйозність загрози, яку становлять координовані дезінформаційні кампанії для стабільності демократичних інститутів, соціальної згуртованості та довіри громадян до офіційних джерел інформації [42, с. 89]. Німецький підхід до протидії дезінформації базується на комплексній стратегії, що поєднує моніторинг інформаційного простору для раннього виявлення дезінформаційних кампаній, оперативне спростування неправдивих наративів через офіційні канали комунікації, підтримку незалежних фактчекінгових організацій та медіаграмотності населення, а також міжнародну співпрацю у виявленні та атрибуції скоординованих інформаційних операцій іноземних акторів, при цьому німецький уряд ретельно уникає створення централізованих урядових структур, які б мали повноваження визначати, що є правдою, а що дезінформацією, побоюючись, що це може створити небезпечні

прецеденти для державної цензури та обмеження свободи слова. Замість цього Німеччина робить ставку на підтримку плюралістичної екосистеми перевірки фактів, де незалежні журналісти, громадянські організації та академічні інституції відіграють провідну роль у викритті дезінформації, тоді як держава забезпечує фінансову підтримку таких ініціатив та створює правові рамки для відповідальності цифрових платформ за поширення неправдивої інформації.

Федеральне міністерство закордонних справ створило спеціалізований підрозділ стратегічних комунікацій, який здійснює цілодобовий моніторинг німецького та міжнародного інформаційного простору для виявлення дезінформаційних наративів, що стосуються Німеччини, її зовнішньої політики або європейської інтеграції, при цьому особлива увага приділяється російським та китайським державним медіа, а також підозрілим акаунтам у соціальних мережах, які демонструють ознаки координованої неавтентичної поведінки [56, с. 134]. Коли виявляється потенційно шкідливий дезінформаційний наратив, підрозділ стратегічних комунікацій оцінює його вірогідний вплив на громадську думку та приймає рішення про необхідність та форму реагування, при цьому стратегія реагування може варіюватися від простого ігнорування маргінальних наративів, які не мають значного поширення і реагування на які лише привернуло б до них додаткову увагу, до активного спростування через офіційні канали Міністерства закордонних справ у соціальних мережах, організації брифінгів для журналістів з наданням фактичної інформації, що спростовує дезінформацію, або координації спільних заяв з європейськими партнерами для демонстрації єдності у протистоянні іноземним інформаційним операціям. Німецькі дипломати також активно використовують двосторонні канали для конфіденційних демаршів щодо урядів держав, з території яких поширюється дезінформація про Німеччину, вимагаючи припинення таких кампаній та попереджаючи про можливі наслідки для двосторонніх відносин у разі продовження інформаційної агресії.

Важливим елементом німецької стратегії протидії дезінформації є підтримка незалежних фактчекінгових організацій через фінансування їхньої діяльності, сприяння їхній інтеграції у міжнародні мережі перевірки фактів та

забезпечення їхнього доступу до урядових джерел інформації для спростування неправдивих тверджень про діяльність німецького уряду [37]. Німеччина фінансує діяльність кількох провідних німецьких фактчекінгових організацій, які співпрацюють з міжнародною мережею перевірки фактів та інтегровані у програми партнерства з цифровими платформами, що дозволяє позначати неправдиву інформацію та зменшувати її поширення через алгоритмічні механізми, при цьому фактчекери зберігають повну редакційну незалежність від уряду та самостійно визначають, які твердження перевіряти та як оцінювати їхню достовірність, що забезпечує легітимність їхньої діяльності в очах громадськості та захищає їх від звинувачень у упередженості чи політичній ангажованості. Німецький уряд також підтримує дослідницькі проекти, спрямовані на вивчення механізмів поширення дезінформації у соціальних мережах, психологічних факторів, що роблять людей вразливими до маніпулятивних наративів, та ефективних стратегій комунікації для спростування неправдивої інформації без непередбаченого посилення її поширення через ефект зворотного удару, коли спроби спростування парадоксально зміцнюють переконання людей, які вже вірять у дезінформацію.

Кібердипломатія як специфічний напрям німецької цифрової дипломатії охоплює дипломатичні зусилля, спрямовані на формування міжнародних норм поведінки держав у кіберпросторі, координацію дипломатичних відповідей на кібератаки, просування застосування міжнародного права до кіберактивностей та розвиток заходів довіри між державами для зниження ризиків конфліктів у цифровому середовищі [40, с. 178]. Німецька кібердипломатія активно просуває ідею, що існуюче міжнародне право, включно зі Статутом ООН, міжнародним гуманітарним правом та принципами суверенітету і невтручання у внутрішні справи держав, повною мірою застосовується до кіберпростору, і держави несуть міжнародну відповідальність за кіберактивності, що порушують ці норми, незалежно від того, чи здійснюються такі дії безпосередньо урядовими структурами, чи недержавними акторами, яким держава надає притулок або підтримку. Німецькі дипломати беруть активну участь у роботі Групи урядових експертів ООН з питань інформаційної безпеки та Відкритої робочої групи, де

представляють європейську позицію щодо застосування міжнародного права до кіберпростору та просувають консенсус навколо додаткових норм відповідальної поведінки держав, які б конкретизували загальні принципи міжнародного права стосовно специфіки кіберсередовища.

Практична реалізація німецької кібердипломатії включає організацію міжнародних конференцій та експертних консультацій з питань кібербезпеки, де німецькі представники мають можливість просувати своє бачення майбутнього глобального кіберпростору та формувати коаліції держав-однодумців навколо спільних підходів до регулювання кіберактивностей [67, с. 201]. Німеччина також використовує двосторонні та багатосторонні канали для консультацій з партнерами про координовану дипломатичну відповідь на серйозні кіберінциденти, що впливають на кілька держав одночасно, при цьому німецькі дипломати наголошують на важливості спільних заяв та скоординованих санкцій проти держав або недержавних акторів, відповідальних за шкідливі кіберактивності, оскільки колективна відповідь має значно більший стримуючий ефект порівняно з діями окремих держав. Німеччина брала участь у кількох випадках координованої атрибуції кібератак на європейському рівні, коли Європейський Союз публічно звинувачував конкретні держави у здійсненні кіберагресії проти європейських інститутів чи держав-членів та застосовував дипломатичні санкції, включно з обмеженнями на видачу віз та заморожуванням активів осіб і організацій, причетних до кібератак, що демонструє готовність європейських держав використовувати дипломатичні інструменти для реагування на кіберзагрози та встановлення певних меж прийнятної поведінки у кіберпросторі.

Цифрові платформи відіграють центральну роль у реалізації німецької цифрової дипломатії, оскільки саме через соціальні мережі, відеохостинги, месенджери та інші онлайн-сервіси німецькі дипломатичні представництва встановлюють прямий контакт з глобальними аудиторіями, транслюють німецькі позиції з актуальних міжнародних питань та формують позитивний імідж Німеччини у різних регіонах світу [38, с. 234]. Федеральне міністерство закордонних справ має офіційні акаунти у всіх основних соціальних мережах,

включно з Twitter, Facebook, Instagram, LinkedIn, YouTube та TikTok, при цьому кожна платформа використовується з урахуванням її специфіки та особливостей аудиторії, що її відвідує, наприклад Twitter використовується переважно для оперативної комунікації з журналістами, політичними аналітиками та іншими професійними спостерігачами за міжнародною політикою, Instagram орієнтований на молодшу аудиторію і використовується для візуального представлення діяльності німецької дипломатії через фотографії та короткі відео, LinkedIn слугує платформою для професійної мережі та залучення експертної спільноти до дискусій про німецьку зовнішню політику, а TikTok експериментально використовується для досягнення наймолодшої аудиторії через розважальні, але інформативні короткі відео про Німеччину та її місце у світі. Німецькі посольства та консульства також мають власні акаунти у соціальних мережах, адаптовані до локальних контекстів та мовних особливостей країн перебування, що дозволяє вести більш таргетовану комунікацію з місцевими аудиторіями та швидко реагувати на події, що відбуваються у конкретних регіонах.

Стратегія використання соціальних мереж німецькою цифровою дипломатією базується на кількох ключових принципах, серед яких особливе значення мають автентичність комунікації, коли німецькі дипломати прагнуть спілкуватися природною мовою без надмірної формальності, що традиційно характеризує офіційну дипломатичну риторику, діалогічність взаємодії, яка передбачає не лише одностороннє транслювання повідомлень, а й активне залучення аудиторії через запитання, опитування та відповіді на коментарі користувачів, візуальність контенту, оскільки дослідження показують, що пости з фотографіями та відео мають значно вищі показники залученості порівняно з текстовими повідомленнями, а також регулярність присутності, що вимагає постійного оновлення контенту та підтримання активності у соціальних мережах навіть у періоди без значних подій [59, с. 267]. Німецьке Міністерство закордонних справ розробило детальні внутрішні керівництва для співробітників, відповідальних за соціальні мережі у дипломатичних представництвах, які визначають допустимі теми для обговорення, тон

комунікації, процедури реагування на критику чи провокації, а також механізми ескалації у випадках, коли ситуація в онлайн-просторі виходить з-під контролю та вимагає втручання вищого керівництва для прийняття рішень про подальшу стратегію комунікації.

Використання стратегічних наративів є важливим інструментом німецької цифрової дипломатії для формування сприятливого інформаційного середовища та просування німецького бачення актуальних міжнародних проблем через конструювання переконливих історій, які резонують з цінностями та переконаннями цільових аудиторій у різних регіонах світу [44, с. 298]. Німецька цифрова дипломатія активно використовує кілька ключових наративів, включно з наративом про Німеччину як відповідального міжнародного актора, який навчився на трагічних уроках своєї історії та тепер послідовно виступає за мирне вирішення конфліктів, повагу до міжнародного права та захист прав людини, наратив про Німеччину як технологічного лідера та надійного партнера у цифровій трансформації, що пропонує етичний підхід до використання нових технологій на противагу авторитарним моделям цифрового контролю, наратив про Німеччину як рушійну силу європейської інтеграції, яка демонструє, що колишні вороги можуть стати близькими партнерами через спільні інститути та цінності, а також наратив про Німеччину як захисника багатосторонності та правозасноваого міжнародного порядку у протистоянні з односторонніми діями та силовою політикою. Ці стратегічні наративи систематично транслюються через різноманітні канали цифрової комунікації, при цьому вони адаптуються до специфіки різних аудиторій та контекстів, щоб максимізувати їхню переконливість та резонанс з локальними дискусіями про актуальні проблеми міжнародної політики.

Фактчекінг як практичний інструмент німецької цифрової дипломатії у сфері інформаційної безпеки передбачає не лише фінансову підтримку незалежних організацій, що займаються перевіркою фактів, а й активну участь німецьких дипломатичних представництв у спростуванні конкретних неправдивих тверджень про Німеччину, її політику чи діяльність німецьких інституцій через надання точної фактичної інформації у доступній формі [3, с.

156]. Федеральне міністерство закордонних справ створило спеціальну рубрику у своїх соціальних мережах під назвою "Факти замість фейків", де регулярно публікуються спростування найбільш поширених неправдивих тверджень про німецьку зовнішню політику, при цьому спростування подаються не у формі агресивної полеміки, а через чітке викладення фактів з посиланнями на перевірені джерела інформації, що дозволяє аудиторії самостійно оцінити достовірність різних версій подій. Німецькі посольства також активно співпрацюють з локальними фактчекінговими організаціями у країнах перебування, надаючи їм доступ до офіційної інформації для перевірки тверджень про діяльність Німеччини та підтримуючи їхні зусилля з викриття дезінформаційних кампаній, що можуть негативно впливати на сприйняття Німеччини у локальних суспільствах, при цьому німецькі дипломати ретельно уникають тиску на фактчекерів щодо висновків їхніх перевірок та поважають їхню редакційну незалежність навіть у випадках, коли результати фактчекінгу не повністю відповідають німецьким інтересам.

Координація діяльності з протидії дезінформації на європейському рівні є важливим аспектом німецької практики використання цифрової дипломатії для забезпечення інформаційної безпеки, оскільки багато дезінформаційних кампаній мають транснаціональний характер і спрямовані не лише проти окремих держав, а проти європейської інтеграції загалом або трансатлантичної єдності [51, с. 189]. Німеччина активно підтримує діяльність Групи стратегічних комунікацій Європейського Союзу, яка здійснює моніторинг російських дезінформаційних кампаній проти ЄС та його держав-членів і координує європейську відповідь через спільні спростування та стратегічні комунікації, при цьому німецькі експерти відіграють провідну роль у роботі цієї групи та сприяють формуванню спільних європейських наративів для протидії ворожій пропаганді. Німеччина також підтримала створення Європейського центру передового досвіду з протидії гібридним загрозам у Гельсінкі, який займається аналізом гібридних кампаній, що поєднують кібератаки, дезінформацію та інші інструменти впливу, і розробкою рекомендацій для європейських держав щодо підвищення стійкості перед такими загрозами, демонструючи тим самим

усвідомлення необхідності комплексного підходу до протидії сучасним інформаційним загрозам, які не обмежуються виключно цифровим простором.

Таким чином, практичні інструменти німецької цифрової дипломатії у сфері інформаційної безпеки охоплюють широкий спектр заходів від протидії дезінформації через моніторинг, оперативне спростування та підтримку фактчекінгу до активного використання соціальних мереж для прямої комунікації з глобальними аудиторіями, просування стратегічних наративів та формування позитивного іміджу Німеччини у світі, при цьому кібердипломатія як специфічний напрям зусиль спрямована на формування міжнародних норм поведінки у кіберпросторі та координацію дипломатичних відповідей на кібератаки. Німецький підхід характеризується прагненням поєднувати ефективність у досягненні зовнішньополітичних цілей з дотриманням демократичних принципів та етичних стандартів, що іноді створює певні обмеження у конкуренції з авторитарними режимами, які не мають подібних самообмежень, водночас німецьке керівництво переконане, що довгострокова ефективність цифрової дипломатії залежить саме від її легітимності та довіри до неї з боку міжнародної спільноти, які можуть бути забезпечені лише через послідовне дотримання декларованих цінностей та відмову від маніпулятивних практик. Розглянуті практичні інструменти німецької цифрової дипломатії демонструють комплексний підхід до забезпечення інформаційної безпеки, який поєднує технологічні рішення з комунікаційними стратегіями, національні зусилля з міжнародною співпрацею, оборонні заходи з проактивним формуванням інформаційного середовища, створюючи багаторівневу систему захисту німецьких інтересів у глобальному цифровому просторі.

Висновки до розділу 2

Аналіз стратегії та інституційного механізму цифрової дипломатії Німеччини, здійснений у другому розділі дослідження, дозволяє сформулювати низку важливих висновків про особливості німецького підходу до використання цифрових технологій у зовнішній політиці та забезпеченні інформаційної

безпеки держави, які відображають як загальні тенденції адаптації традиційної дипломатії до викликів цифрової епохи, так і специфічні риси, зумовлені історичним досвідом Німеччини, її роллю у європейській інтеграції та прагненням поєднувати технологічні інновації з фундаментальними демократичними цінностями. Формування німецької цифрової дипломатії відбувалося поетапно протягом останніх двох десятиліть у відповідь на технологічні зміни глобального комунікаційного середовища та зростаючі загрози інформаційній безпеці, при цьому кожен етап характеризувався поглибленням розуміння стратегічного значення цифрового простору для реалізації національних інтересів та поступовим розширенням інструментарію німецької цифрової дипломатії від простої технічної модернізації комунікаційної інфраструктури до комплексної стратегії формування інформаційного середовища як складової забезпечення національної безпеки.

Еволюція німецької зовнішньої інформаційної політики демонструє якісну трансформацію підходів від переважно технократичного розуміння цифровізації як процесу впровадження нових технологій до стратегічного бачення цифрової дипломатії як важливого інструменту забезпечення національної безпеки, просування німецьких інтересів у глобальному інформаційному просторі та захисту демократичних інститутів від іноземного інформаційного втручання. Каталізаторами цієї трансформації стали кілька ключових подій, включно з розголосом про масове стеження американських спецслужб, яке викрило вразливість німецького інформаційного простору перед зовнішніми загрозами, російською агресією проти України та супутніми інформаційними операціями, які продемонстрували реальність гібридних загроз для європейської безпеки, а також численними спробами втручання у виборчі процеси західних демократій через кібератаки та дезінформаційні кампанії, що остаточно переконали німецьке керівництво у необхідності розвитку адекватних інструментів протидії інформаційній агресії. Концептуалізація німецької цифрової дипломатії через поняття Digitale Außenpolitik та Cyber-Außenpolitik відображає багатовимірний характер цього феномену, що охоплює як широкі питання цифрової трансформації зовнішньої політики та використання цифрових платформ для

комунікації з глобальними аудиторіями, так і специфічні виклики кібербезпеки у міжнародних відносинах, включно з протидією кібератакам, розробкою міжнародних норм відповідальної поведінки держав у кіберпросторі та формуванням механізмів стримування кіберагресії.

Стратегічні пріоритети німецької цифрової дипломатії включають просування концепції відкритого, безпечного та заснованого на правилах кіберпростору як альтернативи авторитарним моделям жорсткого державного контролю над інтернетом, зміцнення кіберстійкості Європейського Союзу та його держав-членів через розвиток спільних механізмів реагування на кіберінциденти та формування європейського технологічного суверенітету, активну протидію дезінформації та захист демократичних процесів від іноземного інформаційного втручання через системну роботу з підвищення медіаграмотності населення та підтримку незалежної журналістики, забезпечення захисту прав людини в цифровому просторі через просування європейських стандартів захисту даних та протидію використанню цифрових технологій для масового стеження і придушення дисидентства, а також розвиток цифрової публічної дипломатії для просування позитивного іміджу Німеччини у світі та формування глобальних мереж підтримки німецьких ініціатив у різних сферах міжнародної політики. Ці стратегічні пріоритети формувалися під впливом усвідомлення множинних викликів та можливостей, що виникають у зв’язку з цифровізацією міжнародних відносин, і відображають прагнення Німеччини зайняти лідируючі позиції у формуванні глобального цифрового порядку, заснованого на демократичних цінностях, верховенстві права та захисті прав людини, при цьому німецький підхід тісно пов’язаний із загальноєвропейськими ініціативами у сфері цифрової політики та кібербезпеки, оскільки Німеччина розглядає Європейський Союз як критично важливу платформу для консолідації зусиль європейських держав у протистоянні глобальним викликам цифрової епохи.

Інституційна структура забезпечення німецької цифрової дипломатії та інформаційної безпеки характеризується розподілом повноважень між численними державними відомствами та спеціалізованими агенціями, що

відображає федеральний устрій Німеччини та традиційний німецький підхід до розподілу влади, спрямований на запобігання надмірній концентрації повноважень у руках однієї інституції, водночас створюючи певні виклики для швидкого прийняття рішень та координації дій у динамічному інформаційному просторі. Федеральне міністерство закордонних справ відіграє центральну координуючу роль у формуванні та реалізації зовнішніх аспектів німецької політики у сфері цифрової дипломатії, створивши спеціалізовані підрозділи стратегічних комунікацій, цифрової та кіберзовнішньої політики, а також призначивши офіцерів цифрової дипломатії у німецьких посольствах по всьому світу для забезпечення ефективної присутності Німеччини у глобальному цифровому просторі. Федеральне відомство з інформаційної безпеки забезпечує технічний захист урядових інформаційних систем, координацію національного реагування на кіберінциденти та надання рекомендацій щодо безпечного використання цифрових технологій державному та приватному секторам, зберігаючи при цьому виключно превентивний та технічний характер своєї діяльності без правоохоронних або розвідувальних повноважень. Федеральна служба захисту конституції займається виявленням та протидією іноземному кібершпигунству та інформаційним операціям іноземних спецслужб на німецькій території, надаючи розвідувальну інформацію для атрибуції кібератак та підготовки дипломатичних відповідей, тоді як Кіберкомандування Бундесверу розвиває військові кіберспроможності для захисту військової інфраструктури та стримування потенційних агресорів.

Ефективність складної інституційної системи німецької цифрової дипломатії та забезпечення інформаційної безпеки значною мірою залежить від якості міжвідомчої координації через Раду національної кібербезпеки та інші механізми узгодження дій різних державних структур у відповідь на інформаційні виклики, при цьому особлива увага приділяється чіткому визначенню сфер відповідальності різних акторів та уникненню дублювання функцій або конфліктів юрисдикцій між відомствами. Європейський та трансатлантичний виміри німецької інституційної архітектури у сфері цифрової дипломатії та інформаційної безпеки відображають стратегічний вибір

Німеччини на користь багатосторонності та колективних підходів до вирішення проблем цифрової епохи, що виявляється в активній підтримці розвитку інституційних спроможностей Європейського Союзу у сфері кібербезпеки, участі у механізмах НАТО з кібероборони та співпраці з міжнародними організаціями для просування німецького бачення глобального цифрового порядку. Інститут Гете як провідна інституція німецької культурної дипломатії доповнює більш політичні аспекти німецької цифрової дипломатії через просування німецької мови та культури у цифровому просторі, створюючи позитивний фон для сприйняття Німеччини у світі та формуючи довгострокові зв'язки з глобальними елітами та молодіжними лідерами думок.

Практичні інструменти німецької цифрової дипломатії у сфері інформаційної безпеки демонструють комплексний підхід, який поєднує протидію дезінформації через моніторинг інформаційного простору, оперативне спростування неправдивих наративів та підтримку незалежного фактчекінгу з активним використанням соціальних мереж для прямої комунікації з глобальними аудиторіями, просуванням стратегічних наративів про Німеччину як відповідального міжнародного актора та технологічного лідера, а також кібердипломатичними зусиллями з формування міжнародних норм поведінки у кіберпросторі та координації дипломатичних відповідей на кібератаки. Німецький підхід до протидії дезінформації базується на принципах підтримки плюралістичної екосистеми перевірки фактів замість створення централізованих урядових структур, що визначають істину, підвищення медіаграмотності населення для формування критичного мислення та стійкості перед маніпулятивними впливами, а також міжнародної співпраці у виявленні та атрибуції скоординованих дезінформаційних кампаній іноземних акторів, при цьому німецький уряд ретельно дотримується балансу між ефективною протидією дезінформації та збереженням свободи слова і уникненням створення прецедентів для державної цензури.

Використання цифрових платформ та соціальних мереж німецькою дипломатією здійснюється з урахуванням специфіки кожної платформи та особливостей її аудиторії, при цьому стратегія комунікації базується на

принципах автентичності, діалогічності, візуальності контенту та регулярності присутності, що дозволяє ефективно досягати різноманітних цільових аудиторій від професійних спостерігачів за міжнародною політикою до молоді, яка отримує інформацію переважно через розважальні платформи. Стратегічні наративи німецької цифрової дипломатії систематично транслюються через різноманітні канали цифрової комунікації та адаптуються до специфіки різних аудиторій для максимізації їхньої переконливості та резонансу з локальними дискусіями про актуальні проблеми міжнародної політики, при цьому ці наративи послідовно підкреслюють прихильність Німеччини міжнародному праву, багатосторонності, захисту прав людини та етичному використанню технологій як альтернативу авторитарним моделям цифрового розвитку. Німецький підхід до цифрової дипломатії характеризується прагненням поєднувати ефективність у досягненні зовнішньополітичних цілей з дотриманням демократичних принципів та етичних стандартів, що створює певну асиметрію у можливостях впливу на інформаційний простір порівняно з авторитарними режимами, водночас німецьке керівництво переконане, що довгострокова ефективність цифрової дипломатії залежить саме від її легітимності та довіри до неї з боку міжнародної спільноти, які можуть бути забезпечені лише через послідовне дотримання декларованих цінностей та відмову від маніпулятивних практик.

РОЗДІЛ 3. ЦИФРОВА ДИПЛОМАТІЯ НІМЕЧЧИНИ ЯК МОДЕЛЬ ДЛЯ ЗМІЦНЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Оцінка ефективності цифрової дипломатії Німеччини у забезпеченні інформаційної безпеки

Оцінка ефективності цифрової дипломатії Німеччини як інструменту забезпечення інформаційної безпеки вимагає комплексного аналізу, який би враховував не лише формальні показники цифрової присутності німецьких дипломатичних представництв у глобальному інформаційному просторі, а й реальний вплив німецьких цифрових дипломатичних практик на формування міжнародного порядку денного, протидію інформаційним загрозам та досягнення конкретних зовнішньополітичних цілей Німеччини в умовах загострення інформаційної конкуренції між державами [40, с. 45]. Порівняльний аналіз німецького підходу до цифрової дипломатії з практиками інших провідних держав та інтеграційних об’єднань дозволяє виявити як сильні сторони німецької моделі, що можуть бути адаптовані іншими країнами для зміцнення власної інформаційної безпеки, так і її обмеження, зумовлені специфічними політичними, інституційними та культурними факторами німецького контексту, які ускладнюють пряме копіювання німецького досвіду без урахування національних особливостей інших держав. Оцінка ефективності цифрової дипломатії є методологічно складним завданням, оскільки традиційні метрики успішності зовнішньої політики часто виявляються недостатніми для вимірювання впливу в інформаційному просторі, де результати можуть бути відстрочені в часі, опосередковані численними факторами та важко атрибутовані до дій конкретних акторів, що вимагає розробки нових підходів до оцінювання ефективності цифрової дипломатії через поєднання кількісних показників цифрової присутності з якісним аналізом стратегічних наслідків цифрових дипломатичних практик для досягнення національних інтересів держави.

Порівняльний аналіз німецької моделі цифрової дипломатії з французькою практикою виявляє як схожості у загальних підходах європейських держав до використання цифрових технологій у зовнішній політиці, так і суттєві відмінності в акцентах, інституційних механізмах та риториці, що відображають

різні національні традиції дипломатії та різне розуміння ролі держави в інформаційному просторі [54, с. 112]. Франція традиційно демонструє більш централізований та державоцентричний підхід до цифрової дипломатії, коли Міністерство закордонних справ та інші державні інституції відіграють домінуючу роль у формуванні французької присутності в цифровому просторі, тоді як німецький підхід характеризується більшою децентралізацією та залученням недержавних акторів, включно з академічними інституціями, громадянськими організаціями та приватними компаніями, до реалізації цифрової дипломатичної стратегії. Французька цифрова дипломатія традиційно приділяє більше уваги просуванню французької мови та культури як інструментів м'якої сили, використовуючи цифрові платформи для глобального поширення франкофонії та французьких культурних цінностей, натомість німецька цифрова дипломатія більше зосереджена на просуванні конкретних політичних ініціатив, нормативних програм у сфері регулювання цифрового простору та формуванні міжнародних коаліцій навколо спільних підходів до вирішення глобальних викликів цифрової епохи, що відображає різні національні ідентичності та історичні традиції зовнішньої політики цих двох провідних європейських держав.

Водночас і Німеччина, і Франція демонструють спільну прихильність європейському підходу до регулювання цифрового простору, заснованому на захисті прав людини, верховенстві права та демократичних цінностях, що відрізняє європейську модель цифрової дипломатії від американської, яка більше акцентує свободу комерції та мінімальне державне регулювання інтернету, та від китайської, що наголошує на цифровому суверенітеті та праві держав контролювати інформаційні потоки на своїй території [38]. Німеччина та Франція тісно координують свої позиції у європейських та міжнародних форумах з питань цифрової політики та кібербезпеки, часто виступаючи спільно для просування європейських ініціатив та формування балансу між американським та китайським підходами до регулювання глобального цифрового простору, при цьому обидві держави інвестують значні ресурси у розвиток європейської технологічної автономії та зміцнення кіберстійкості

Європейського Союзу як передумови ефективної європейської цифрової дипломатії. Специфічною особливістю німецького підходу порівняно з французьким є більша обережність у питаннях розвитку наступальних кіберспроможностей та публічної комунікації про військові аспекти кібербезпеки, що відображає більш пацифістську політичну культуру Німеччини та чутливість німецького суспільства до питань мілітаризації будь-яких сфер державної політики внаслідок історичного досвіду двох світових воєн.

Порівняння німецької цифрової дипломатії з загальноєвропейським підходом, втіленим у діяльності Європейської служби зовнішніх дій та інших інституцій Європейського Союзу, виявляє, що Німеччина часто виступає рушійною силою європейських ініціатив у сфері цифрової політики та інформаційної безпеки, при цьому німецькі дипломати та експерти відіграють провідну роль у формуванні європейської стратегії протидії дезінформації, розробці загальноєвропейських підходів до кібербезпеки та просуванні європейських цінностей у глобальних дискусіях про майбутнє цифрового простору [43, с. 156]. Водночас європейський рівень надає Німеччині додаткові можливості для реалізації своєї цифрової дипломатичної стратегії через мультиплікацію німецького впливу завдяки європейським інституціям, які мають більші ресурси та легітимність порівняно з окремими державами-членами, при цьому Німеччина прагне забезпечити, щоб європейська цифрова дипломатія відображала німецькі пріоритети та підходи, активно працюючи над формуванням консенсусу серед держав-членів навколо німецького бачення ключових питань цифрової політики. Європейський Союз як колективний актор цифрової дипломатії має певні переваги порівняно з окремими державами-членами, оскільки може пропонувати доступ до великого єдиного ринку як стимул для третіх країн приймати європейські стандарти регулювання цифрового простору, має більші фінансові ресурси для підтримки партнерів у розбудові їхньої кіберстійкості та може говорити від імені понад чотирьохсот мільйонів громадян, що надає європейським позиціям значну вагу в міжнародних дискусіях про глобальне цифрове управління.

Порівняння німецької та американської моделей цифрової дипломатії

виявляє фундаментальні відмінності у підходах, ресурсах та пріоритетах, що відображають різні геополітичні позиції цих держав та різні політичні культури щодо ролі держави в інформаційному просторі і відносин між урядом та технологічним сектором [39]. Сполучені Штати мають значні переваги у цифровій дипломатії завдяки домінуванню американських технологічних компаній у глобальному цифровому просторі, що надає американському уряду потужні інструменти впливу через контроль над цифровою інфраструктурою, на якій базується сучасна міжнародна комунікація, при цьому американська цифрова дипломатія може опиратися на величезні ресурси та глобальний досяг таких компаній як Google, Facebook, Twitter та інших цифрових платформ, які хоча формально і є приватними компаніями, але часто співпрацюють з американським урядом у просуванні американських інтересів за кордоном. Американська модель цифрової дипломатії характеризується більш агресивним використанням цифрових технологій для просування демократії та підтримки опозиційних рухів в авторитарних країнах, що іноді викликає звинувачення у втручанні у внутрішні справи інших держав, тоді як німецький підхід є більш обережним та зосередженим на багатосторонніх механізмах просування демократичних цінностей через міжнародні інституції та підтримку незалежних громадянських організацій без прямого державного керівництва їхньою діяльністю.

Водночас німецька модель має певні переваги порівняно з американською у контексті європейського регіону та відносин з партнерами, які скептично ставляться до американського глобального лідерства, оскільки Німеччина сприймається як менш загрозлива для суверенітету інших держав і більш послідовна у дотриманні міжнародного права та багатосторонніх підходів до вирішення глобальних проблем [54, с. 178]. Німецька цифрова дипломатія також може бути більш ефективною у просуванні регуляторних підходів до управління цифровим простором, оскільки Європейський Союз під німецьким лідерством розробив найбільш комплексну систему регулювання цифрових технологій, включно з Загальним регламентом захисту даних, Актом про цифрові послуги та Актом про цифрові ринки, які поступово стають глобальними стандартами через

процес так званої брюссельської ефекту, коли інші держави та компанії приймають європейські стандарти для збереження доступу до європейського ринку. Американська цифрова дипломатія натомість більше зосереджена на просуванні свободи інтернету та мінімального державного регулювання, що відображає як економічні інтереси американських технологічних компаній, так і ідеологічну прихильність американського суспільства принципам вільного ринку та обмеженого урядового втручання, при цьому останніми роками спостерігається певне зближення американського та європейського підходів у міру зростання занепокоєння в США щодо зловживань цифровими платформами своїм ринковим становищем та недостатнього захисту приватності користувачів.

Оцінка результатів німецької цифрової дипломатії у забезпеченні інформаційної безпеки свідчить про певні успіхи у досягненні стратегічних цілей, включно з формуванням міжнародного консенсусу навколо застосування міжнародного права до кіберпростору, розбудовою європейських механізмів протидії дезінформації та кіберзагрозам, а також зміцненням позицій Німеччини як провідного гравця у глобальних дискусіях про майбутнє цифрового управління [51, с. 201]. Німеччина успішно використала свою цифрову дипломатію для мобілізації міжнародної підтримки європейських ініціатив у сфері захисту персональних даних, що знайшло відображення у прийнятті багатьма країнами законодавства, інспірованого європейським Загальним регламентом захисту даних, а також для формування коаліцій держав-однодумців, які підтримують німецькі позиції щодо неприпустимості використання кіберзброї проти критичної цивільної інфраструктури та необхідності розвитку заходів довіри у кіберпросторі для зниження ризиків конфліктів. Німецькі цифрові дипломатичні зусилля також сприяли підвищенню міжнародної обізнаності про загрози дезінформації для демократичних процесів та мобілізації ресурсів для підтримки незалежної журналістики, фактчекінгу та медіаграмотності як у Європі, так і в інших регіонах світу, при цьому Німеччина змогла позиціонувати себе як надійного партнера для країн, що прагнуть зміцнити свою інформаційну стійкість без впровадження авторитарних методів контролю над інформаційним простором.

Водночас німецька цифрова дипломатія стикається з низкою викликів, які обмежують її ефективність у досягненні всіх поставлених цілей та вимагають подальшого розвитку стратегії, інституційних механізмів та практичних інструментів для адаптації до динамічного інформаційного середовища [39]. Першим викликом є обмеженість ресурсів, які Німеччина може виділити на цифрову дипломатію порівняно з масштабами завдань, оскільки протидія добре фінансованим дезінформаційним кампаніям авторитарних режимів, моніторинг глобального інформаційного простору та утримання постійної присутності у численних цифрових платформах вимагають значних людських та фінансових ресурсів, які часто перевищують можливості навіть такої економічно потужної держави як Німеччина. Другим викликом є складність швидкого реагування на інформаційні інциденти через бюрократичні процедури узгодження позицій між різними відомствами та необхідність дотримання правових обмежень на комунікаційну діяльність держави, що іноді призводить до того, що німецькі офіційні спростування дезінформації з'являються з затримкою, коли неправдивий наратив уже встиг поширитися та укорінитися у свідомості певної частини аудиторії. Третім викликом є асиметрія між демократичними обмеженнями німецької цифрової дипломатії, яка не може використовувати маніпулятивні техніки та дезінформацію навіть у протистоянні з ворожими інформаційними кампаніями, та відсутністю подібних обмежень у авторитарних режимів, що створює нерівні умови конкуренції в інформаційному просторі та іноді дозволяє противникам ефективніше впливати на певні аудиторії через використання емоційно заряджених, хоча і неправдивих, наративів.

Четвертим викликом для німецької цифрової дипломатії є технологічна залежність від іноземних цифрових платформ, переважно американських, які контролюють значну частину глобального інформаційного простору та можуть змінювати алгоритми видимості контенту, правила модерації або навіть блокувати акаунти на власний розсуд, що створює вразливості для німецької цифрової присутності та обмежує автономію німецької цифрової дипломатії [64, с. 234]. П'ятим викликом є складність вимірювання ефективності цифрової дипломатії та демонстрації конкретних результатів політичному керівництву та

громадськості, оскільки вплив цифрових комунікацій на формування міжнародної громадської думки та досягнення зовнішньополітичних цілей часто є опосередкованим, відстроченим у часі та важким для кількісного вимірювання, що ускладнює аргументацію на користь додаткових інвестицій у розвиток цифрової дипломатії в умовах конкуренції за бюджетні ресурси з іншими пріоритетами зовнішньої політики. Шостим викликом є необхідність постійної адаптації до швидких технологічних змін, оскільки нові цифрові платформи, формати контенту та комунікаційні практики виникають дуже швидко, а бюрократичні структури дипломатичних відомств часто не встигають адаптуватися до цих змін, внаслідок чого німецька цифрова дипломатія ризикує втратити релевантність для молодших поколінь, які мігрують на нові платформи швидше, ніж державні інституції можуть розгорнути там свою присутність.

Сьомим викликом є зростаюча поляризація глобального цифрового простору на конкуруючі інформаційні екосистеми, де аудиторії споживають інформацію переважно з джерел, що підтверджують їхні існуючі переконання, а алгоритми цифрових платформ посилюють цю тенденцію через персоналізацію контенту, що ускладнює досягнення німецькою цифровою дипломатією аудиторій, які скептично налаштовані до західних інституцій або вже піддалися впливу антизахідної пропаганди [37]. Восьмим викликом є етичні дилеми, пов’язані з використанням технологій штучного інтелекту, таргетованої реклами та аналітики великих даних у цифровій дипломатії, оскільки ці технології, хоча і можуть підвищити ефективність комунікації, також піднімають питання про маніпулювання поведінкою людей, порушення приватності та демократичну легітимність використання таких інструментів державою для впливу на громадську думку як всередині країни, так і за кордоном. Дев’ятим викликом є координація між національним рівнем німецької цифрової дипломатії та європейським рівнем, оскільки іноді виникають розбіжності у пріоритетах, підходах або риториці між німецькими та загальноєвропейськими цифровими дипломатичними ініціативами, що може призводити до плутанини у міжнародних партнерів щодо того, яка позиція є авторитетною, та зменшувати загальну ефективність європейської цифрової дипломатії через відсутність

єдиного голосу.

Попри ці виклики, німецька цифрова дипломатія демонструє певну ефективність у досягненні стратегічних цілей забезпечення інформаційної безпеки через поєднання різноманітних інструментів, багатостороннього підходу та послідовного дотримання демократичних цінностей, що забезпечує довгострокову легітимність німецьких ініціатив навіть за умови тактичних невдач у конкретних інформаційних кампаніях [40, с. 267]. Німецький досвід свідчить, що ефективна цифрова дипломатія вимагає не лише технологічних інвестицій та присутності у соціальних мережах, а й чіткого стратегічного бачення, розвинутих інституційних механізмів міжвідомчої координації, підготовлених кадрів з цифровими компетенціями, а також готовності до постійного навчання та адаптації до динамічних змін цифрового середовища, при цьому найбільш успішні аспекти німецької цифрової дипломатії пов’язані саме з тими напрямами, де Німеччина могла опертися на європейську співпрацю та залучити ресурси багатосторонніх механізмів для досягнення цілей, які були б недосяжними для окремої держави навіть з потужною економікою та розвиненою дипломатичною службою.

Таким чином, оцінка ефективності німецької цифрової дипломатії у забезпеченні інформаційної безпеки виявляє складну картину часткових успіхів та постійних викликів, при цьому порівняльний аналіз з французькою, загальноєвропейською та американською моделями демонструє, що німецький підхід має певні унікальні характеристики, включно з акцентом на багатосторонності, регуляторних ініціативах та етичних обмеженнях у використанні цифрових технологій для впливу на інформаційний простір, які відрізняють його від практик інших провідних акторів цифрової дипломатії. Німеччина досягла певних результатів у формуванні міжнародних норм поведінки у кіберпросторі, розбудові європейських механізмів протидії інформаційним загрозам та позиціонуванні себе як відповідального міжнародного актора у сфері цифрової політики, водночас стикаючись з викликами обмежених ресурсів, технологічної залежності від іноземних платформ, асиметрії у протистоянні з авторитарними режимами та складності

адаптації бюрократичних структур до динамічного цифрового середовища. Розуміння сильних сторін та обмежень німецької моделі цифрової дипломатії створює необхідне підґрунтя для аналізу впливу Німеччини на формування європейського інформаційного порядку та виявлення можливостей адаптації німецького досвіду для потреб інших держав, зокрема України, яка стикається з безпрецедентними інформаційними загрозами та потребує розвитку ефективних інструментів цифрової дипломатії для забезпечення своєї інформаційної безпеки.

3.2. Вплив цифрової дипломатії Німеччини на європейський інформаційний порядок

Німеччина як найбільша економіка Європейського Союзу та провідна політична сила європейської інтеграції відіграє ключову роль у формуванні європейського інформаційного порядку через активне використання цифрової дипломатії для просування спільних європейських підходів до регулювання цифрового простору, протидії інформаційним загрозам та захисту демократичних цінностей в умовах зростаючої інформаційної конкуренції з авторитарними режимами та транснаціональними недержавними акторами [46, с. 89]. Вплив німецької цифрової дипломатії на європейський інформаційний порядок здійснюється через кілька взаємопов’язаних механізмів, включно з ініціюванням та підтримкою загальноєвропейських законодавчих та політичних ініціатив у сфері цифрової політики та інформаційної безпеки, забезпеченням фінансових та експертних ресурсів для реалізації європейських програм протидії дезінформації та зміцнення кіберстійкості, формуванням консенсусу серед держав-членів Європейського Союзу навколо спільних підходів до актуальних викликів цифрової епохи, а також представленням європейської позиції у глобальних дискусіях про майбутнє цифрового управління, де Німеччина часто виступає від імені всього Європейського Союзу або в тісній координації з європейськими партнерами. Аналіз німецького впливу на європейський інформаційний порядок дозволяє зрозуміти механізми, через які середні держави

можуть мультиплікувати свій вплив у глобальному інформаційному просторі через регіональну інтеграцію та колективні дії, що має особливе значення для України як європейської держави, яка прагне інтегруватися до європейських інституцій та може скористатися європейськими механізмами для зміцнення власної інформаційної безпеки.

Роль Німеччини у формуванні політик Європейського Союзу проти дезінформації є центральною, оскільки саме німецькі ініціативи та фінансова підтримка в значній мірі зумовили створення та розвиток європейських механізмів моніторингу, аналізу та протидії дезінформаційним кампаніям, що загрожують демократичним процесам та соціальній згуртованості європейських суспільств [32, с. 112]. Після виявлення масштабних російських спроб втручання у виборчі процеси західних демократій, включно з американськими президентськими виборами 2016 року та референдумом про Brexit, Німеччина стала одним з найактивніших прихильників розбудови європейських спроможностей протидії дезінформації, усвідомлюючи, що федеральні вибори 2017 року в Німеччині також можуть стати об’єктом подібних інформаційних операцій, при цьому німецьке керівництво наголошувало на необхідності саме європейського, а не виключно національного, підходу до протидії дезінформації, оскільки транснаціональний характер цієї загрози вимагає координованих дій усіх держав-членів та розвитку спільних інструментів раннього виявлення та спростування дезінформаційних кампаній. Німеччина активно підтримала створення Групи стратегічних комунікацій Європейського Союзу при Європейській службі зовнішніх дій, яка здійснює систематичний моніторинг російських дезінформаційних кампаній проти ЄС та його держав-членів і координує європейську відповідь через щотижневі звіти про виявлені випадки дезінформації, стратегічні аналізи довгострокових тенденцій у російській пропаганді та рекомендації щодо ефективних комунікаційних стратегій для протидії ворожим наративам.

Німецький внесок у розвиток європейських механізмів протидії дезінформації включає не лише політичну підтримку, а й значні фінансові ресурси для забезпечення діяльності відповідних структур Європейського

Союзу, підтримку незалежних фактчекінгових організацій та дослідницьких центрів, що вивчають феномен дезінформації та розробляють ефективні стратегії протидії їй, а також експертизу німецьких фахівців, які беруть активну участь у роботі європейських структур та вносять досвід німецької практики протидії інформаційним загрозам [53]. Німеччина також ініціювала створення Європейської обсерваторії з цифрових медіа, яка об'єднує дослідників, представників цифрових платформ, фактчекерів та громадянських організацій для спільної роботи над виявленням дезінформації та розробкою кращих практик протидії їй без порушення свободи слова та інших фундаментальних прав, при цьому німецький підхід наголошує на важливості залучення самих цифрових платформ до відповідальності за поширення дезінформації через їхні сервіси та необхідності розвитку саморегуляторних механізмів індустрії під наглядом держави замість прямого урядового контролю над контентом, що циркулює в інтернеті. Німецький досвід прийняття закону про покращення забезпечення правопорядку в соціальних мережах, який зобов'язує великі платформи оперативно видаляти незаконний контент під загрозою значних штрафів, хоча і викликав критику з боку деяких правозахисників, які побоювалися надмірної цензури, став важливим прецедентом для інших європейських держав і вплинув на розробку загальноєвропейського Акту про цифрові послуги, який встановлює спільні правила відповідальності цифрових платформ за контент на всій території Європейського Союзу.

Німеччина також відіграла провідну роль у розробці та просуванні Європейського плану дій з демократії, представленого Європейською комісією у 2020 році, який охоплює комплекс заходів для захисту демократичних процесів від дезінформації та іноземного втручання, зміцнення незалежності та плюралізму медіа, підвищення медіаграмотності громадян та забезпечення прозорості політичної реклами, при цьому багато елементів цього плану відображають німецькі пріоритети та досвід роботи з інформаційними загрозами [38, с. 156]. Німецькі представники в європейських інституціях активно лобіювали включення до цього плану положень про необхідність посилення спроможностей незалежної журналістики через фінансову підтримку якісних

медіа, які зазнають економічних труднощів внаслідок трансформації бізнес-моделей у цифрову епоху, а також про важливість розвитку європейської цифрової інфраструктури та зменшення залежності від технологічних гігантів з інших регіонів світу для забезпечення європейської стратегічної автономії в інформаційній сфері. Німеччина також підтримала створення Європейського фонду для демократії, який надає фінансову допомогу незалежним медіа та громадянським організаціям у країнах Східного партнерства та на Західних Балканах для зміцнення їхньої стійкості перед дезінформацією та авторитарним тиском, розглядаючи підтримку демократичних процесів у сусідніх регіонах як важливий елемент забезпечення власної інформаційної безпеки через створення поясу стабільних демократій навколо Європейського Союзу.

Вплив Німеччини на формування європейської політики кібербезпеки також є значним, оскільки Німеччина послідовно виступає за розвиток спільних європейських спроможностей реагування на кіберінциденти, гармонізацію національних підходів до захисту критичної інфраструктури та створення європейської технологічної бази для забезпечення кібербезпеки без надмірної залежності від технологій з третіх країн [47, с. 189]. Німеччина активно підтримала прийняття та імплементацію Директиви про мережеву та інформаційну безпеку, яка встановлює мінімальні стандарти кібербезпеки для критичної інфраструктури у всіх державах-членах Європейського Союзу та вимагає створення національних центрів реагування на кіберінциденти і механізмів обміну інформацією про кіберзагрози між державами-членами та на рівні ЄС, при цьому німецький Федеральний офіс з інформаційної безпеки відіграв важливу роль у розробці технічних специфікацій та кращих практик для імплементації цієї директиви в національних контекстах різних держав-членів. Німеччина також виступила одним з головних прихильників створення Європейського центру компетенції з кібербезпеки та мережі національних координаційних центрів, які мають об’єднати дослідницькі та інноваційні зусилля у сфері кібербезпекових технологій на європейському рівні для розвитку європейської технологічної автономії та зменшення розриву з провідними світовими гравцями у цій критично важливій сфері, при цьому Німеччина

забезпечує значну частину фінансування цієї ініціативи та надає експертизу своїх провідних дослідницьких інститутів для роботи центру.

Німецький вплив на європейську політику регулювання цифрових платформ виявляється у послідовному просуванні ідеї, що великі технологічні компанії несуть соціальну відповідальність за наслідки функціонування їхніх платформ для суспільства і не можуть ховатися за статусом нейтральних посередників, коли їхні алгоритми активно формують інформаційне середовище та впливають на те, яку інформацію бачать користувачі [61]. Німеччина активно підтримала розробку Акту про цифрові послуги та Акту про цифрові ринки, які встановлюють нові правила для цифрових платформ у Європейському Союзі, включно з вимогами прозорості алгоритмів, відповідальності за незаконний контент, заборони дискримінаційних практик щодо бізнес-користувачів платформ та обмежень на використання персональних даних для таргетованої реклами, при цьому німецькі законодавці та регулятори активно ділилися своїм досвідом регулювання цифрових платформ на національному рівні для інформування європейського законодавчого процесу. Німецький підхід до регулювання цифрових платформ базується на принципі, що регулювання має бути пропорційним впливу платформи на суспільство, внаслідок чого найбільші платформи, які досягають статусу так званих привратників цифрової економіки, підлягають більш суворому регулюванню та несуть додаткові зобов’язання щодо забезпечення справедливої конкуренції, захисту користувачів та співпраці з державними органами у протидії незаконному контенту, при цьому цей принцип був значною мірою інкорпорований у європейське законодавство завдяки німецькому впливу на законодавчий процес Європейського Союзу.

Європейські ініціативи, очолювані або активно підтримані Німеччиною, демонструють комплексний підхід до формування європейського інформаційного порядку, який би поєднував захист демократичних цінностей та прав людини з інноваціями та економічним розвитком цифрової сфери, уникаючи як надмірного державного контролю за зразком авторитарних режимів, так і нерегульованого ринкового підходу, який дозволяє технологічним гігантам діяти без достатнього демократичного контролю [41, с. 223]. Німеччина

ініціювала створення Європейсько-німецького центру цифрової безпеки та демократії, який має об’єднати зусилля німецьких та інших європейських експертів у розробці інноваційних підходів до захисту демократичних процесів від цифрових загроз, включно з використанням штучного інтелекту для виявлення дезінформації, блокчейн-технологій для забезпечення достовірності інформації та інших передових технологій для зміцнення інформаційної стійкості європейських суспільств. Німеччина також підтримала ініціативу щодо створення Європейської академії цифрової дипломатії, яка має забезпечити спільну підготовку дипломатичних кадрів держав-членів Європейського Союзу до роботи в цифровому середовищі, обмін кращими практиками цифрової дипломатії та розвиток спільних підходів до використання цифрових технологій у зовнішній політиці ЄС, при цьому Німеччина забезпечує значну частину викладацького складу цієї академії та ділиться своїм досвідом розвитку цифрових дипломатичних спроможностей.

Німецький внесок у розвиток європейської стратегічної комунікації також є важливим, оскільки Німеччина послідовно наголошує на необхідності не лише реактивного спростування дезінформації, а й проактивного формування позитивних наративів про Європейський Союз, його цінності та досягнення для протидії євроскептичній пропаганді та зміцнення підтримки європейської інтеграції серед громадян держав-членів [46, с. 256]. Німеччина підтримала розширення мандату та ресурсів Європейської служби зовнішніх дій у сфері стратегічних комунікацій, включно зі створенням регіональних груп стратегічних комунікацій, які зосереджуються на специфічних викликах різних географічних регіонів, таких як російська дезінформація у Східному партнерстві, джихадистська пропаганда на Близькому Сході та в Північній Африці або китайські інформаційні операції в Індо-Тихоокеанському регіоні, при цьому німецькі експерти беруть активну участь у роботі цих груп та забезпечують методологічну підтримку їхньої діяльності на основі німецького досвіду стратегічних комунікацій. Німеччина також ініціювала створення спільної європейської платформи для координації цифрових публічних дипломатичних кампаній держав-членів ЄС, яка дозволяє узгоджувати повідомлення різних

національних дипломатичних служб у соціальних мережах для досягнення синергетичного ефекту та посилення європейського голосу в глобальному інформаційному просторі, при цьому Німеччина надає технічну інфраструктуру для функціонування цієї платформи та забезпечує навчання представників інших держав-членів роботі з нею.

Вплив Німеччини на формування європейського підходу до міжнародних переговорів про регулювання кіберпростору також є значним, оскільки Німеччина послідовно просуває європейське бачення застосування міжнародного права до кіберактивностей держав та необхідності розвитку додаткових норм відповідальної поведінки у кіберпросторі як альтернативу спробам авторитарних режимів легітимізувати необмежений державний суверенітет над національними сегментами інтернету [67]. Німеччина координує позиції держав-членів Європейського Союзу у роботі Групи урядових експертів ООН з питань інформаційної безпеки та Відкритої робочої групи, забезпечуючи, щоб європейські держави виступали з узгодженими позиціями та максимізували свій вплив на формування глобального консенсусу навколо правил гри в кіберпросторі, при цьому німецькі дипломати часто виступають від імені всього Європейського Союзу або координованої групи європейських держав у цих міжнародних форумах. Німеччина також активно підтримує європейську політику кібердипломатичного інструментарію, яка передбачає можливість застосування дипломатичних санкцій проти держав або недержавних акторів, відповідальних за шкідливі кіберактивності проти Європейського Союзу або його держав-членів, включно з обмеженнями на видачу віз, заморожуванням активів та публічним засудженням, що має стримуючий ефект на потенційних кіберагресорів та демонструє рішучість Європейського Союзу захищати свої інтереси в кіберпросторі.

Німецький вплив на європейський інформаційний порядок також виявляється у просуванні ініціатив щодо захисту прав людини в цифровому просторі, включно з правом на приватність, свободою вираження поглядів онлайн, захистом від дискримінації алгоритмами штучного інтелекту та забезпеченням цифрової інклюзії для всіх верств населення незалежно від віку,

освіти чи матеріального становища [32, с. 289]. Німеччина активно підтримала розробку та імплементацію Загального регламенту захисту даних Європейського Союзу, який встановив найсуворіші у світі стандарти захисту персональних даних та створив прецедент для аналогічного законодавства в інших регіонах світу через процес брюссельського ефекту, коли глобальні компанії змушені приймати європейські стандарти для збереження доступу до європейського ринку та часто поширюють ці стандарти на свою діяльність в інших юрисдикціях через економічну недоцільність підтримки різних режимів захисту даних для різних регіонів. Німеччина також підтримала європейські ініціативи щодо регулювання штучного інтелекта, включно з пропозицією Акту про штучний інтелект, який має встановити правові рамки для розробки та використання систем штучного інтелекта в Європейському Союзі, забезпечуючи баланс між стимулюванням інновацій та захистом фундаментальних прав людини від потенційних зловживань цими потужними технологіями, при цьому німецькі експерти з етики штучного інтелекта відіграли провідну роль у розробці принципів, закладених в основу європейського підходу до регулювання цієї технології.

Німецька ініціатива щодо створення європейської цифрової ідентичності, яка дозволить громадянам Європейського Союзу безпечно ідентифікуватися онлайн для отримання цифрових послуг як у державному, так і в приватному секторі, також відображає німецьке прагнення формувати європейський інформаційний порядок, заснований на захисті приватності та користувацькому контролі над власними даними на противагу моделям, де корпорації або уряди мають необмежений доступ до персональної інформації громадян [53, с. 201]. Німеччина забезпечує значну частину технічної розробки та фінансування проекту європейської цифрової ідентичності, а також координує зусилля різних держав-членів для забезпечення сумісності національних систем цифрової ідентифікації та їхньої інтеграції в єдину європейську систему, при цьому німецький підхід наголошує на важливості децентралізованої архітектури, яка мінімізує ризики витоку даних та зловживань через концентрацію інформації про громадян у центральних базах даних. Ця ініціатива має стратегічне значення не

лише для зручності громадян, а й для зміцнення європейської цифрової автономії через зменшення залежності від американських або китайських систем ідентифікації та створення європейської альтернативи, яка відповідає європейським цінностям захисту приватності та користувацького контролю над даними.

Таким чином, вплив німецької цифрової дипломатії на європейський інформаційний порядок є значним та багатовимірним, оскільки Німеччина відіграє ключову роль у формуванні європейських політик протидії дезінформації, кібербезпеки, регулювання цифрових платформ та захисту прав людини в цифровому просторі через ініціювання та підтримку численних загальноєвропейських законодавчих та політичних ініціатив, забезпечення фінансових та експертних ресурсів для їхньої реалізації, а також координацію позицій держав-членів Європейського Союзу у міжнародних дискусіях про майбутнє глобального цифрового управління. Німецький підхід до формування європейського інформаційного порядку характеризується прагненням поєднувати захист демократичних цінностей та фундаментальних прав з підтримкою інновацій та економічного розвитку цифрової сфери, при цьому уникаючи як надмірного державного контролю за зразком авторитарних режимів, так і нерегульованого ринкового підходу, який дозволяє технологічним корпораціям діяти без достатнього демократичного нагляду. Європейські ініціативи, очолювані або активно підтримані Німеччиною, поступово формують унікальну європейську модель цифрового управління, яка стає альтернативою американському та китайському підходам і поширюється на інші регіони світу через механізм брюссельського ефекту, коли інші держави та компанії приймають європейські стандарти для збереження доступу до європейського ринку або як взірець кращих практик у регулюванні цифрового простору. Розуміння механізмів німецького впливу на європейський інформаційний порядок та успішних європейських ініціатив у сфері цифрової політики створює важливий контекст для аналізу можливостей використання німецького та європейського досвіду для зміцнення інформаційної безпеки України.

3.3. Перспективи використання німецького досвіду для України

Україна як держава, що стикається з безпрецедентними інформаційними загрозами внаслідок російської агресії та гібридної війни, може значною мірою скористатися з вивчення та адаптації німецького досвіду цифрової дипломатії для зміцнення власної інформаційної безпеки, водночас враховуючи специфічні умови українського контексту, включно з обмеженими ресурсами порівняно з Німеччиною, іншою природою та інтенсивністю інформаційних загроз, а також відмінностями в інституційних спроможностях та політичній культурі, що вимагають творчої адаптації німецьких практик замість їхнього механічного копіювання [12, с. 67]. Перспективи використання німецького досвіду для України охоплюють кілька ключових напрямів, включно з інституційною розбудовою структур, відповідальних за цифрову дипломатію та інформаційну безпеку, впровадженням технологічних рішень для моніторингу інформаційного простору та протидії дезінформації, розвитком комунікаційних стратегій для ефективної взаємодії з різноманітними аудиторіями через цифрові платформи, а також поглибленням співпраці з європейськими партнерами для інтеграції України у європейські механізми забезпечення інформаційної безпеки та доступу до європейських ресурсів і експертизи у цій сфері. Аналіз німецького досвіду через призму українських потреб дозволяє сформулювати конкретні рекомендації, які могли б підвищити ефективність української цифрової дипломатії та зміцнити інформаційну стійкість українського суспільства перед ворожими інформаційними впливами, при цьому критично важливо враховувати, що Україна знаходиться в іншій ситуації порівняно з Німеччиною, оскільки веде фактичну війну з державою, яка має потужні можливості інформаційного впливу та не обмежує себе жодними етичними чи правовими нормами у використанні дезінформації та маніпуляцій.

Інституційні рекомендації для України на основі німецького досвіду включають насамперед необхідність створення чіткої координаційної структури, яка би об’єднувала зусилля різних державних відомств у сфері цифрової дипломатії та інформаційної безпеки, подолюючи фрагментацію повноважень та дублювання функцій, що часто характеризує українську систему управління у

цій сфері [9, с. 89]. Німецький досвід Ради національної кібербезпеки як міжвідомчого органу, що забезпечує координацію дій різних державних структур у відповідь на інформаційні виклики, може бути корисним для України, де існують численні відомства з частково перетинаючими повноваженнями у сфері інформаційної безпеки, включно з Міністерством закордонних справ, Міністерством цифрової трансформації, Службою безпеки України, розвідувальними органами та іншими структурами, які не завжди ефективно координують свої дії, що призводить до втрати ресурсів та зниження загальної ефективності української відповіді на інформаційні загрози. Створення в Україні аналогічного координаційного механізму з чітко визначеними повноваженнями, регулярними засіданнями на високому рівні та можливістю приймати рішення, обов'язкові для всіх відомств, могло б значно підвищити ефективність української системи забезпечення інформаційної безпеки через синхронізацію зусиль різних акторів та уникнення конфліктів між відомствами за сферами впливу.

Друга інституційна рекомендація стосується необхідності створення в Міністерстві закордонних справ України спеціалізованого підрозділу цифрової дипломатії, який би мав достатні ресурси та повноваження для координації української присутності у глобальному цифровому просторі, розробки стратегічних комунікаційних кампаній та оперативного реагування на дезінформацію про Україну [4]. Німецький досвід створення відділу стратегічних комунікацій у Федеральному міністерстві закордонних справ, який здійснює цілодобовий моніторинг інформаційного простору та координує німецьку відповідь на дезінформаційні кампанії, демонструє важливість наявності спеціалізованої структури з відповідними технічними можливостями та підготовленими кадрами для ефективної цифрової дипломатії, при цьому такий підрозділ має бути інтегрований у загальну структуру міністерства та мати прямий доступ до вищого керівництва для забезпечення оперативності прийняття рішень у динамічному інформаційному середовищі. Український підрозділ цифрової дипломатії міг би опиратися на німецький досвід у розробці внутрішніх керівництв для роботи дипломатів у соціальних мережах,

методологій моніторингу дезінформації та протоколів реагування на різні типи інформаційних інцидентів, адаптуючи ці документи до специфіки українського контексту та більш агресивного інформаційного середовища, у якому працює українська дипломатія порівняно з німецькою.

Третя інституційна рекомендація полягає у необхідності систематичного навчання українських дипломатів цифровим компетенціям та стратегічним комунікаціям, оскільки ефективна цифрова дипломатія вимагає не лише технічних навичок роботи з цифровими платформами, а й розуміння специфіки онлайн-комунікації, здатності швидко адаптуватися до нових форматів та платформ, а також вміння розробляти та реалізовувати комунікаційні стратегії для досягнення конкретних зовнішньополітичних цілей [17, с. 112]. Німецький досвід інвестування у спеціалізовані навчальні програми для дипломатів, включно з модулями про цифрову дипломатію, протидію дезінформації та стратегічні комунікації у Дипломатичній академії, може бути адаптований для України через створення аналогічних навчальних програм у Дипломатичній академії України при Міністерстві закордонних справ або через залучення українських дипломатів до участі у європейських навчальних програмах, де вони могли б обмінюватися досвідом з колегами з інших країн та вивчати кращі практики цифрової дипломатії. Особливої уваги заслуговує необхідність навчання українських дипломатів роботі в умовах активних дезінформаційних кампаній та інформаційних атак, оскільки українські представники за кордоном регулярно стикаються з більш агресивним інформаційним середовищем порівняно з їхніми німецькими колегами, що вимагає специфічних навичок та психологічної стійкості для ефективного виконання своїх функцій.

Технологічні рекомендації для України на основі німецького досвіду включають необхідність розвитку власних спроможностей моніторингу українського та міжнародного інформаційного простору для раннього виявлення дезінформаційних кампаній проти України, відстеження російської пропаганди та аналізу ефективності української комунікації з різними аудиторіями [24]. Німецький досвід використання спеціалізованих програмних інструментів для моніторингу соціальних мереж, аналізу великих масивів даних та виявлення

координованої неавтентичної поведінки може бути корисним для України, яка потребує розвитку подібних технічних спроможностей для ефективної протидії російським інформаційним операціям, при цьому Україна може або розвивати власні технологічні рішення через залучення українських ІТ-компаній, які мають значний досвід у галузі аналізу даних та штучного інтелекту, або закуповувати готові комерційні рішення у провідних західних компаній, що спеціалізуються на моніторингу інформаційного простору та виявленні дезінформації. Важливою є також розбудова українських спроможностей атрибуції джерел дезінформаційних кампаній через технічний аналіз цифрових слідів, що дозволило б Україні більш переконливо доводити міжнародній спільноті російську відповідальність за конкретні інформаційні операції та мобілізовувати підтримку партнерів для спільної відповіді на російську інформаційну агресію.

Друга технологічна рекомендація стосується необхідності розвитку технічних спроможностей кіберзахисту критичної інформаційної інфраструктури України, включно з урядовими інформаційними системами, інфраструктурою виборчих процесів та медіа, оскільки кібератаки часто поєднуються з дезінформаційними кампаніями у рамках комплексних гібридних операцій для досягнення максимального дестабілізуючого ефекту [21, с. 145]. Німецький досвід централізованої координації кіберзахисту через Федеральне відомство з інформаційної безпеки, яке надає технічну підтримку всім урядовим структурам та координує обмін інформацією про кіберзагрози між державним і приватним секторами, може бути частково адаптований для України через зміцнення спроможностей Державної служби спеціального зв’язку та захисту інформації України або створення нової спеціалізованої структури з виключно технічним мандатом у сфері кіберзахисту без правоохоронних чи розвідувальних функцій, що могло б підвищити довіру приватного сектору до співпраці з цією структурою та полегшити обмін інформацією про кіберзагрози. Україна також потребує інвестицій у розвиток національних кадрів у сфері кібербезпеки через створення спеціалізованих освітніх програм, стипендій для навчання за кордоном та створення привабливих умов праці у державному секторі для утримання талановитих фахівців, які інакше мігрують до приватного сектору або

за кордон через вищі зарплати та кращі умови праці.

Комунікаційні рекомендації для України на основі німецького досвіду підкреслюють важливість розвитку проактивних стратегічних комунікацій замість виключно реактивного спростування російської дезінформації, оскільки постійна гра у догонялки за російськими фейками виснажує ресурси та дозволяє противнику контролювати порядок денний інформаційного простору [12, с. 134]. Німецький досвід розробки та систематичного просування стратегічних наративів про Німеччину як відповідального міжнародного актора, технологічного лідера та захисника демократичних цінностей може бути адаптований для України через формування переконливих наративів про Україну як форпост європейської демократії у протистоянні з російським авторитаризмом, успішну історію трансформації пострадянської держави у сучасну європейську країну попри численні перешкоди, та надійного партнера для західних демократій у забезпеченні європейської безпеки, при цьому ці наративи мають систематично транслюватися через різноманітні канали цифрової комунікації та адаптуватися до специфіки різних аудиторій для максимізації їхнього резонансу. Україна має також розвивати емоційну складову своїх стратегічних комунікацій, використовуючи історії конкретних людей, візуальний контент високої якості та наративи, що апелюють до універсальних цінностей та викликають емпатію міжнародних аудиторій, оскільки дослідження показують, що емоційно заряджений контент має значно вищі показники поширення та впливу порівняно з суто фактичною інформацією.

Друга комунікаційна рекомендація стосується необхідності диференціації комунікаційних стратегій для різних аудиторій, оскільки універсальні повідомлення рідко є ефективними для всіх груп, і успішна цифрова дипломатія вимагає глибокого розуміння специфіки різних аудиторій, їхніх інформаційних потреб, цінностей та уподобань щодо форматів контенту і комунікаційних каналів [19]. Німецький досвід використання різних цифрових платформ для досягнення різних аудиторій, від Twitter для професійних спостерігачів до TikTok для молоді, може бути адаптований для України через більш стратегічне використання різноманітних цифрових платформ відповідно до їхньої специфіки

та аудиторій, при цьому українська цифрова дипломатія має приділяти особливу увагу платформам, популярним у ключових регіонах, де Україна прагне зміцнити свої позиції, таких як Латинська Америка, Африка або Азія, де домінують інші платформи порівняно з Європою та Північною Америкою. Україна також має розвивати багатомовну комунікацію, забезпечуючи присутність української дипломатії не лише англійською мовою, а й мовами ключових регіонів світу, що вимагає залучення перекладачів та локальних експертів для адаптації українських повідомлень до культурних контекстів різних суспільств та уникнення непорозумінь через культурні відмінності у сприйнятті певних символів, метафор чи способів аргументації.

Третя комунікаційна рекомендація підкреслює важливість розвитку партнерств з недержавними акторами, включно з незалежними медіа, фактчекерами, блогерами, культурними діячами та громадянськими організаціями, для мультиплікації українських повідомлень та досягнення аудиторій, які можуть бути скептичними до офіційних урядових джерел інформації [9, с. 178]. Німецький досвід підтримки незалежних фактчекінгових організацій при збереженні їхньої редакційної незалежності демонструє, що держава може бути каталізатором розвитку екосистеми верифікації інформації без прямого контролю над нею, що забезпечує більшу довіру до результатів фактчекінгу порівняно з ситуацією, коли держава сама визначає, що є правдою, а що дезінформацією, при цьому Україна вже має певний досвід підтримки незалежних фактчекерів через такі ініціативи як програми грантів для медіаграмотності та фактчекінгу, але цю підтримку варто розширювати та систематизувати для створення стійкої екосистеми перевірки інформації, здатної протистояти російській дезінформаційній машині. Україна також має активніше залучати українську діаспору за кордоном до цифрових комунікаційних зусиль, оскільки представники діаспори часто мають кращий доступ до локальних аудиторій, розуміють культурний контекст країн проживання та можуть бути переконливішими посланцями української позиції порівняно з офіційними дипломатами, при цьому держава може підтримувати діаспору через надання їй якісних інформаційних матеріалів, навчання стратегічним комунікаціям та

координацію зусиль різних діаспорних організацій для максимізації їхнього впливу.

Рекомендації щодо поглиблення співпраці з європейськими партнерами підкреслюють, що Україна має максимально використовувати можливості інтеграції у європейські механізми забезпечення інформаційної безпеки як через формальні канали співпраці у статусі кандидата на вступ до Європейського Союзу, так і через неформальні мережі обміну досвідом, спільні навчання та проекти з європейськими партнерами [36, с. 201]. Німецький досвід активної участі у європейських ініціативах протидії дезінформації та зміцнення кібербезпеки демонструє переваги багатостороннього підходу, коли держави об'єднують ресурси та експертизу для спільного вирішення транснаціональних проблем, при цьому Україна має домагатися повноцінної участі у роботі таких європейських структур як Група стратегічних комунікацій Європейського Союзу, Європейський центр компетенції з кібербезпеки та інші спеціалізовані механізми, що дозволило б Україні отримати доступ до європейської експертизи, технологій та ресурсів для зміцнення власної інформаційної безпеки. Німеччина як провідна держава Європейського Союзу та послідовний підтримувач європейської інтеграції України може відіграти важливу роль у сприянні такій інтеграції через підтримку українських запитів на участь у європейських програмах, надання двосторонньої технічної допомоги Україні для розбудови її спроможностей у сфері цифрової дипломатії та інформаційної безпеки, а також лобіювання інтересів України в європейських інституціях.

Друга рекомендація щодо європейської співпраці стосується необхідності активнішого залучення України до європейських ініціатив у сфері протидії російській дезінформації, оскільки Україна як держава, що безпосередньо протистоїть російській агресії, має унікальний досвід та експертизу у виявленні та аналізі російських інформаційних операцій, яка могла б збагатити європейське розуміння російської тактики та стратегії у інформаційній сфері [4, с. 234]. Україна вже співпрацює з Групою стратегічних комунікацій Європейського Союзу та іншими європейськими структурами, але цю співпрацю варто інституціоналізувати та поглиблювати через створення постійних механізмів

обміну інформацією, спільного аналізу загроз та координації відповідей на російські дезінформаційні кампанії, що загрожують як Україні, так і Європейському Союзу, при цьому Німеччина могла б виступити ініціатором створення спеціальної робочої групи з питань співпраці з Україною у сфері стратегічних комунікацій у рамках Європейської служби зовнішніх дій або іншої відповідної європейської структури. Україна також має активніше пропонувати свій досвід іншим державам, які стикаються з російськими інформаційними загрозами, включно з країнами Балтії, Центральної Європи, Західних Балканів та Східного партнерства, позиціонуючи себе як центр компетенції з питань протидії російській дезінформації та гібридним загрозам і пропонуючи навчання, консультації та обмін досвідом зацікавленим партнерам, що могло б не лише зміцнити колективну стійкість європейського регіону перед російськими інформаційними загрозами, а й підвищити міжнародний статус України як важливого актора європейської безпеки.

Третя рекомендація щодо європейської співпраці підкреслює необхідність активного залучення України до європейських дискусій про регулювання цифрового простору, кібербезпеку та захист прав людини онлайн, оскільки Україна як майбутній член Європейського Союзу має зацікавленість у формуванні європейських підходів у цих сферах відповідно до своїх інтересів та цінностей [25]. Україна має систематично вивчати європейське законодавство та політики у сфері цифрового управління, оцінювати їхню відповідність українським потребам та розпочинати процес гармонізації українського законодавства з європейськими стандартами вже до формального вступу до Європейського Союзу, що полегшить майбутню інтеграцію та дозволить Україні скористатися європейським досвідом для модернізації власного регуляторного середовища у цифровій сфері. Німеччина як провідна держава у формуванні європейської цифрової політики може надати Україні технічну допомогу у адаптації європейських стандартів, включно з консультаціями щодо імплементації Загального регламенту захисту даних, Директиви про мережеву та інформаційну безпеку та інших європейських нормативних актів, при цьому така співпраця буде взаємовигідною, оскільки Німеччина зможе краще зрозуміти

специфічні виклики, з якими стикаються держави на східному кордоні Європейського Союзу, і врахувати їх у подальшому розвитку європейської політики у сфері інформаційної безпеки.

Таким чином, перспективи використання німецького досвіду для зміцнення інформаційної безпеки України є значними та охоплюють інституційні, технологічні та комунікаційні аспекти розбудови української цифрової дипломатії, при цьому критично важливою є творча адаптація німецьких практик до специфічних умов українського контексту замість механічного копіювання, оскільки Україна стикається з більш інтенсивними та різноманітними інформаційними загрозами порівняно з Німеччиною та має інші ресурсні можливості і інституційні традиції. Інституційні рекомендації підкреслюють необхідність створення ефективних координаційних механізмів для синхронізації зусиль різних державних відомств, розбудови спеціалізованих структур цифрової дипломатії у Міністерстві закордонних справ та систематичного навчання українських дипломатів цифровим компетенціям та стратегічним комунікаціям, технологічні рекомендації акцентують важливість розвитку власних спроможностей моніторингу інформаційного простору та кіберзахисту критичної інфраструктури, а комунікаційні рекомендації наголошують на необхідності проактивних стратегічних комунікацій, диференціації повідомлень для різних аудиторій та розвитку партнерств з недержавними акторами для мультиплікації українського впливу. Поглиблення співпраці з європейськими партнерами, особливо з Німеччиною як провідною європейською державою та послідовним підтримувачем України, відкриває додаткові можливості для української інтеграції у європейські механізми забезпечення інформаційної безпеки та доступу до європейських ресурсів і експертизи, що могло б значно підвищити ефективність української протидії російській інформаційній агресії та зміцнити інформаційну стійкість українського суспільства в умовах тривалого гібридного протистояння.

Висновки до розділу 3

Аналіз цифрової дипломатії Німеччини як моделі для зміцнення інформаційної безпеки України, здійснений у третьому розділі дослідження, дозволяє сформулювати низку важливих висновків про ефективність німецького підходу, його вплив на формування європейського інформаційного порядку та можливості адаптації німецького досвіду для потреб України в умовах безпрецедентних інформаційних загроз внаслідок російської агресії та гібридної війни. Оцінка ефективності німецької цифрової дипломатії у забезпеченні інформаційної безпеки виявила складну картину часткових успіхів та постійних викликів, при цьому порівняльний аналіз з французькою, загальноєвропейською та американською моделями продемонстрував, що німецький підхід має певні унікальні характеристики, які відрізняють його від практик інших провідних акторів цифрової дипломатії та відображають специфічні німецькі традиції багатосторонності, прихильності верховенству права та етичним обмеженням у використанні цифрових технологій для впливу на інформаційний простір.

Німеччина досягла відчутних результатів у формуванні міжнародних норм відповідальної поведінки держав у кіберпросторі через активну участь у роботі Групи урядових експертів ООН та інших міжнародних форумах, розбудові європейських механізмів протидії дезінформації та кіберзагрозам через ініціювання та фінансову підтримку численних загальноєвропейських ініціатив, а також позиціонуванні себе як відповідального міжнародного актора у сфері цифрової політики, який пропонує альтернативу як американському ринковому підходу з мінімальним державним регулюванням, так і китайській моделі жорсткого державного контролю над інформаційним простором. Водночас німецька цифрова дипломатія стикається з численними викликами, включно з обмеженістю ресурсів порівняно з масштабами завдань протидії добре фінансованим дезінформаційним кампаніям авторитарних режимів, складністю швидкого реагування на інформаційні інциденти через бюрократичні процедури, асиметрією між демократичними обмеженнями німецького підходу та відсутністю подібних обмежень у противників, технологічною залежністю від іноземних цифрових платформ, а також необхідністю постійної адаптації до

швидких технологічних змін, що іноді випереджають здатність дипломатичних інституцій адаптуватися до нових форматів комунікації та цифрових платформ.

Вплив німецької цифрової дипломатії на європейський інформаційний порядок є значним та багатовимірним, оскільки Німеччина відіграє ключову роль у формуванні європейських політик у сфері протидії дезінформації, кібербезпеки, регулювання цифрових платформ та захисту прав людини в цифровому просторі через ініціювання законодавчих та політичних ініціатив, забезпечення фінансових та експертних ресурсів для їхньої реалізації, координацію позицій держав-членів Європейського Союзу та представлення європейської позиції у глобальних дискусіях про майбутнє цифрового управління. Німецький внесок у розвиток європейських механізмів протидії дезінформації включає політичну та фінансову підтримку Групи стратегічних комунікацій Європейського Союзу, ініціювання створення Європейської обсерваторії з цифрових медіа, просування Європейського плану дій з демократії та підтримку Європейського фонду для демократії, при цьому німецький досвід національного регулювання цифрових платформ через закон про покращення забезпечення правопорядку в соціальних мережах став важливим прецедентом для розробки загальноєвропейського Акту про цифрові послуги. Німеччина також відіграла провідну роль у розвитку європейської політики кібербезпеки через підтримку Директиви про мережеву та інформаційну безпеку, створення Європейського центру компетенції з кібербезпеки та просування ініціатив щодо європейської цифрової ідентичності, при цьому німецький підхід послідовно наголошує на необхідності поєднання захисту демократичних цінностей з підтримкою інновацій та уникнення як надмірного державного контролю, так і нерегульованого ринкового підходу до цифрового простору.

Перспективи використання німецького досвіду для зміцнення інформаційної безпеки України є значними, хоча вимагають творчої адаптації замість механічного копіювання через суттєві відмінності у контекстах, ресурсних можливостях та природі інформаційних загроз, з якими стикаються обидві держави. Інституційні рекомендації для України підкреслюють необхідність створення ефективного координаційного механізму на зразок

німецької Ради національної кібербезпеки для синхронізації зусиль різних державних відомств у сфері цифрової дипломатії та інформаційної безпеки, розбудови спеціалізованого підрозділу цифрової дипломатії у Міністерстві закордонних справ з достатніми ресурсами та повноваженнями для координації української присутності у глобальному цифровому просторі, а також систематичного навчання українських дипломатів цифровим компетенціям та стратегічним комунікаціям через створення спеціалізованих навчальних програм у Дипломатичній академії України або залучення до європейських навчальних ініціатив. Технологічні рекомендації акцентують важливість розвитку власних спроможностей моніторингу інформаційного простору для раннього виявлення дезінформаційних кампаній, зміцнення кіберзахисту критичної інфраструктури через централізовану координацію та обмін інформацією про загрози, а також інвестування у розвиток національних кадрів у сфері кібербезпеки через освітні програми та створення привабливих умов праці у державному секторі.

Комунікаційні рекомендації наголошують на необхідності переходу від виключно реактивного спростування російської дезінформації до проактивних стратегічних комунікацій через формування та систематичне просування переконливих наративів про Україну, диференціації комунікаційних стратегій для різних аудиторій з урахуванням специфіки різних цифрових платформ та культурних контекстів, розвитку партнерств з недержавними акторами для мультиплікації українських повідомлень, а також активнішого залучення української діаспори до цифрових комунікаційних зусиль як природних посередників між Україною та локальними аудиторіями у країнах проживання. Рекомендації щодо поглиблення європейської співпраці підкреслюють важливість максимального використання можливостей інтеграції у європейські механізми забезпечення інформаційної безпеки через формальні та неформальні канали, активнішого залучення до європейських ініціатив протидії російській дезінформації з використанням унікального українського досвіду протистояння російській інформаційній агресії, а також систематичної гармонізації українського законодавства з європейськими стандартами у сфері цифрового управління, при цьому Німеччина як провідна європейська держава та

послідовний підтримувач України може відіграти ключову роль у сприянні українській інтеграції через лобіювання українських інтересів у європейських інституціях та надання двосторонньої технічної допомоги.

Німецький досвід цифрової дипломатії демонструє, що ефективне забезпечення інформаційної безпеки вимагає не лише технологічних інвестицій та присутності у соціальних мережах, а й чіткого стратегічного бачення ролі інформаційного простору для національної безпеки, розвинутих інституційних механізмів координації між різними відомствами, підготовлених кадрів з відповідними компетенціями, а також готовності до постійного навчання та адаптації до динамічних змін цифрового середовища, при цьому найуспішніші аспекти німецької практики пов’язані саме з напрямами, де Німеччина могла опертися на європейську співпрацю та мультиплікувати свій вплив через багатосторонні механізми. Для України, яка стикається з більш інтенсивними та екзистенційними інформаційними загрозами порівняно з Німеччиною, адаптація німецького та європейського досвіду має поєднуватися з розвитком власних інноваційних підходів, що враховують специфіку української ситуації, включно з необхідністю балансування між ефективною протидією російській інформаційній агресії та збереженням демократичних цінностей і свобод, які Україна захищає у протистоянні з авторитарним агресором, при цьому поглиблення співпраці з Німеччиною та іншими європейськими партнерами відкриває для України доступ до ресурсів, експертизи та солідарності, необхідних для успішного протистояння інформаційним викликам та зміцнення інформаційної стійкості українського суспільства.

ВИСНОВКИ

Проведене дослідження цифрової дипломатії Німеччини як інструменту формування інформаційної безпеки дозволило здійснити комплексний аналіз теоретичних засад, інституційних механізмів та практичних інструментів німецького підходу до використання цифрових технологій у зовнішній поліітиці для забезпечення національної безпеки в умовах трансформації глобального комунікаційного середовища, а також оцінити можливості адаптації німецького досвіду для зміцнення інформаційної безпеки України. Логіка дослідження передбачала рух від теоретичного осмислення взаємозв'язку між цифровою дипломатією та інформаційною безпекою через емпіричний аналіз німецької практики до формулювання практичних рекомендацій для України, що дозволило забезпечити органічний зв'язок між концептуальними положеннями, аналітичними результатами та прикладними висновками роботи.

1. У результаті дослідження було з'ясовано концептуальні засади цифрової дипломатії та інформаційної безпеки у сучасній системі міжнародних відносин, що дозволило виявити багатовимірний характер обох феноменів та складність їхнього взаємозв'язку в умовах цифровізації міжнародних відносин. Цифрова дипломатія постає як результат конвергенції технологічного прогресу та еволюції дипломатичних практик, що створило якісно нову парадигму міждержавної комунікації, яка органічно поєднує традиційні інструменти зовнішньої політики з можливостями інформаційно-комунікаційних технологій для досягнення зовнішньополітичних цілей держави. Еволюція цифрової дипломатії демонструє поступовий перехід від односторонньої трансляції інформації через офіційні веб-сайти до діалогу з глобальними аудиторіями через соціальні мережі та використання передових технологій штучного інтелекту для таргетованого впливу на цільові аудиторії. Інформаційна безпека як відносно новий концепт у теорії та практиці міжнародних відносин характеризується багаторівневою структурою, що охоплює технічний, юридичний, організаційний та змістовий виміри захисту інформаційного простору від різноманітних загроз, при цьому інформаційна безпека тісно інтегрована в загальну систему національної безпеки держави через критичну залежність функціонування

державних і приватних структур від безперебійної роботи інформаційно-комунікаційних систем.

Теоретичне осмислення цифрової дипломатії як інструменту забезпечення інформаційної безпеки виявило необхідність мультипарадигмального підходу, оскільки різні теоретичні перспективи міжнародних відносин розкривають специфічні аспекти цього складного взаємозв'язку. Неореалістична парадигма акцентує конкурентний характер інформаційного простору та необхідність розвитку автономних національних спроможностей для забезпечення інформаційної безпеки, неоліберальстський підхід виявляє потенціал міжнародної кооперації та ролі інституцій у формуванні режимів співробітництва, конструктивізм привертає увагу до значення ідей та дискурсивних практик у конструюванні безпекового середовища, комунікативна теорія підкреслює потенціал раціонального дискурсу для досягнення консенсусу, а концепції інформаційної стійкості та стратегічних комунікацій пропонують операційні рамки для практичного використання цифрової дипломатії в цілях інформаційної безпеки. Комплементарне використання цих теоретичних підходів дозволяє уникнути однобічності в аналізі та врахувати різні аспекти складного взаємозв'язку між цифровою дипломатією та інформаційною безпекою, що створює міцне теоретичне підґрунтя для емпіричного дослідження конкретних національних практик.

2. Виявлення специфіки формування німецької цифрової дипломатії продемонструвало поетапний характер цього процесу протягом останніх двох десятиліть у відповідь на технологічні зміни та зростаючі інформаційні загрози. Німецький підхід еволюціонував від простої технічної модернізації комунікаційної інфраструктури до комплексного стратегічного бачення цифрової дипломатії як важливого інструменту забезпечення національної безпеки, при цьому каталізаторами цієї трансформації стали розголос про масове стеження американських спецслужб, російська агресія проти України з супутніми інформаційними операціями та численні спроби втручання у виборчі процеси західних демократій. Концептуалізація німецької цифрової дипломатії через поняття Digitale Außenpolitik та Cyber-Außenpolitik відображає

багатовимірний характер цього феномену, що охоплює як широкі питання цифрової трансформації зовнішньої політики, так і специфічні виклики кібербезпеки у міжнародних відносинах. Стратегічні пріоритети німецької цифрової дипломатії включають просування концепції відкритого та безпечного кіберпростору, зміцнення кіберстійкості Європейського Союзу, активну протидію дезінформації, забезпечення захисту прав людини в цифровому просторі та розвиток цифрової публічної дипломатії, при цьому німецький підхід тісно пов'язаний із загальноєвропейськими ініціативами, оскільки Німеччина розглядає Європейський Союз як критично важливу платформу для консолідації зусиль європейських держав у протистоянні глобальним викликам цифрової епохи.

3. Розкриття інституційної структури забезпечення цифрової дипломатії та інформаційної безпеки Німеччини виявило складну архітектуру з розподілом повноважень між численними державними відомствами та спеціалізованими агенціями, що відображає федеральний устрій Німеччини та традиційний німецький підхід до розподілу влади. Федеральне міністерство закордонних справ відіграє центральну координуючу роль у формуванні зовнішніх аспектів німецької політики у сфері цифрової дипломатії через спеціалізовані підрозділи стратегічних комунікацій та цифрової зовнішньої політики, Федеральне відомство з інформаційної безпеки забезпечує технічний захист урядових інформаційних систем та координацію національного реагування на кіберінциденти, Федеральна служба захисту конституції займається виявленням іноземного кібершпигунства та інформаційних операцій, Кіберкомандування Бундесверу розвиває військові кіберспроможності, а Інститут Гете просуває німецьку культуру у цифровому просторі як елемент м'якої сили. Ефективність цієї складної системи значною мірою залежить від якості міжвідомчої координації через Раду національної кібербезпеки та інші механізми узгодження дій різних державних структур, при цьому європейський та трансатлантичний виміри німецької інституційної архітектури відображають стратегічний вибір Німеччини на користь багатосторонності та колективних підходів до вирішення проблем цифрової епохи через активну участь у діяльності Європейського

Союзу, НАТО та міжнародних організацій.

4. Визначення практичних інструментів німецької цифрової дипломатії у сфері інформаційної безпеки продемонструвало комплексний підхід, який поєднує протидію дезінформації, кібердипломатію та активне використання цифрових платформ для досягнення зовнішньополітичних цілей. Німецький підхід до протидії дезінформації базується на моніторингу інформаційного простору для раннього виявлення дезінформаційних кампаній, оперативному спростуванні неправдивих наративів через офіційні канали комунікації, підтримці незалежних фактчекінгових організацій та медіаграмотності населення, а також міжнародній співпраці у виявленні скоординованих дезінформаційних кампаній, при цьому німецький уряд ретельно дотримується балансу між ефективною протидією дезінформації та збереженням свободи слова через підтримку плюралістичної екосистеми перевірки фактів замість створення централізованих урядових структур, що визначають істину. Кібердипломатія як специфічний напрям охоплює дипломатичні зусилля з формування міжнародних норм поведінки держав у кіберпросторі, координацію дипломатичних відповідей на кібератаки та просування застосування міжнародного права до кіберактивностей через активну участь у роботі міжнародних форумів та формування коаліцій держав-однодумців. Використання цифрових платформ та соціальних мереж здійснюється з урахуванням специфіки кожної платформи та особливостей її аудиторії, при цьому стратегія комунікації базується на принципах автентичності, діалогічності, візуальності контенту та регулярності присутності, а стратегічні наративи німецької цифрової дипломатії систематично транслюються через різноманітні канали та адаптуються до специфіки різних аудиторій для максимізації їхньої переконливості.

5. Встановлення характеру впливу німецької цифрової дипломатії на формування європейського інформаційного порядку продемонструвало, що Німеччина відіграє ключову роль у розробці та реалізації європейських політик у сфері протидії дезінформації, кібербезпеки, регулювання цифрових платформ та захисту прав людини в цифровому просторі. Німецький внесок включає

політичну та фінансову підтримку Групи стратегічних комунікацій Європейського Союзу, ініціювання створення Європейської обсерваторії з цифрових медіа, просування Європейського плану дій з демократії та підтримку Європейського фонду для демократії, при цьому німецький досвід національного регулювання цифрових платформ став важливим прецедентом для розробки загальноєвропейського законодавства. Німеччина також відіграла провідну роль у розвитку європейської політики кібербезпеки через підтримку Директиви про мережеву та інформаційну безпеку, створення Європейського центру компетенції з кібербезпеки та просування ініціатив щодо європейської цифрової ідентичності, координуючи позиції держав-членів у міжнародних переговорах про регулювання кіберпростору та забезпечуючи узгоджене просування європейських позицій. Європейські ініціативи, очолювані або активно підтримані Німеччиною, поступово формують унікальну європейську модель цифрового управління, яка стає альтернативою американському та китайському підходам і поширюється на інші регіони світу через механізм брюссельського ефекту, що підтверджує значний вплив Німеччини на глобальний інформаційний порядок через європейські механізми.

6. Обґрунтування рекомендацій щодо використання німецького досвіду для зміцнення інформаційної безпеки України виявило значні можливості адаптації німецьких практик при обов’язковому врахуванні специфіки українського контексту, включно з більш інтенсивними інформаційними загрозами та обмеженішими ресурсами порівняно з Німеччиною. Інституційні рекомендації підкреслюють необхідність створення ефективного координаційного механізму для синхронізації зусиль різних державних відомств у сфері цифрової дипломатії та інформаційної безпеки, розбудови спеціалізованого підрозділу цифрової дипломатії у Міністерстві закордонних справ України з достатніми ресурсами та повноваженнями, а також систематичного навчання українських дипломатів цифровим компетенціям та стратегічним комунікаціям через спеціалізовані програми або залучення до європейських навчальних ініціатив. Технологічні рекомендації акцентують важливість розвитку власних спроможностей моніторингу інформаційного

простору для раннього виявлення дезінформаційних кампаній, зміцнення кіберзахисту критичної інфраструктури через централізовану координацію та інвестування у розвиток національних кадрів у сфері кібербезпеки через освітні програми та створення привабливих умов праці у державному секторі. Комунікаційні рекомендації наголошують на необхідності переходу від виключно реактивного спростування російської дезінформації до проактивних стратегічних комунікацій через формування переконливих наративів про Україну, диференціації комунікаційних стратегій для різних аудиторій, розвитку партнерств з недержавними акторами та активнішого залучення української діаспори до цифрових комунікаційних зусиль. Рекомендації щодо поглиблення європейської співпраці підкреслюють важливість максимального використання можливостей інтеграції у європейські механізми забезпечення інформаційної безпеки, активнішого залучення до європейських ініціатив протидії російській дезінформації та систематичної гармонізації українського законодавства з європейськими стандартами у сфері цифрового управління, при цьому Німеччина може відіграти ключову роль у сприянні українській інтеграції через лобіювання українських інтересів у європейських інституціях та надання двосторонньої технічної допомоги.

Таким чином, проведене дослідження цифрової дипломатії Німеччини як інструменту формування інформаційної безпеки підтвердило комплексний характер німецького підходу, який поєднує розвиток технічних спроможностей з інституційною розбудовою, стратегічними комунікаціями та міжнародною співпрацею, при цьому німецький досвід демонструє можливості середніх держав мультиплікувати свій вплив у глобальному інформаційному просторі через регіональну інтеграцію та колективні дії у рамках Європейського Союзу. Для України адаптація німецького досвіду має поєднуватися з розвитком власних інноваційних підходів, що враховують специфіку українського контексту та інтенсивність інформаційних загроз внаслідок російської агресії, при цьому поглиблення співпраці з Німеччиною та іншими європейськими партнерами відкриває для України доступ до ресурсів, експертизи та солідарності, необхідних для успішного протистояння інформаційним викликам

та зміцнення інформаційної стійкості українського суспільства у тривалій перспективі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балабанов К. В., Трофименко М. В. «Публічна дипломатія» як відповідь на виклики сучасності. *Україна дипломатична*. 2020. Вип. 14. С. 989–1021.

2. Баловсяк Н. В. Інформаційна безпека держави. Київ: Ліра-К, 2021. 320 с.

3. Баранік Р. В., Бабенко В. М., Рижов Д. А. Кібербезпека і управління інформаційними ресурсами: навчальний посібник. Запоріжжя: ЗНУ, 2025. 156 с.

4. Баровська А. Цифрова дипломатія України: виклики та можливості. *Зовнішні справи.* 2020. № 7. С. 12–16.

5. Бобало Ю. Я., Горбатий І. В., Schrijver М. М. Інформаційна безпека: навчальний посібник. Львів: Видавництво Львівської політехніки, 2020. 580 с.

6. Братута О. Публічна дипломатія в умовах гібридної агресії РФ: виклики для інформаційної безпеки України. *Публічна дипломатія.* 2023. Вип. 6. С. 45–58.

7. Висоцький О. Ю. Публічна дипломатія: конспект лекцій. Ч. І. Дніпро: СПД «Охотнік», 2020. 56 с.

8. Висоцький О. Ю. Публічна дипломатія: конспект лекцій. Ч. ІІ. Дніпро: СПД «Охотнік», 2020. 48 с.

9. Горбулін В., Додонов О., Ланде Д. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. Київ: Інтертехнологія, 2020. 278 с.

10. Гур'єв В. І., Мехед Д. Б., Ткач Ю. М., Шаронова О. М. Інформаційна безпека держави: навчальний посібник. Ніжин: Видавництво «Орхідея», 2020. 166 с.

11. Державно-приватне партнерство у сфері кібербезпеки: досвід Німеччини: аналітична доповідь. Київ: Національний інститут стратегічних досліджень, 2020. 52 с.

12. Дубов Д. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. *Стратегічні пріоритети.* 2021. № 4. С. 9–23.

13. Єфремова Т. О., Наумова М. Г., Мішанчук О. В. Особливості використання цифрової дипломатії в діяльності МЗС України. *LAIS / Law:*

Artificial Intelligence & Society. 2023. № 4. С. 78–89.

14. Звоздецька О. Інституційні механізми протидії дезінформації в ЄС: проблеми та здобутки. Медіафорум: аналітика, прогнози, інформаційний менеджмент. 2022. Т. 10. С. 107–122.

15. Звоздецька О. Кібербезпека ЄС в умовах посилення кіберзагроз в сучасному глобалізованому світі. Медіафорум: аналітика, прогнози, інформаційний менеджмент. 2020. Т. 7. С. 27–46.

16. Інформаційна та кібербезпека: підручник / за ред. В. Л. Бурячка. Київ: Державний університет телекомунікацій, 2020. 346 с.

17. Камінська Н. Інформаційна безпека України в умовах гібридної війни. *Науковий вісник Національної академії внутрішніх справ.* 2021. № 2. С. 234–245.

18. Ковальчук А. Ю., Чернявська Б. В. Європейський досвід протидії дезінформаційним впливам. *ScienceRise: Juridical Science.* 2024. № 2 (28). С. 50–54.

19. Кушнір В. Публічна дипломатія в умовах інформаційного суспільства. *Міжнародні відносини: теоретико-практичні аспекти.* 2022. Вип. 4. С. 156–168.

20. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія. Житомир: Видавництво ЖВІ, 2022. 248 с.

21. Ліпкан В. Національна безпека України. Київ: КНТ, 2020. 576 с.

22. Марченко В. В. Забезпечення інформаційної безпеки в умовах воєнного стану: сучасні виклики та правові механізми. *Юридичний науковий електронний журнал.* 2025. № 1. С. 234–237.

23. Мірошниченко Т. Цифрова дипломатія як сучасний комунікаційний інструмент міжнародних відносин. *Грані.* 2021. Т. 24, № 5. С. 56–64.

24. Почепцов Г. Сучасні інформаційні війни. Київ: Видавничий дім «Києво-Могилянська академія», 2024. 497 с.

25. Про Стратегію кібербезпеки України: Указ Президента України від 14 березня 2016 року № 96/2016. *Офіційний вісник України.* 2022. № 23. Ст. 899.

26. Публічна дипломатія: навчальний посібник / за заг. ред. І. Матяш. Київ: МЗС України; Національний університет «Острозька академія»; Наукове товариство історії дипломатії та міжнародних відносин, 2021. 224 с.

27. Руднєва А. О., Мальована Ю. Г. Цифрова дипломатія у формуванні системи національної безпеки України в умовах війни з РФ. *Регіональні студії.* 2023. № 34. С. 111–115.

28. Санжарова Г. Ф., Мацелик М. О., Санжаров В. А. Еволюція стратегії кібербезпеки Німеччини протягом останніх трьох десятиліть: інституційний та правничий виміри. Наукові тренди постіндустріального суспільства: матеріали IV Міжнародної наукової конференції. Вінниця: Європейська наукова платформа, 2023. С. 71–73.

29. Свідлер Д. В. Роль цифрової дипломатії в сучасній зовнішній політиці Німеччини: бакалаврська робота. Київ: Київський столичний університет імені Бориса Грінченка, 2025. 58 с.

30. Сегеда О. О. Цифрова дипломатія України як елемент нової публічної дипломатії. *Політикус.* 2020. № 3. С. 139–148.

31. Стратегія публічної дипломатії Міністерства закордонних справ України на 2021–2025 роки. Київ: МЗС України, 2021. 28 с.

32. Тимошенко О. Цифрова дипломатія як інструмент зовнішньої політики сучасних держав. *Актуальні проблеми міжнародних відносин.* 2021. Вип. 147. С. 89–102.

33. Титова Н. М., Молчанова Т. В., Бреславський А. Інформаційна безпека та кібербезпека держави: навчальний посібник. Київ: Видавництво Ліра-К, 2020. 304 с.

34. Цифрова дипломатія України: синергія реального і віртуального: матеріали міжнародної науково-практичної конференції (Львів, 24 листопада 2023 р.). Львів: ЛНУ імені Івана Франка, 2023. 186 с.

35. Ціватий В. Г. Феномен цифрової дипломатії в міжнародних відносинах і світовій політиці XXI століття: поліцентричний дискурс культурних і креативних індустрій. *Культурологічний альманах.* 2022. № 2. С. 40–49.

36. Шевчук О. Європейська інтеграція України: безпековий вимір. Київ:

НИСД, 2021. 196 с.

37. Bayer J., Bitiukova N., Bárd P. et al. Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. Brussels: European Parliament, 2020. 108 p.

38. Bendiek A., Römer M. Cybersicherheitspolitik in der EU: Akteure, Instrumente und Strategien. Berlin: Stiftung Wissenschaft und Politik, 2021. 32 S.

39. Bjola C., Cassidy J. Understanding digital diplomacy. *Digital Diplomacy: Theory and Practice* / ed. by C. Bjola, M. Holmes. London: Routledge, 2021. P. 1–20.

40. Bjola C., Holmes M. Digital Diplomacy: Theory and Practice. London: Routledge, 2021. 328 p.

41. Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford: Oxford University Press, 2020. 424 p.

42. Brattberg E., Maier T. Russian Election Interference: Europe's Counter to Fake News and Disinformation. Washington: Carnegie Endowment for International Peace, 2022. 36 p.

43. Brattberg E., Maier T. Russian Election Interference: Europe's Counter to Fake News and Disinformation. Washington: Carnegie Endowment for International Peace, 2023. 36 p.

44. Bundesamt für Verfassungsschutz. Verfassungsschutzbericht 2022. Köln: Bundesministerium des Innern und für Heimat, 2023. 418 S.

45. Deibert R. J. Reset: Reclaiming the Internet for Civil Society. Toronto: House of Anansi Press, 2020. 304 p.

46. European Commission. European Democracy Action Plan. Brussels: European Commission, 2020. 24 p.

47. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023. Luxembourg: Publications Office of the European Union, 2023. 156 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

48. Giles K. Handbook of Russian Information Warfare. Rome: NATO Defense College, 2022. 92 p.

49. Goff P. M. Cultural Diplomacy. The Oxford Handbook of Modern Diplomacy / ed. by A. F. Cooper, J. Heine, R. Thakur. Oxford: Oxford University

Press, 2021. P. 419–435.

50. Hanson F. Revolution @State: The Spread of eDiplomacy. Sydney: Lowy Institute for International Policy, 2022. 68 p.

51. Herpig S., Reinhold T. Germany's Cybersecurity Strategy: More Coherence in Sight? Berlin: Stiftung Neue Verantwortung, 2020. 28 p.

52. Hocking B., Melissen J. Diplomacy in the Digital Age. Clingendael: Netherlands Institute of International Relations, 2022. 112 p.

53. Horbulin V., Lytvynenko O. Cybersecurity of Ukraine: Analytical Report. Kyiv: National Institute for Strategic Studies, 2020. 144 p.

54. Huijgh E. Public Diplomacy in the Digital Age: France's Approach. *The Hague Journal of Diplomacy.* 2021. Vol. 11, №. 1. P. 83–104.

55. Kampf R., Ma№r I., Segev E. Digital diplomacy 2.0? A cross-national comparison of public engagement in Facebook and Twitter. *The Hague Journal of Diplomacy.* 2015. Vol. 10, №. 4. P. 331–362.

56. Käsehage N. Contestations of Liberal Order: The West in Crisis? Cambridge: Cambridge Scholars Publishing, 2020. 267 p.

57. Klimburg A. The Darkening Web: The War for Cyberspace. New York: Penguin Press, 2021. 368 p.

58. Lobato R., Meese J. Kittler №w: Current Perspectives in Kittler Studies. Cambridge: Polity Press, 2022. 256 p.

59. Ma№r I. The Digitalization of Public Diplomacy. Cham: Palgrave Macmillan, 2023. 402 p.

60. Ma№r I. The Digitalization of Public Diplomacy. Cham: Palgrave Macmillan, 2022. 402 p.

61. Marsden C. Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace. Cambridge: Cambridge University Press, 2022. 338 p.

62. Mearsheimer J. J. The Tragedy of Great Power Politics. New York: W.W. №rton & Company, 2020. 555 p.

63. Nye J. S. Cyber Power. Cambridge: Harvard Kennedy School Belfer Center for Science and International Relations, 2022. 34 p.

64. Pohle J., Thiel T. Digital sovereignty. *Internet Policy Review.* 2020. Vol. 9, №. 4. P. 1–19.

65. Rid T. Cyber War Will №t Take Place. Oxford: Oxford University Press, 2023. 248 p.

66. Sandre A. Digital Diplomacy: Conversations on In№vation in Foreign Policy. Lanham: Rowman & Littlefield, 2025. 184 p.

67. Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2022. 598 p.

68. Seib P. Real-Time Diplomacy: Politics and Power in the Social Media Era. New York: Palgrave Macmillan, 2022. 256 p.

69. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to K№w. Oxford: Oxford University Press, 2024. 320 p.

70. Tikk E., Kerttunen M. Parabasis: Cyber-diplomacy in Stalemate. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020. 48 p.

71. Tikk E., Kerttunen M. The Alleged Demise of the UN GGE: An Autopsy and Eulogy. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2021. 24 p.

72. Westcott N. Digital diplomacy: The impact of the internet on international relations. *Research Report. Oxford Internet Institute,* 2020. URL: https://www.oii.ox.ac.uk/research/digital-diplomacy/

73. Zaharna R. S., Arsenault A., Fisher A. Relational, Networked and Collaborative Approaches to Public Diplomacy: The Connective Mindshift. New York: Routledge, 2023. 312 p.

АНОТАЦІЯ

Гадючко Т. Є. Цифрова дипломатія Німеччини як інструмент формування інформаційної безпеки (магістерська робота). Харків: Харківський національний університет імені В. Н. Каразіна, 2025. 110 с. (рукопис).

Мета дослідження полягає у з'ясуванні ролі цифрової дипломатії Німеччини як інструменту забезпечення інформаційної безпеки та обґрунтуванні напрямів адаптації німецького досвіду для зміцнення інформаційної стійкості України.

Об'єктом дослідження є цифрова дипломатія як інструмент зовнішньої політики держав у сучасній системі міжнародних відносин.

Предметом дослідження виступає цифрова дипломатія Німеччини у її взаємозв'язку з формуванням інформаційної безпеки держави та європейського інформаційного порядку.

У першому розділі представлено теоретичні засади цифрової дипломатії та інформаційної безпеки. Розглянуто поняття та еволюцію цифрової дипломатії, функціональне призначення цифрових інструментів у зовнішній політиці, ключові теоретичні підходи до аналізу цифрової дипломатії як чинника інформаційної безпеки. Окрему увагу приділено трактуванню інформаційної безпеки у міжнародних відносинах, структурі інформаційних загроз, трансформації глобального інформаційного простору та ролі держав у забезпеченні стійкості цифрових комунікацій.

У другому розділі досліджено стратегію та інституційне забезпечення цифрової дипломатії Німеччини. Проаналізовано формування цифрової дипломатії, компетенції Федерального міністерства закордонних справ та спеціалізованих установ, а також інструменти цифрової комунікації, що застосовуються для протидії дезінформації, забезпечення захисту персональних даних і формування позитивного міжнародного іміджу. Оцінено взаємодію державних структур з міжнародними організаціями у сфері кібербезпеки та цифрової політики.

У третьому розділі окреслено можливості використання німецького досвіду для України. Визначено шляхи адаптації цифрових механізмів для посилення української інформаційної стійкості, розширення стратегічних комунікацій, протидії дезінформаційним кампаніям та підвищення рівня кіберзахисту державних структур. Сформульовано рекомендації щодо гармонізації української цифрової політики із європейськими стандартами інформаційної безпеки та вдосконалення міжвідомчої координації у сфері цифрової дипломатії.

Ключові слова: безпека, дезінформація, дипломатія, інформаційний простір, кібербезпека, комунікація, стратегічні комунікації, цифрова дипломатія.

ANNOTATION

Hadiuchko T. Ye. Germany's Digital Diplomacy as a Tool for Shaping Information Security (Master's thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 110 p. (manuscript).

The aim of the study is to clarify the role of Germany's digital diplomacy as a tool for ensuring information security and to substantiate the directions for adapting the German experience to strengthen Ukraine's information resilience.

The object of the study is digital diplomacy as an instrument of states' foreign policy in the contemporary system of international relations. The subject of the study is Germany's digital diplomacy in its connection with the formation of state information security and the European information order.

The first section presents the theoretical foundations of digital diplomacy and information security. It examines the concept and evolution of digital diplomacy, the functional purpose of digital tools in foreign policy, and key theoretical approaches to analysing digital diplomacy as a factor of information security. Special attention is paid to interpreting information security in international relations, the structure of information threats, the transformation of the global information space, and the role of states in ensuring the resilience of digital communications.

The second section examines the strategy and institutional framework of Germany's digital diplomacy. It analyses the development of digital diplomacy, the competences of the Federal Foreign Office and specialised agencies, as well as digital communication tools used to counter disinformation, protect personal data, and build a positive international image. Interaction between state institutions and international organisations in the field of cybersecurity and digital policy is assessed.

The third section outlines the possibilities of applying the German experience in Ukraine. It identifies ways to adapt digital mechanisms to strengthen Ukrainian information resilience, expand strategic communications, counter disinformation campaigns, and increase the level of cybersecurity of state structures. Recommendations are formulated regarding the harmonisation of Ukrainian digital policy with European information security standards and the improvement of interagency coordination in the field of digital diplomacy.

Keywords: communication, cybersecurity, digital diplomacy, disinformation, information security, information space, security, strategic communications.

ВІДГУК

на кваліфікаційну роботу магістра
студентки 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Гадючко Тетяни Євгенівни
на тему: **«Цифрова дипломатія Німеччини як інструмент формування інформаційної безпеки»**

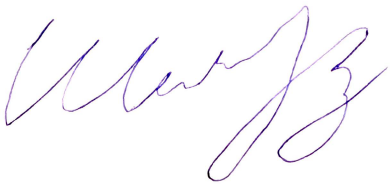
Магістерська кваліфікаційна робота Гадючко Тетяни Євгенівни присвячена актуальній та науково значущій темі, яка органічно поєднує питання цифрової дипломатії, інформаційної безпеки та зовнішньої політики сучасних держав. Зростання ролі цифрових інструментів у міжнародних відносинах, а також посилення інформаційних загроз у глобальному середовищі зумовлюють важливість дослідження, що було виконано здобувачкою. Вибір німецького досвіду як предмета аналізу є обґрунтованим, адже саме Німеччина виступає одним із лідерів у формуванні європейських стандартів інформаційної стійкості та цифрової дипломатії.

Робота вирізняється логічною побудовою, послідовністю викладення та належною структуризацією матеріалу. Авторка всебічно розкрила теоретичні засади цифрової дипломатії та інформаційної безпеки, продемонструвавши хороше володіння науковим апаратом і здатність системно працювати з понятійно-категоріальним інструментарієм. Значна увага приділена аналізу еволюції цифрової дипломатії та підходів провідних дослідників, що підсилює теоретичну цінність роботи. У другому розділі ґрунтовно розглянуто стратегію та інституційне забезпечення цифрової дипломатії Німеччини, проаналізовано діяльність ключових структур, нормативно-правові рамки, а також практичні механізми реагування на інформаційні загрози. У третьому розділі вдалим є акцент на можливостях адаптації німецького досвіду для України: авторка запропонувала низку конкретних рекомендацій, що свідчать про її здатність до практичного узагальнення і стратегічного бачення проблеми.

Суттєвою перевагою роботи є широке і різнопланове джерельне підґрунтя: використано монографії, наукові статті, офіційні документи Німеччини та Європейського Союзу, аналітику міжнародних організацій, сучасні звіти з кібербезпеки та матеріали стратегічних комунікацій. Це свідчить про високу культуру дослідження, уміння працювати з якісними джерелами та здійснювати комплексний аналіз проблеми. Студентка продемонструвала глибоке розуміння міжнародно-політичного контексту та здатність співвідносити окремі концепції з реальними практиками державної політики.

Разом із тим окремі аспекти роботи могли би бути висвітлені більш деталізовано. Зокрема, у практичній частині дослідження доцільно було б глибше проаналізувати конкретні цифрові кейси Німеччини у сфері протидії дезінформації або розширити порівняльний аналіз із підходами інших європейських держав. Однак зазначені зауваження не мають принципового характеру та не применшують загальної якості проведеного дослідження.

Магістерська робота Гадючко Тетяни Євгенівни виконана на високому академічному рівні, відзначається самостійністю суджень, аналітичністю та практичною спрямованістю висновків. Вона відповідає встановленим вимогам до кваліфікаційних робіт другого (магістерського) рівня вищої освіти й може бути рекомендована до захисту перед екзаменаційною комісією.

Науковий керівник:
доктор політичних наук,
професор, професор
кафедри міжнародних відносин  **Шамраєва В.М.**

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студентки 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Гадючко Тетяни Євгенівни
на тему: **«Цифрова дипломатія Німеччини як інструмент формування інформаційної безпеки»**

1. Актуальність теми

Дослідження цифрової дипломатії Німеччини є важливим у контексті зростаючих інформаційних загроз, трансформації міжнародної безпеки та розвитку інструментів державної протидії дезінформації. У сучасних умовах Німеччина відіграє помітну роль у формуванні європейських стандартів інформаційної безпеки, а її підходи до цифрової дипломатії суттєво впливають на спільну політику ЄС. Тому тема роботи відзначається високою актуальністю, оскільки поєднує аналіз концептуальних засад інформаційної безпеки та практичні механізми цифрової взаємодії держави із зовнішнім середовищем.

2. Характеристика якості виконання розділів роботи

Перший розділ присвячено теоретичним основам цифрової дипломатії та інформаційної безпеки. Автор послідовно розглядає ключові поняття, простежує еволюцію цифрових комунікацій у міжнародних відносинах, а також подає узагальнений огляд наукових підходів до аналізу цифрової дипломатії як інструменту інформаційної безпеки. Розділ вирізняється логічною структурою та комплексністю опрацювання теоретичного матеріалу.

Другий розділ аналізує становлення цифрової дипломатії Німеччини та розкриває інституційні механізми, які забезпечують її реалізацію. Особлива увага приділяється функціям федеральних відомств, відповідальних за інформаційну політику, а також особливостям державних програм цифрової трансформації. Авторка коректно структурує матеріал і демонструє розуміння внутрішньополітичних передумов формування німецької цифрової дипломатії.

У третьому розділі розглянуто прикладні інструменти цифрової дипломатії Німеччини та їхній вплив на інформаційну безпеку. Автор аналізує практичні механізми реагування на виклики, пов'язані з дезінформацією, кіберзагрозами та цифровою комунікацією державних інституцій. Важливою перевагою розділу є увага до результативності окремих рішень і можливостей їх адаптації для українського контексту.

3. Ступінь обґрунтованості висновків роботи

Висновки роботи логічно випливають із проведеного аналізу та відповідають сформульованим завданням, які визначені у завданні на КРМ . Автор узагальнює ключові результати, робить коректні висновки щодо ролі німецької цифрової дипломатії у забезпеченні інформаційної безпеки та окреслює можливості використання німецького досвіду Україною. Обґрунтованість висновків підтверджується достатнім фактичним матеріалом і послідовністю викладу.

4. Позитивні сторони роботи

Серед позитивних характеристик варто відзначити структурованість дослідження, чітке розмежування теоретичних і практичних аспектів, а також актуальність використаної літератури. Автор демонструє вміння працювати з офіційними документами Німеччини та ЄС, вдалим чином поєднує концептуальний аналіз із описом конкретних інституцій та цифрових інструментів. Крім того, робота містить елементи порівняльного аналізу та пропозиції щодо застосування досвіду Німеччини для зміцнення української інформаційної безпеки, що підсилює її практичну цінність.

5. Недоліки роботи

До недоліків можна віднести недостатній аналіз складнощів, пов'язаних із координацією цифрової політики між федеральними та земельними рівнями влади у Німеччині. Також було б доцільно приділити більше уваги оцінці ефективності конкретних цифрових ініціатив на основі емпіричних даних. Проте зазначені аспекти не знижують загальної якості дослідження і не впливають на його цілісність.

6. Загальна оцінка кваліфікаційної роботи

Кваліфікаційна робота Гадючко Тетяни Євгенівни відповідає вимогам до магістерських досліджень за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Робота виконана на належному академічному рівні, має логічну структуру, аналітичну глибину і практичну спрямованість. Результати дослідження можуть бути використані для подальшого вивчення інструментів цифрової дипломатії та формування національної інформаційної безпеки. Робота заслуговує на позитивну оцінку.

Рецензент:
д.держ.упр., професор
завідувач кафедри публічної політики
ННІ ««Інститут державного управління»
Харківський національний університет
імені В. Н. Каразіна _____ В. Б. Дзюндзюк