

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

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «Політика ЄС у сфері цифрової дипломатії»

Виконав:

студент 2 курсу, групи УМІБ-61

другого (магістерського) рівня вищої освіти,
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»

ОПП «Міжнародна інформаційна безпека»

Зайко Ігор Дмитрович

(прізвище, ім'я по батькові)



Керівник:

д.держ.упр, професор Солових В.П.

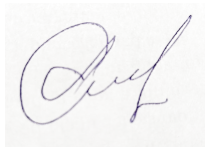
(науковий ступінь, вчене звання, прізвище, ім'я по батькові)



Рецензент:

д.і.н., професор Лиман Сергій Іванович

(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

Наталія ВІННИКОВА

ініціали, прізвище

«2» червня 2025 року

(зі змінами від 10.09.2025, 06.10.2025)

ЗАВДАННЯ

на кваліфікаційну роботу магістра

Зайка Ігоря Дмитровича

(прізвище, ім'я та по батькові)

1. Тема роботи «Політика ЄС у сфері цифрової дипломатії»

керівник роботи Солових Віталій Павлович, д.держ.упр., 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:

визначити зміст, сутність та еволюцію поняття цифрової дипломатії у системі сучасних міжнародних відносин; – описати теоретико-методологічні підходи до аналізу феномену цифрової дипломатії та їхніх евристичних можливостей; оцінити нормативно-правові та концептуальні основи політики ЄС у сфері цифрової дипломатії; з'ясувати інституційну архітектуру формування та реалізації цифрової дипломатії Європейського Союзу; охарактеризувати інструменти, програми та механізми практичної реалізації політики ЄС у сфері цифрової дипломатії у глобальному та регіональному вимірах; обґрунтувати пропозицій щодо вдосконалення політики цифрової дипломатії Європейського Союзу та оптимізації шляхів інтеграції України у європейський цифровий простір..

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	24.11.2025-28.11.2025
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)

Ігор ЗАЙКО

(ініціали, прізвище)

Керівник роботи



(підпис)

Віталій СОЛОВИХ

(ініціали, прізвище)

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЦИФРОВОЇ ДИПЛОМАТІЇ В ЄВРОПЕЙСЬКОМУ СОЮЗІ.....	9
1.1. Поняття та сутність цифрової дипломатії в системі сучасних міжнародних відносин.....	9
1.2. Теоретичні підходи до розкриття змісту цифрової дипломатії.....	15
1.3. Нормативно-правові та концептуальні основи цифрової дипломатії Європейського Союзу	23
Висновки до розділу 1	34
РОЗДІЛ 2. ІНСТИТУЦІЙНО-АНАЛІТИЧНИЙ ВИМІР ПОЛІТИКИ ЄС У СФЕРІ ЦИФРОВОЇ ДИПЛОМАТІЇ	38
2.1. Суб'єкти формування цифрової дипломатії Європейського Союзу	38
2.2. Інструменти реалізації цифрової дипломатії ЄС	45
2.3. Цифрова дипломатія ЄС у глобальному та регіональному вимірах.....	53
Висновки до розділу 2	64
РОЗДІЛ 3. ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОЇ ДИПЛОМАТІЇ ЄС ТА ЇЇ СПІВПРАЦЯ З УКРАЇНОЮ	67
3.1. Цифрова дипломатія як складова зовнішньої політики розширення ЄС.	67
3.2. Напрями цифрової взаємодії ЄС та України	76
3.3. Пропозиції щодо вдосконалення політики цифрової дипломатії ЄС та інтеграції України	86
Висновки до розділу 3	95
ВИСНОВКИ.....	98
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	102

ВСТУП

Актуальність роботи. У сучасних умовах цифровізації міжнародних комунікацій та трансформації глобального інформаційного простору політика Європейського Союзу у сфері цифрової дипломатії набуває особливого значення як механізм реалізації стратегічних інтересів Співки у глобальному кіберпросторі та інструмент формування міжнародного порядку, заснованого на демократичних цінностях, верховенстві права та захисті прав людини у цифровому середовищі. Стрімкий розвиток інформаційно-комунікаційних технологій, поширення соціальних мереж та цифровізація суспільних процесів радикально змінили характер взаємодії між державами, міжнародними організаціями та недержавними акторами, створивши принципово нові можливості для здійснення дипломатичної діяльності, водночас породивши безпрецедентні виклики, пов'язані з кіберзагрозами, дезінформацією, маніпулюванням громадською думкою та підризом демократичних інституцій через цифрові канали впливу. Повномасштабне російське вторгнення в Україну у лютому 2022 року драматично оголило критичну важливість цифрового виміру сучасних конфліктів, де кібератаки на критичну інфраструктуру, масштабні дезінформаційні кампанії та інформаційне протиборство стали невід'ємними компонентами гібридної війни, що актуалізувало питання цифрової стійкості, кібербезпеки та стратегічних комунікацій як критичних факторів національної безпеки та державного суверенітету. У цьому контексті цифрова дипломатія Європейського Союзу трансформується з інструменту публічної комунікації та наративного впливу у комплексну систему практик, механізмів та програм, що охоплює широкий спектр активностей від протидії дезінформації та підтримки кібербезпеки партнерських країн до просування європейських регуляторних стандартів та формування глобальних норм цифрового управління, що відповідають цінностям демократії, прав людини та відкритого суспільства.

Ступінь наукової розробленості проблеми цифрової дипломатії свідчить про зростаючу увагу дослідників міжнародних відносин до цього феномену, що відображається у роботах провідних зарубіжних науковців, зокрема Корнеліу Бйолі та Маркуса Холмса, які концептуалізували цифрову дипломатію як

використання цифрових технологій для досягнення дипломатичних цілей, Ітая Менора, що проаналізував трансформацію публічної дипломатії під впливом цифровізації, Джеймса Першінга, який розмежував поняття електронної та цифрової дипломатії, та інших дослідників, що внесли значний вклад у теоретичне осмислення цього явища. Водночас у вітчизняній науці про міжнародні відносини питання цифрової дипломатії також привертають дедалі більшу увагу, що засвідчують праці українських дослідників, присвячені різним аспектам цифровізації зовнішньої політики, стратегічним комунікаціям, кібербезпеці та інформаційному протиборству, проте комплексний аналіз політики Європейського Союзу у сфері цифрової дипломатії як цілісної системи з власною інституційною архітектурою, нормативно-правовою базою, специфічними інструментами реалізації та унікальною моделлю, що відрізняється від підходів національних держав, залишається недостатньо дослідженим у вітчизняній науковій літературі. Особливої уваги потребує аналіз досвіду та перспектив цифрової взаємодії між ЄС та Україною в контексті європейської інтеграції України та її адаптації до стандартів цифрової дипломатії Європейського Союзу, що становить значну прогалину у існуючих дослідженнях та обґрунтовує необхідність системного наукового осмислення цієї проблематики.

Метою магістерської роботи є визначення концептуальних засад, інституційних особливостей та практичних механізмів політики Європейського Союзу у сфері цифрової дипломатії як складової його зовнішньополітичної діяльності.

Досягнення поставленої мети передбачає розв'язання таких **завдань дослідження**:

- визначити зміст, сутність та еволюцію поняття цифрової дипломатії у системі сучасних міжнародних відносин;
- окреслити теоретичні підходи до аналізу феномену цифрової дипломатії та їхніх евристичних можливостей;
- з'ясувати інституційну архітектуру формування та реалізації цифрової дипломатії Європейського Союзу;

– охарактеризувати інструменти, програми та механізми практичної реалізації політики ЄС у сфері цифрової дипломатії у глобальному та регіональному вимірах;

– обґрунтувати пропозиції щодо вдосконалення політики цифрової дипломатії Європейського Союзу та оптимізації шляхів інтеграції України у європейський цифровий простір.

Об’єктом дослідження є політика Європейського Союзу у сфері міжнародних комунікацій та зовнішньополітичних відносин у цифрову епоху.

Предмет дослідження – зміст, принципи, інституційні механізми та практичні інструменти реалізації політики ЄС у сфері цифрової дипломатії.

Методи дослідження є системний підхід, що дозволяє розглядати цифрову дипломатію ЄС як цілісну систему взаємопов’язаних елементів, включаючи інституційні структури, нормативно-правові рамки, інструменти реалізації та механізми координації між різними акторами, інституційний підхід, що фокусується на ролі європейських інституцій у формуванні та імплементації політики цифрової дипломатії, а також на процесах інституціоналізації нових практик та механізмів цифрової взаємодії, конструктивістський підхід, що розкриває процеси конструювання значень, наративів та ідентичностей через цифрову дипломатичну комунікацію, неоліберальний інституціоналізм, що пояснює роль міжнародних інституцій, норм та режимів у структуруванні цифрової дипломатичної практики, та компаративний підхід, що дозволяє зіставляти різні національні та регіональні моделі цифрової дипломатії для виявлення специфіки європейського підходу. Міждисциплінарний характер дослідження зумовлює необхідність інтеграції концептуальних інструментів теорії міжнародних відносин, теорії комунікації, медіа-студій, досліджень науки і технологій та політичного аналізу для комплексного осмислення багатогранного феномену цифрової дипломатії, що функціонує одночасно як комунікативна практика, регуляторна політика, технологічна система та геополітична стратегія.

Інформаційну базу дослідження становлять офіційні документи Європейського Союзу, включаючи стратегії, регламенти, директиви, рішення

Ради ЄС та Європейського Парламенту, комунікації Європейської Комісії, звіти Європейської служби зовнішніх дій, що визначають концептуальні засади, нормативно-правову базу та практичні механізми реалізації політики ЄС у цифровій сфері, зокрема Глобальна стратегія ЄС 2016 року та її оновлення, Стратегія кібердипломатії ЄС, План дій щодо стратегічних комунікацій, Стратегічний компас для безпеки та оборони 2022 року, регламенти про захист персональних даних, цифрові послуги та цифрові ринки, аналітичні звіти та дослідження міжнародних організацій, аналітичних центрів та незалежних експертів з питань цифрової дипломатії, кібербезпеки та стратегічних комунікацій, включаючи публікації Організації економічного співробітництва та розвитку, Центру передового досвіду стратегічних комунікацій НАТО, Європейського агентства з кібербезпеки, монографії, наукові статті та матеріали конференцій вітчизняних та зарубіжних дослідників, опубліковані у провідних наукових журналах та виданнях, індексованих у міжнародних наукометричних базах даних, статистичні дані та інформаційні матеріали, розміщені на офіційних веб-сайтах європейських інституцій, дипломатичних служб держав-членів ЄС, міжнародних організацій та аналітичних центрів, а також матеріали платформи EUvsDisinfo, звіти про реалізацію програм EU4Digital та Digital Europe, документи українсько-європейського кібердіалогу та інші первинні джерела, що забезпечують емпіричну основу для аналізу практичної реалізації політики цифрової дипломатії ЄС.

Практичне значення результатів дослідження полягає у можливості їхнього використання у практичній діяльності органів державної влади України, відповідальних за формування та реалізацію зовнішньої політики, європейську інтеграцію, кібербезпеку та стратегічні комунікації, зокрема Міністерства закордонних справ України, Міністерства цифрової трансформації України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України та інших установ, що працюють у сфері цифровізації міжнародних відносин та протидії гібридним загрозам, у розробленні освітніх програм, навчальних курсів та методичних матеріалів з цифрової дипломатії, публічної дипломатії, міжнародних комунікацій та європейської інтеграції для

закладів вищої освіти, що готують фахівців у галузі міжнародних відносин, у діяльності аналітичних центрів, неурядових організацій та експертних спільнот, що займаються дослідженням питань цифровізації зовнішньої політики, кібербезпеки, протидії дезінформації та європейської інтеграції України, а також у подальших наукових дослідженнях проблематики цифрової дипломатії як нового феномену міжнародних відносин та інноваційного інструменту зовнішньої політики у цифрову епоху.

Апробація результатів дослідження здійснена через участь автора у всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, листопад 2025 р.), до якого були підготовлені тези за темою «Політика ЄС у сфері цифрової дипломатії та її значення для України в умовах гібридних загроз».

Структура роботи зумовлена метою, завданнями та логікою дослідження і складається зі вступу, трьох розділів, висновків, списку використаних джерел. Загальний обсяг кваліфікаційної роботи становить 107 сторінок, з яких основний текст складає 101 сторінка, а список використаних джерел налічує 77 найменувань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЦИФРОВОЇ ДИПЛОМАТІЇ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

1.1. Поняття та сутність цифрової дипломатії в системі сучасних міжнародних відносин

Трансформація глобального комунікаційного простору, що відбувається впродовж останніх двох десятиліть, радикально змінила характер взаємодії між державами, міжнародними організаціями та недержавними акторами, створивши принципово нові можливості для здійснення дипломатичної діяльності в умовах цифрової реальності. Стрімкий розвиток інформаційно-комунікаційних технологій, поширення соціальних мереж та цифровізація суспільних процесів зумовили появу якісно нового феномену в системі міжнародних відносин, який дослідники концептуалізують як цифрову дипломатію, що являє собою комплексну систему практик, інструментів та стратегій зовнішньополітичної комунікації, реалізованих через цифрові платформи та технології. Осмислення сутності цифрової дипломатії потребує ретельного аналізу еволюції дипломатичних практик, розуміння специфіки цифрового середовища та визначення місця цього феномену в архітектурі сучасних міжнародних відносин, що набуває особливої актуальності в контексті геополітичних викликів та інформаційних загроз сучасності.

Концептуалізація цифрової дипломатії як наукового поняття розпочалася на початку 2010-х років, коли дослідники міжнародних відносин звернули увагу на систематичне використання цифрових технологій у зовнішньополітичній практиці провідних держав світу. Корнеліу Бйола та Маркус Холмс у своєму дослідженні визначають цифрову дипломатію як використання цифрових технологій для досягнення дипломатичних цілей, наголошуючи на трансформаційному характері цього процесу для традиційних дипломатичних інституцій [21, с. 34]. Це визначення акцентує увагу на інструментальному виді цифрових технологій, проте не розкриває повною мірою глибинних змін у самій природі дипломатичної комунікації, які відбуваються внаслідок цифровізації міжнародних відносин, що потребує більш комплексного концептуального підходу до розуміння цього феномену.

Поглиблене осмислення сутності цифрової дипломатії вимагає розмежування кількох споріднених, але не тотожних понять, які часто використовуються дослідниками як синоніми, створюючи термінологічну плутанину в науковому дискурсі. Джеймс Першінг наголошує на необхідності розрізняти е-дипломатію, яка передбачає використання електронних засобів комунікації в традиційних дипломатичних практиках, та власне цифрову дипломатію, що охоплює більш широкий спектр діяльності, включаючи стратегічну присутність у соціальних мережах, цифрову публічну дипломатію та управління цифровою репутацією держави [59]. Аналогічно, концепція твіпломатії, запроваджена дослідниками для позначення дипломатичної діяльності в соціальній мережі Twitter, являє собою лише один із компонентів ширшого феномену цифрової дипломатії, який охоплює різноманітні цифрові платформи, інструменти та стратегії комунікації в глобальному інформаційному просторі.

Структурний аналіз цифрової дипломатії дозволяє виокремити декілька ключових вимірів цього феномену, які у своїй сукупності формують цілісну систему цифрової дипломатичної практики сучасних міжнародних акторів. По-перше, технологічний вимір охоплює весь спектр цифрових інструментів та платформ, які використовуються для здійснення дипломатичної комунікації, включаючи соціальні мережі, відеоконференц-платформи, месенджери, веб-сайти дипломатичних місій, мобільні додатки та інші цифрові канали взаємодії з різноманітними цільовими аудиторіями. По-друге, комунікативний вимір відображає специфіку дипломатичної комунікації в цифровому середовищі, що характеризується інтерактивністю, миттєвістю, багатоканальністю, мультимедійністю та можливістю прямої взаємодії з громадянами інших держав, bypassing традиційних посередників у вигляді засобів масової інформації та урядових структур. По-третє, стратегічний вимір визначає цілі, завдання та методи використання цифрових технологій для досягнення зовнішньополітичних цілей, формування міжнародного іміджу, просування національних інтересів та впливу на міжнародний порядок денний, що вимагає розробки комплексних стратегій цифрової присутності та комунікації.

Функціональний аналіз цифрової дипломатії виявляє її багатогранність та багатоцільовий характер, що відрізняє її від традиційних форм дипломатичної діяльності, орієнтованих переважно на міждержавну комунікацію та переговорний процес. Ітай Менор у своєму дослідженні ідентифікує чотири ключові функції цифрової дипломатії: інформаційну, яка полягає у поширенні інформації про зовнішню політику держави та її позицію щодо міжнародних подій; комунікаційну, що передбачає налагодження діалогу з різними аудиторіями та стейкхолдерами; репутаційну, спрямовану на формування та підтримку позитивного іміджу держави в міжнародному інформаційному просторі; та консульську, яка охоплює надання цифрових консульських послуг громадянам за кордоном [53, с. 67-69]. Ця функціональна диференціація демонструє, що цифрова дипломатія не обмежується лише публічною комунікацією, а охоплює різноманітні аспекти дипломатичної діяльності, трансформуючи їх відповідно до можливостей та викликів цифрового середовища.

Особливу увагу в контексті осмислення сутності цифрової дипломатії заслуговує питання її співвідношення з концепцією публічної дипломатії, яка традиційно розглядається як комунікація держави з іноземними громадськостями з метою просування своїх цінностей, культури та зовнішньополітичних цілей. Кристофер Пол стверджує, що цифрова дипломатія являє собою еволюційний етап розвитку публічної дипломатії, адаптований до умов цифрової епохи, проте вона не зводиться виключно до публічної дипломатії, оскільки охоплює також інші аспекти дипломатичної діяльності, включаючи традиційну міждержавну комунікацію, консульські послуги, кризове реагування та цифрову взаємодію з діаспорами [61]. Водночас очевидно, що публічний вимір залишається одним із центральних компонентів цифрової дипломатії, оскільки цифрові технології створюють безпрецедентні можливості для прямої комунікації з глобальною аудиторією, формування наративів та впливу на громадську думку в інших країнах, що значно розширює інструментарій м'якої сили держав та міжнародних організацій.

Трансформаційний вплив цифрових технологій на дипломатичну практику

проявляється у декількох ключових аспектах, які радикально змінюють характер дипломатичної роботи та вимоги до дипломатичних служб сучасних держав. Передусім, цифровізація дипломатії призводить до демократизації міжнародної комунікації, оскільки дипломатичні представники отримують можливість безпосередньо звертатися до широких аудиторій, минаючи традиційних медіа-посередників, що змінює баланс сил у формуванні міжнародних наративів та громадської думки. Майкл Сейб та Кайл Тейлор наголошують, що ця демократизація має амбівалентний характер, адже вона не лише розширює можливості офіційної дипломатії, але й створює виклики, пов'язані з конкуренцією за увагу аудиторії, необхідністю швидкого реагування на події та ризиками дезінформації [67, с. 112-114]. Крім того, цифрові платформи сприяють горизонталізації дипломатичної комунікації, руйнуючи традиційні ієрархічні структури та протокольні обмеження, що дозволяє дипломатам різного рангу брати участь у формуванні зовнішньополітичного дискурсу та взаємодіяти безпосередньо з різними категоріями стейкхолдерів у режимі реального часу.

Аналізуючи специфіку цифрової дипломатії в системі сучасних міжнародних відносин, важливо враховувати контекст глибоких трансформацій міжнародного порядку, що відбуваються на тлі зростаючої міждержавної конкуренції, ерозії традиційних інституцій глобального управління та загострення геополітичного суперництва великих держав. Пітер Віглеб стверджує, що цифрова дипломатія стає агеною геополітичної конкуренції, де держави намагаються встановити цифрову гегемонію, просувати свої наративи та підривати позиції опонентів через інформаційний вплив, стратегічні комунікації та кібероперації [75]. У цьому контексті цифрова дипломатія перестає бути нейтральним інструментом комунікації і перетворюється на поле битви за формування глобальних наративів, встановлення норм цифрового простору та забезпечення національної безпеки в інформаційному вимірі, що вимагає від дипломатичних служб не лише комунікативних навичок, але й розуміння динаміки інформаційного протиборства та вміння захищати цифровий суверенітет держави.

Концептуальне осмислення цифрової дипломатії також потребує аналізу її

етичного виміру, оскільки використання цифрових технологій у дипломатичній практиці породжує численні етичні дилеми та питання про легітимність певних форм цифрового впливу. Бйола та Менор у спільній роботі порушують питання про межі прийняттого використання цифрових технологій у дипломатії, наголошуючи на необхідності розробки етичних норм та професійних стандартів цифрової дипломатичної практики, які б запобігали зловживанням, маніпуляціям та порушенням цифрових прав громадян [25, с. 89-92]. Особливої актуальності набувають питання про використання автоматизованих систем поширення інформації, таргетованого впливу на основі big data, мікротаргетингу політичних повідомлень та використання штучного інтелекту для генерації контенту, що розмиває межі між легітимною публічною дипломатією та маніпулятивним інформаційним впливом, створюючи нові виклики для міжнародного права та дипломатичної етики.

Інституційний вимір цифрової дипломатії відображає процеси адаптації традиційних дипломатичних служб до вимог цифрової епохи, що передбачає створення спеціалізованих підрозділів, розробку стратегій цифрової присутності, підготовку кадрів з відповідними компетенціями та інтеграцію цифрових практик у всі аспекти дипломатичної роботи. Шахар Ратцон у своєму дослідженні організаційних змін у міністерствах закордонних справ провідних держав зазначає, що інституціоналізація цифрової дипломатії відбувається нерівномірно, залежно від рівня технологічного розвитку країни, організаційної культури дипломатичної служби та пріоритетів зовнішньої політики [62]. Найбільш просунуті держави створили спеціалізовані департаменти цифрової дипломатії, розробили комплексні стратегічні документи та інвестували значні ресурси у розбудову цифрової дипломатичної інфраструктури, тоді як інші країни перебувають на початкових етапах цифровізації своїх дипломатичних служб, обмежуючись епізодичним використанням соціальних мереж без системного стратегічного підходу.

Важливим аспектом розуміння сутності цифрової дипломатії є аналіз її ефективності та методів її вимірювання, що становить значний методологічний виклик для дослідників через складність квантифікації впливу цифрової

комунікації на зовнішньополітичні результати. Елса Хендлер та Гай Йехімович наголошують, що традиційні метрики соціальних мереж, такі як кількість підписників, лайків та репостів, не дають адекватного уявлення про реальну ефективність цифрової дипломатії, оскільки не враховують якість взаємодії, глибину впливу на громадську думку та довгострокові ефекти на міжнародний імідж держави [40, с. 45-47]. Розробка комплексних систем оцінки ефективності цифрової дипломатії потребує поєднання кількісних та якісних методів, включаючи аналіз даних соціальних мереж, моніторинг медіа-покриття, дослідження громадської думки в цільових країнах та оцінку впливу цифрових кампаній на досягнення конкретних зовнішньополітичних цілей, що залишається предметом активних наукових дискусій та експериментування в практичній площині.

Розглядаючи цифрову дипломатію в контексті глобальних викликів сучасності, неможливо оминати увагою її роль у протидії дезінформації та захисті інформаційного простору, що стало одним із ключових завдань дипломатичних служб багатьох країн після серії інформаційних операцій, спрямованих на підрив демократичних процесів та дестабілізацію міжнародної безпеки. Алісса Купер та Френсіс Браун стверджують, що цифрова дипломатія набуває оборонного виміру, коли держави використовують її не лише для просування своїх інтересів, але й для захисту свого інформаційного простору від зовнішнього маніпулятивного впливу, протидії фейковим новинам та розвінчування ворожих наративів [25]. Це призводить до формування нової парадигми цифрової дипломатії, яка поєднує традиційні комунікативні функції з елементами стратегічних комунікацій, інформаційної безпеки та когнітивної оборони, що вимагає міжвідомчої координації та залучення експертизи з різних галузей, включаючи кібербезпеку, медіаграмотність та аналіз даних.

Узагальнюючи теоретичне осмислення поняття та сутності цифрової дипломатії, доцільно констатувати, що цей феномен являє собою складну, багатовимірну систему практик, інструментів та стратегій, які трансформують традиційну дипломатію під впливом цифрових технологій, створюючи нові можливості для міжнародної комунікації, публічної дипломатії та просування

національних інтересів, водночас породжуючи значні виклики, пов'язані з інформаційною безпекою, етичними дилемами та необхідністю адаптації дипломатичних інституцій. Цифрова дипломатія не є простим перенесенням традиційних дипломатичних практик у цифровий простір, а являє собою якісно новий тип дипломатичної діяльності, що характеризується інтерактивністю, публічністю, швидкістю реагування та можливістю прямого впливу на глобальні аудиторії, що радикально змінює логіку функціонування дипломатичних служб, вимоги до професійних компетенцій дипломатів та саму природу міжнародної комунікації в умовах глобалізованого цифрового світу. Розуміння цих фундаментальних характеристик цифрової дипломатії створює необхідну концептуальну основу для подальшого аналізу теоретико-методологічних підходів до її дослідження, що дозволить глибше осмислити механізми функціонування цього феномену та визначити оптимальні стратегії його застосування міжнародними акторами, зокрема Європейським Союзом, який розглядає цифрову дипломатію як один із ключових інструментів реалізації своєї глобальної стратегії та забезпечення своїх інтересів у міжнародній arena.

1.2. Теоретичні підходи до розкриття змісту цифрової дипломатії

Методологічна специфіка дослідження цифрової дипломатії впливає з її гібридної природи як феномену, що перебуває на перетині декількох наукових дисциплін та потребує інтегрованого аналітичного інструментарію, здатного охопити технологічні, комунікативні, політичні та інституційні виміри цього явища. Складність методологічного виклику полягає в тому, що цифрова дипломатія не може бути адекватно концептуалізована в межах однієї теоретичної парадигми чи дисциплінарного підходу, оскільки її функціонування зумовлюється взаємодією факторів різної природи – від технологічних можливостей цифрових платформ до глибинних трансформацій структури міжнародної системи, від психологічних механізмів сприйняття інформації до інституційних особливостей дипломатичних служб. Відтак, побудова coherentної методологічної рамки для аналізу цифрової дипломатії вимагає критичного

переосмислення існуючих теоретичних підходів теорії міжнародних відносин, їх адаптації до специфіки цифрового середовища та синтезу з концептуальними інструментами суміжних дисциплін, включаючи теорію комунікації, медіа-студії, політичну психологію та дослідження науки і технологій.

Застосування реалістичної парадигми до аналізу цифрової дипломатії дозволяє розглядати цей феномен крізь призму міждержавної конкуренції за владу та вплив, де цифрові технології виступають новим інструментом у традиційному геополітичному суперництві держав за домінування в міжнародній системі. З позицій структурного реалізму, цифрова дипломатія являє собою адаптацію держав до зміни розподілу можливостей в міжнародній системі, де інформаційна могутність стає дедалі важливішим компонентом національної сили поряд із традиційними військовими та економічними ресурсами, що змушує держави інвестувати в розбудову цифрової дипломатичної інфраструктури для збереження або покращення своїх позицій у глобальній ієрархії. Проте реалістична оптика виявляється обмеженою у поясненні кооперативних аспектів цифрової дипломатії, ролі недержавних акторів у формуванні цифрового дипломатичного простору та нормативних вимірів цифрової комунікації, які не зводяться виключно до логіки силової політики та національних інтересів, що спонукає дослідників звертатися до альтернативних теоретичних рамок.

Ліберальний інституціоналізм пропонує принципово відмінну аналітичну перспективу, фокусуючись на ролі міжнародних інституцій, норм та режимів у структуруванні цифрової дипломатичної практики та формуванні правил поведінки держав у цифровому просторі. Бйола та Холмс аргументують, що інституціональна перспектива дозволяє концептуалізувати цифрову дипломатію як колективну відповідь міжнародного співтовариства на виклики глобалізації та цифровізації, що передбачає розробку спільних стандартів, обмін найкращими практиками та створення механізмів координації національних цифрових дипломатичних стратегій [21, с. 78-81]. Особливої ваги набуває аналіз процесів інституціоналізації цифрової дипломатії всередині міжнародних організацій, зокрема Європейського Союзу, де формуються наднаціональні структури

координації цифрової зовнішньої політики, розробляються спільні стратегічні документи та встановлюються норми цифрової дипломатичної поведінки для держав-членів. Водночас ліберальна парадигма схильна недооцінювати конфліктний потенціал цифрової дипломатії, асиметрію можливостей різних акторів та роль цифрових технологій як інструментів маніпуляції та примусу, що обмежує пояснювальну силу цього підходу в умовах загострення інформаційного протиборства між великими державами.

Конструктивістська методологія відкриває евристично продуктивну перспективу для аналізу цифрової дипломатії через фокус на процесах конструювання смислів, ідентичностей та соціальних реальностей за допомогою цифрових комунікативних практик. Менор обґрунтовує, що цифрова дипломатія є насамперед практикою конструювання наративів про державу, її зовнішню політику та її місце в міжнародній системі, де дипломати виступають агентами формування колективних уявлень та інтерпретацій міжнародних подій у свідомості глобальних аудиторій [53, с. 134-137]. Ця перспектива дозволяє аналізувати цифрову дипломатію не як прямолінійну трансляцію інформації від держави до аудиторій, а як складний інтерактивний процес виробництва та змагання за нав'язування певних інтерпретацій реальності, де успіх залежить не стільки від обсягу повідомлень чи технічної досконалості каналів, скільки від здатності резонувати з існуючими системами значень, культурними кодами та когнітивними схемами цільових аудиторій. Конструктивістський аналіз також висвітлює процеси взаємного конституювання технологій та соціальних практик, демонструючи, що цифрові платформи не є нейтральними інструментами, а активно формують можливості та обмеження дипломатичної комунікації, структуруючи форми взаємодії, типи дискурсів та модальності репрезентації.

Теорія мережевого суспільства Мануеля Кастельса становить важливу методологічну рамку для осмислення трансформації дипломатичних практик у контексті переходу від вертикально організованих ієрархічних структур до горизонтальних мережевих форм соціальної організації. Застосування мережевої перспективи до аналізу цифрової дипломатії дозволяє концептуалізувати її як систему децентралізованих, але взаємопов'язаних вузлів комунікації, де

дипломатичні актори різного рівня – від міністерств закордонних справ до окремих дипломатів та посольств – формують складну екосистему інформаційних потоків, що не може бути зведена до простої ієрархічної структури. Віглеб стверджує, що мережева логіка цифрової дипломатії фундаментально суперечить традиційній бюрократичній організації дипломатичних служб, створюючи організаційне напруження між вимогами оперативності та гнучкості цифрової комунікації та інституційними процедурами контролю й координації [75]. Аналіз мережевих структур цифрової дипломатії методами соціального мережевого аналізу відкриває можливості для емпіричного дослідження патернів взаємодії між дипломатичними акторами, ідентифікації центральних вузлів впливу, виявлення кластерів та коаліцій у цифровому дипломатичному просторі.

Методологічний потенціал теорії комунікації для дослідження цифрової дипломатії полягає у можливості застосування розвинутого концептуального апарату аналізу комунікативних процесів до специфічного контексту міжнародної дипломатичної взаємодії в цифровому середовищі. Пол наголошує на необхідності розрізняти різні моделі комунікації в цифровій дипломатії – від односпрямованої трансляції інформації, що відповідає традиційній моделі масової комунікації, до діалогічної інтерактивної комунікації, що передбачає двостороннє спілкування та обмін думками між дипломатами та аудиторіями [4]. Застосування теорії медіатизації політики до аналізу цифрової дипломатії дозволяє осмислити, як логіка функціонування цифрових медіа трансформують саму природу дипломатичної діяльності, коли необхідність присутності в соціальних мережах, адаптації до форматів цифрових платформ та конкуренції за увагу аудиторій стає не зовнішнім додатком, а внутрішнім імперативом дипломатичної роботи. Критична комунікативна перспектива, розвинута представниками Франкфуртської школи та їхніми послідовниками, спрямовує увагу на владні відносини, що конституюються через цифрову дипломатичну комунікацію, виявляючи механізми символічного насильства, маніпуляції та гегемонії в інформаційному просторі.

Метод порівняльного аналізу посідає центральне місце в емпіричних

дослідженнях цифрової дипломатії, дозволяючи систематично зіставляти стратегії, практики та результати цифрової дипломатії різних акторів для виявлення успішних моделей, ідентифікації факторів ефективності та розуміння контекстуальних детермінант національних підходів до цифровізації зовнішньої політики. Ратцон у своєму компаративному дослідженні цифрової дипломатії США, Ізраїлю та скандинавських країн демонструє, що відмінності в організаційних структурах, ресурсному забезпеченні, стратегічних пріоритетах та політичних культурах призводять до формування різних моделей цифрової дипломатії, які по-різному балансують між централізацією та децентралізацією, між публічною та традиційною дипломатією, між наступальними та оборонними стратегіями [62]. Компаративний аналіз дозволяє також виявити конвергентні тенденції, коли різні актори незалежно один від одного приходять до схожих рішень, що може свідчити про існування універсальних закономірностей або найкращих практик цифрової дипломатії, незалежних від специфічного національного контексту.

Емпіричне дослідження цифрової дипломатії вимагає розробки адекватних методів збору та аналізу даних, що створює низку методологічних викликів, пов'язаних із специфікою цифрового середовища, обсягом інформації та динамічним характером онлайн-комунікації. Методи цифрової етнографії та віртуального включеного спостереження дозволяють дослідникам занурюватися в живу практику цифрової дипломатії, відстежувати взаємодії в режимі реального часу та фіксувати нюанси комунікативних стратегій, які залишаються невидимими при використанні суто кількісних методів збору даних. Купер та Браун описують методологію *longitudinal* дослідження цифрової дипломатії, що передбачає систематичне спостереження за дипломатичною активністю в соціальних мережах протягом тривалого періоду для виявлення еволюції стратегій, реакцій на кризи та адаптації до змін цифрового ландшафту [25]. Важливим методологічним інструментом стає аналіз великих даних (*big data analytics*), який дозволяє обробляти масиви інформації з соціальних мереж, ідентифікувати патерни, тренди та аномалії в цифровій дипломатичній активності різних акторів, проте його використання потребує критичної

рефлексії щодо репрезентативності даних, алгоритмічних упереджень та етичних імплікацій масового збору інформації.

Контент-аналіз як метод систематичного дослідження повідомлень дипломатичних акторів у цифровому просторі дозволяє виявляти домінуючі наративи, фрейми та дискурсивні стратегії, що використовуються для просування зовнішньополітичних цілей та формування міжнародного іміджу. Хендлер та Йехімович розробляють методологію багаторівневого контент-аналізу цифрової дипломатії, що поєднує кількісний аналіз частотності тем, тональності повідомлень та використання мультимедійних елементів з якісним дискурс-аналізом риторичних стратегій, аргументаційних структур та інтертекстуальних зв'язків [40, с. 89-93]. Особливої уваги заслуговує аналіз візуальної комунікації в цифровій дипломатії, оскільки зображення, відео та інфографіка стають дедалі важливішими елементами дипломатичних повідомлень у візуально орієнтованому середовищі соціальних мереж, що вимагає розробки спеціалізованих методів візуального аналізу з урахуванням семіотичних, естетичних та культурних вимірів візуальних репрезентацій.

Методологія аналізу політичного дискурсу, розвинута в рамках критичних дискурсивних студій, пропонує потужний інструментарій для дослідження того, як мова та комунікативні практики конституюють владні відносини, легітимують певні політичні позиції та маргіналізують альтернативні голоси в цифровому дипломатичному просторі. Застосування критичного дискурс-аналізу до цифрової дипломатії дозволяє виявляти приховані ідеологічні припущення, що лежать в основі дипломатичних наративів, розкривати механізми конструювання образів «своїх» та «чужих», аналізувати стратегії легітимації зовнішньополітичних дій та делігітімізації опонентів через дискурсивні практики. Сейб та Тейлор демонструють, як різні дипломатичні актори використовують специфічні дискурсивні репертуари та топоси для фреймування міжнародних подій у спосіб, що відповідає їхнім стратегічним інтересам, при цьому маскуючи партикулярний характер цих інтерпретацій під гаслом універсальних цінностей чи об'єктивної правди [67, с. 167-170].

Аналіз соціальних мереж (Social Network Analysis) як формалізований

метод дослідження структури відносин між акторами знаходить продуктивне застосування для картографування цифрового дипломатичного простору, виявлення центральних вузлів впливу, кластерів взаємодії та патернів інформаційних потоків між дипломатичними акторами. Цей метод дозволяє візуалізувати складні мережі цифрової дипломатичної взаємодії, де вузлами виступають акаунти дипломатичних інституцій, окремих дипломатів, політичних лідерів та інших релевантних акторів, а зв'язками – різні форми взаємодії від підписок та згадок до ретвітів та коментарів, що створює можливість для емпіричного вимірювання ступеня центральності, впливовості та інтегрованості різних акторів у цифрову дипломатичну екосистему. Застосування метрик центральності, таких як *degree centrality*, *betweenness centrality* та *eigenvector centrality*, дозволяє ідентифікувати найбільш впливових акторів не лише за формальним статусом, але й за фактичною позицією в мережевій структурі цифрової дипломатії.

Інтердисциплінарний характер цифрової дипломатії зумовлює необхідність інтеграції методологічних підходів з дослідження науки і технологій (*Science and Technology Studies*), які дозволяють аналізувати роль технологічних артефактів у формуванні соціальних практик та владних відносин. Концепція технополітики, розроблена Габрієллою Колеман, спрямовує увагу на те, як архітектура цифрових платформ, алгоритми ранжування контенту, інтерфейси користувача та інші технічні елементи не є нейтральними технічними рішеннями, а втілюють певні політичні логіки, норми та цінності, що активно формують можливості та обмеження дипломатичної комунікації в цифровому просторі. Аналіз матеріальності цифрової інфраструктури – від підводних кабелів та серверів до протоколів передачі даних та систем модерації контенту – розкриває геополітичні виміри технологічної залежності, питання цифрового суверенітету та асиметрії влади між власниками цифрових платформ та їхніми користувачами, включаючи дипломатичних акторів.

Психологічні підходи до вивчення цифрової дипломатії фокусуються на когнітивних та емоційних механізмах сприйняття, обробки та реагування на дипломатичні повідомлення в цифровому середовищі, що відкриває можливості

для мікрорівневого аналізу ефективності різних комунікативних стратегій. Теорія переконання та моделі зміни установок дозволяють концептуалізувати умови, за яких цифрова дипломатична комунікація може впливати на думки та поведінку цільових аудиторій, ідентифікуючи фактори, що сприяють або перешкоджають прийняттю дипломатичних повідомлень. Дослідження когнітивних упереджень, таких як *confirmation bias*, *echo chamber effects* та *filter bubbles*, розкривають обмеження можливостей цифрової дипломатії переконувати опонентів або досягати аудиторій з протилежними поглядами в поляризованому інформаційному середовищі, де алгоритми персоналізації контенту створюють ізольовані інформаційні бульбашки. Емоційний вимір цифрової дипломатії, включаючи використання афективних апелів, створення емпатії та мобілізацію почуттів солідарності чи обурення, потребує залучення теоретичних рамок афективних студій для розуміння механізмів емоційного резонансу дипломатичних наративів.

Критична геополітика як методологічний підхід пропонує інструментарій для деконструкції геополітичних уявлень, що транслуються через цифрову дипломатію, розкриваючи механізми конструювання просторових уявлень, територіальних ідентичностей та геополітичних наративів за допомогою цифрових комунікативних практик. Аналіз з позицій критичної геополітики виявляє, як дипломатичні актори використовують цифрові платформи для просування специфічних геополітичних візій світового порядку, регіональних конфігурацій та міжнародних ієрархій, при цьому натуралізуючи партикулярні інтереси як універсальні цінності та представляючи контингентні політичні вибори як об'єктивні географічні або історичні необхідності. Бйола аргументує, що цифрова дипломатія стає ареною змагання між конкуруючими геополітичними наративами, де різні актори намагаються встановити гегемонію своїх інтерпретацій міжнародних подій, географічних реальностей та історичних процесів [21, с. 203-206].

Методологічна рефлексивність вимагає критичного усвідомлення обмежень та упереджень, властивих різним дослідницьким підходам до цифрової дипломатії, включаючи проблеми доступу до даних,

репрезентативності вибірок, валідності вимірювань та узагальнюваності висновків. Специфіка цифрового середовища створює нові етичні виклики для дослідників, пов'язані з питаннями приватності, інформованої згоди, відповідального використання даних та можливих негативних наслідків публікації результатів досліджень для об'єктів дослідження. Менор наголошує на необхідності розробки етичних протоколів для дослідження цифрової дипломатії, що враховували б баланс між науковою свободою та захистом прав і інтересів досліджуваних суб'єктів, особливо у випадках вивчення сензитивних питань, конфліктних ситуацій або репресивних режимів [53, с. 278-281].

Синтезуючи розглянуті теоретико-методологічні підходи, доцільно констатувати, що адекватне дослідження цифрової дипломатії потребує методологічного плюралізму та творчої комбінації різних аналітичних інструментів залежно від конкретних дослідницьких питань, рівня аналізу та емпіричного контексту. Жоден окремий теоретичний підхід не може претендувати на вичерпне пояснення багатогранного феномену цифрової дипломатії, що функціонує одночасно як технологічна система, комунікативна практика, інституційний процес та геополітична стратегія, вимагаючи інтегрованих аналітичних рамок, здатних охоплювати взаємодію цих різних вимірів. Розуміння методологічних можливостей та обмежень різних підходів створює основу для ретельного емпіричного аналізу конкретних випадків цифрової дипломатії, зокрема практики Європейського Союзу, чиї унікальні інституційні характеристики як наднаціонального актора вимагають специфічної аналітичної оптики для розуміння нормативно-правових та концептуальних основ його цифрової дипломатичної діяльності, до аналізу яких доцільно перейти в наступному підрозділі дослідження.

1.3. Нормативно-правові та концептуальні основи цифрової дипломатії Європейського Союзу

Формування нормативно-правової бази цифрової дипломатії Європейського Союзу відбувається в контексті складної інституційної

архітектури цього наднаціонального утворення, де компетенції у сфері зовнішньої політики розподілені між наднаціональними інституціями та державами-членами, що створює специфічну конфігурацію повноважень, процедур прийняття рішень та механізмів імплементації, які фундаментально відрізняються від моделей національної дипломатії. Особливість правового регулювання цифрової дипломатії ЄС полягає в тому, що воно не кодифіковане в єдиному нормативному акті, а розпорошене в численних стратегічних документах, регламентах, директивах та рішеннях, які охоплюють різні аспекти цифровізації зовнішньої політики від кібербезпеки до цифрових прав людини, від стратегічних комунікацій до регулювання цифрових платформ. Водночас нормативна рамка цифрової дипломатії ЄС тісно переплетена з ширшою системою *acquis communautaire* у сферах цифрової економіки, захисту даних, боротьби з дезінформацією та кібербезпеки, що відображає холістичний підхід Союзу до цифрових питань як міжсекторального виклику, який не може бути редукований виключно до дипломатичного виміру.

Первинне право Європейського Союзу закладає фундаментальні принципи та інституційні рамки для здійснення зовнішньої політики, включаючи її цифровий вимір, навіть якщо термін «цифрова дипломатія» не фігурує експліцитно в установчих договорах. Лісабонський договір 2009 року створив Європейську службу зовнішніх дій (European External Action Service, EEAS) як унікальну дипломатичну службу *suí generis*, що поєднує елементи міжурядової координації та наднаціональної інтеграції, наділивши її повноваженнями підтримувати Високого представника Союзу з питань зовнішньої політики та політики безпеки у виконанні мандату щодо проведення Спільної зовнішньої та безпекової політики. Віглеб зазначає, що інституційна автономія EEAS створила організаційні передумови для розвитку власної цифрової дипломатичної спроможності ЄС, незалежної від національних дипломатичних служб держав-членів, хоча на практиці ефективність цифрової дипломатії Союзу значною мірою залежить від координації та синергії між рівнем ЄС та національним рівнем [75]. Договірні положення про лояльне співробітництво між інституціями ЄС та державами-членами набувають особливого значення в контексті цифрової

дипломатії, де необхідна узгодженість повідомлень та координація активності в цифровому просторі для забезпечення когерентності зовнішньополітичного представлення Союзу.

Стратегічна рамка цифрової дипломатії ЄС почала формуватися в середині 2010-х років як відповідь на зростаюче усвідомлення важливості цифрового виміру зовнішньої політики та необхідності системного підходу до використання цифрових інструментів для просування інтересів та цінностей Союзу. Глобальна стратегія Європейського Союзу 2016 року «Shared Vision, Common Action: A Stronger Europe», представлена Високим представником Федерікою Могеріні, стала поворотним документом, який визначив стратегічні пріоритети зовнішньої політики ЄС у новому геополітичному контексті та експліцитно визнав важливість стратегічних комунікацій і цифрових технологій для реалізації амбіцій Союзу як глобального актора. Бйола та Холмс аргументують, що Глобальна стратегія 2016 року ознаменувала парадигмальний зсув у зовнішній політиці ЄС від переважно нормативної та економічної сили до більш прагматичного та геополітичного позиціонування, де цифрова дипломатія розглядається як інструмент забезпечення стратегічної автономії та захисту європейських інтересів [21, с. 289-292].

Концептуалізація цифрової дипломатії в документах ЄС еволюціонувала від вузького розуміння як присутності в соціальних мережах до комплексного підходу, що охоплює широкий спектр цифрових практик, інструментів та політик. Стратегія кібердипломатії ЄС, прийнята Радою у 2015 році та оновлена у 2021 році, визначає принципи та інструменти дипломатичної відповіді Союзу на шкідливу кібердіяльність, включаючи режим рестриктивних заходів проти відповідальних за кібератаки, що демонструє розуміння цифрової дипломатії не лише як комунікативної практики, але й як інструменту примусу та стримування у кіберпросторі. План дій щодо стратегічних комунікацій 2015 року, розроблений у відповідь на російську дезінформаційну кампанію, створив інституційну основу для систематичної протидії іноземному інформаційному впливу через мережу оперативних груп East StratCom та інших регіональних підрозділів, що свідчить про еволюцію цифрової дипломатії ЄС у напрямку

включення оборонних та контрнарративних елементів.

Нормативне регулювання цифрового простору в ЄС, хоча формально не є частиною дипломатичної політики, створює важливий контекст та інструментарій для цифрової дипломатії Союзу, перетворюючи регуляторну потужність на форму структурної влади у глобальному цифровому середовищі. Загальний регламент про захист даних (General Data Protection Regulation, GDPR) 2016 року встановив високі стандарти захисту персональних даних, які завдяки екстратериторіальному застосуванню та ефекту Брюсселя де-факто стали глобальним benchmark, що дозволяє ЄС позиціонувати себе як лідера в питаннях цифрових прав і створює нормативну основу для критики практик інших акторів, що не відповідають європейським стандартам. Менор стверджує, що регуляторна дипломатія стає ключовим компонентом цифрової зовнішньої політики ЄС, де Союз використовує свою внутрішню регуляторну спроможність для формування глобальних норм та стандартів цифрового простору відповідно до європейських цінностей демократії, прав людини та верховенства права [53, с. 312-315].

Акт про цифрові послуги (Digital Services Act, DSA) та Акт про цифрові ринки (Digital Markets Act, DMA), прийняті у 2022 році, становлять наступний етап європейського регуляторного підходу до цифрового простору, спрямованого на обмеження влади великих технологічних платформ, забезпечення справедливої конкуренції, прозорості алгоритмів та відповідальності за контент, що має прямі імплікації для цифрової дипломатії через встановлення правил модерації контенту, боротьби з дезінформацією та архітектури вибору користувачів. Ці регуляторні інструменти дозволяють ЄС формувати структурні умови функціонування цифрових платформ, на яких здійснюється значна частина цифрової дипломатичної активності, що надає Союзу унікальний важіль впливу порівняно з іншими міжнародними акторами, які можуть регулювати лише діяльність своїх власних дипломатичних служб, але не саму цифрову інфраструктуру комунікації. Пол наголошує, що цей регуляторний підхід відображає специфічну модель цифрової влади ЄС, яка компенсує обмежені військові та економічні ресурси через нормативну та

регуляторну потужність у цифровій сфері [61].

Стратегія цифрової трансформації дипломатії EEAS, презентована у 2020 році, являє собою найбільш комплексний документ, що безпосередньо присвячений цифровізації дипломатичної діяльності Європейського Союзу та визначає конкретні цілі, завдання та механізми імплементації цифрової дипломатії на рівні інституцій ЄС. Стратегія артикулює три основні pillar'i цифрової трансформації EEAS: розвиток цифрової грамотності та навичок персоналу; модернізація цифрової інфраструктури та інструментів; та посилення цифрової безпеки дипломатичних комунікацій та систем, що відображає розуміння цифрової дипломатії як комплексного феномену, який вимагає не лише зовнішньої комунікації, але й внутрішньої організаційної трансформації. Сейб та Тейлор зазначають, що імплементація цієї стратегії стикається з численними викликами, включаючи бюджетні обмеження, інституційну інерцію, відмінності у цифровій зрілості різних підрозділів та необхідність балансування між інноваційністю та безпекою [67, с. 234-237].

Концепція стратегічної автономії, що стала центральною у зовнішньополітичному дискурсі ЄС останніх років, має важливі імплікації для розуміння цілей та напрямків цифрової дипломатії Союзу в контексті зростаючої геополітичної конкуренції та технологічного суперництва великих держав. Прагнення до цифрового суверенітету, артикульоване в численних документах Європейської Комісії та EEAS, передбачає зменшення залежності від цифрових технологій та платформ, контрольованих іноземними акторами, розвиток власних європейських альтернатив та забезпечення здатності Союзу автономно діяти в цифровому просторі відповідно до своїх цінностей та інтересів. Ратцон аргументує, що концепція цифрового суверенітету відображає усвідомлення ЄС геополітичного виміру технологій та намагання трансформувати регуляторну потужність у справжню стратегічну спроможність, хоча реалізація цієї амбіції стикається з фундаментальними викликами, пов'язаними з фрагментацією європейського технологічного ландшафту та відставанням від США та Китаю у ключових цифрових секторах [62].

Інституційна архітектура цифрової дипломатії ЄС характеризується

складною системою розподілу повноважень та координаційних механізмів між різними акторами, що включають EEAS, Європейську Комісію, держави-члени та їхні дипломатичні служби, делегації ЄС у третіх країнах та міжнародних організаціях, спеціалізовані агенції та органи Союзу. Створення у 2015 році Оперативної групи East StratCom у складі EEAS ознаменувало інституціоналізацію функції стратегічних комунікацій на рівні ЄС з конкретним мандатом протидії дезінформації та просування позитивного наративу про політику Союзу у східному сусідстві, що стало прецедентом для подальшого розширення спроможностей стратегічних комунікацій через створення аналогічних структур для інших регіонів. Купер та Браун наголошують, що ефективність інституційної архітектури цифрової дипломатії ЄС значною мірою залежить від якості координації між різними акторами та здатності забезпечити узгодженість повідомлень та дій у цифровому просторі, що залишається постійним викликом через інституційну складність та множинність голосів Союзу [25].

Нормативна основа протидії дезінформації в ЄС еволюціонувала від м'яких інструментів саморегуляції до більш жорстких регуляторних механізмів, відображаючи зростаюче усвідомлення серйозності загрози іноземного інформаційного впливу для демократичних процесів та суспільної згуртованості. Кодекс практик щодо дезінформації, запроваджений у 2018 році та посилений у 2022 році, являє собою систему добровільних зобов'язань великих цифрових платформ щодо боротьби з дезінформацією через прозорість політичної реклами, позначення ботів, співпрацю з фактчекерами та обмеження монетизації дезінформації, що становить форму со-regulation між державою та приватними корпораціями. Хендлер та Йехімович зазначають, що перехід від першої версії Кодексу до посиленої версії 2022 року відображає визнання недостатності pure voluntary підходу та необхідності більш обов'язкових механізмів підзвітності платформ, що було закріплено у положеннях Акту про цифрові послуги [40, с. 178-181].

План дій для європейської демократії 2020 року та наступні законодавчі ініціативи щодо політичної реклами та прозорості формують комплексну

нормативну рамку для захисту демократичних процесів від маніпулятивного цифрового впливу, що має безпосередні імплікації для цифрової дипломатії через встановлення правил щодо іноземного фінансування політичних кампаній, таргетованої політичної реклами та використання персональних даних для політичного мікротаргетингу. Ці регуляторні заходи відображають прагнення ЄС поєднати цифрову відкритість з захистом від зловживань, дозволяючи легітимну публічну дипломатію іноземних акторів, водночас обмежуючи приховані маніпулятивні впливи, що розмиває традиційні дихотомії між внутрішньою та зовнішньою політикою, між регуляцією та дипломатією, між захистом суверенітету та відкритістю до світу. Бйола та Холмс стверджують, що ця нормативна рамка являє собою спробу артикулювати специфічну європейську модель цифрового ліберального порядку, альтернативну як американському *laissez-faire* підходу, так і китайській моделі цифрового авторитаризму [21, с. 356-359].

Зовнішній вимір європейської цифрової політики, артикульований у численних стратегічних документах, включаючи «Формування цифрового майбутнього Європи» 2020 року та «Глобальний підхід до цифрової дипломатії» 2021 року, визначає амбіції ЄС щодо просування європейських цінностей, норм та стандартів у глобальному цифровому просторі через дипломатичну взаємодію, міжнародні партнерства та багатосторонні форуми. Ключовими елементами цього зовнішнього виміру є просування багатостороннього, заснованого на правилах підходу до глобального інтернет-управління; захист прав людини в цифровому просторі, включаючи свободу вираження поглядів, приватність та доступ до інформації; боротьба проти авторитарного використання цифрових технологій для масового спостереження та соціального контролю; та підтримка цифрової трансформації в країнах-партнерах відповідно до європейських стандартів та цінностей. Віглеб зазначає, що реалізація цих амбіцій стикається з фундаментальним викликом *fragmentation* глобального цифрового простору на конкуруючі нормативні блоки, де європейська модель конкурує з альтернативними візіями цифрового порядку, що просуваються іншими великими державами [75].

Partnerships та багатосторонні ініціативи становлять важливий інструмент цифрової дипломатії ЄС, дозволяючи Союзу поширювати свій вплив через створення коаліцій однодумців та формування міжнародних норм у ключових цифрових питаннях. Ініціатива «Партнерство для відкритого Інтернету», запущена у 2022 році, об'єднує демократичні держави та приватний сектор навколо зобов'язань захищати відкритий, вільний, глобальний, сумісний, надійний та безпечний Інтернет, що відображає прагнення протиставити альянс демократій фрагментаційним тенденціям та авторитарним моделям цифрового управління. Менор аргументує, що ця форма коаліційної дипломатії дозволяє ЄС множити свій вплив через об'єднання зусиль з партнерами-однодумцями, водночас створюючи peer pressure на держави, які не приєднуються до цих ініціатив, щоб пояснювати або переглядати свої політики [53, с. 398-401].

Цифрова допомога та capacity building у країнах-партнерах становлять важливий, хоча часто недооцінений компонент цифрової дипломатії ЄС, що передбачає передачу технологій, знань та ресурсів для підтримки цифрової трансформації відповідно до європейських стандартів та підходів. Програми цифрової допомоги в рамках European Neighbourhood Policy, Development Cooperation Instrument та інших інструментів зовнішнього фінансування дозволяють ЄС формувати цифровий розвиток країн-партнерів у напрямку, сумісному з європейськими цінностями та нормами, що створює довгострокові умови для поширення європейської моделі цифрового управління. Пол зазначає, що ця форма структурної влади через формування інституцій, регуляторних рамок та технологічних систем у третіх країнах може мати більш довготривалий ефект, ніж прямі комунікативні заходи цифрової публічної дипломатії [61].

Кібербезпекова дипломатія становить критично важливий компонент цифрової зовнішньої політики ЄС, що охоплює широкий спектр активностей від confidence-building measures та Norm-setting у багатосторонніх форумах до attribution кібератак та застосування дипломатичних санкцій проти відповідальних акторів. Режим кібердипломатичного інструментарію ЄС, встановлений у 2017 році та посилений у наступних роках, дозволяє Союзу застосовувати рестриктивні заходи, включаючи заморожування активів та

заборони на видачу віз, проти індивідів та організацій, відповідальних за кібератаки, що становить форму примусової дипломатії в цифровому просторі. Сейб та Тейлор підкреслюють, що ефективність цього інструментарію залежить від спроможності ЄС та держав-членів здійснювати технічну attribution кібератак з достатньою впевненістю та швидкістю для забезпечення своєчасної та переконливої дипломатичної відповіді, що вимагає значних інвестицій у технічні можливості кіберрозвідки та аналізу [67, с. 289-292].

Участь ЄС у багатосторонніх форумах з питань цифрового управління, включаючи Internet Governance Forum, ITU, OECD та інші міжнародні майданчики, становить важливий канал просування європейських позицій та формування глобальних норм у цифровій сфері. Ратцон зазначає, що багатосторонній підхід відповідає фундаментальним цінностям та інтересам ЄС як актора, чия влада базується переважно на нормативному впливі та інституційній спроможності, а не на військовій силі чи технологічному домінуванні, що робить багатосторонні інституції природним середовищем для реалізації європейського впливу [62]. Водночас ефективність багатостороннього підходу підривається фрагментацією міжнародного співтовариства з цифрових питань, зростаючим напруженням між великими державами та відсутністю консенсусу щодо базових принципів цифрового управління, що змушує ЄС дедалі більше покладатися на *minilateral* підходи та *partnerships* з демократичними однодумцями.

Інформаційна безпека та протидія іноземному інформаційному впливу стали центральними елементами цифрової дипломатії ЄС після серії інформаційних операцій, спрямованих на підриг демократичних процесів у державах-членах та сусідніх країнах, що призвело до розробки комплексної системи виявлення, аналізу та спростування дезінформації. Система раннього попередження про дезінформацію (*Rapid Alert System*), створена у 2019 році, забезпечує обмін інформацією між державами-членами про виявлені дезінформаційні кампанії та координацію відповідних заходів, що становить форму колективної інформаційної оборони на рівні ЄС. Купер та Браун наголошують, що ефективність протидії дезінформації залежить не лише від

технічних спроможностей виявлення та спростування, але й від здатності розробляти compelling позитивні наративи, які можуть конкурувати за увагу аудиторій з емоційно зарядженим маніпулятивним контентом, що вимагає переходу від pure defensive позиції до більш проактивного narrative engagement [25].

Концептуальна рамка європейської моделі цифрової дипломатії базується на специфічній комбінації ліберальних цінностей, регуляторного підходу та багатостороннього інституціоналізму, що відрізняє її як від американської моделі, орієнтованої на свободу приватного сектору та мінімальне державне втручання, так і від авторитарних моделей, що використовують цифрові технології для соціального контролю та інформаційного домінування. Хендлер та Йехімович ідентифікують три ключові pillar'и європейської цифрової дипломатичної моделі: людино-центричний підхід, що ставить права людини та демократичні цінності в центр цифрової політики; регуляторний активізм, що передбачає активну роль держави у формуванні цифрового простору відповідно до суспільних інтересів; та багатосторонній підхід до глобального цифрового управління, що відкидає як односторонні дії, так і fragmentation цифрового простору на закриті національні сегменти [40, с. 267-270].

Виклики імплементації нормативно-правової рамки цифрової дипломатії ЄС пов'язані як з внутрішніми факторами інституційної складності, обмежених ресурсів та відмінностей між державами-членами, так і з зовнішніми факторами геополітичного протистояння, технологічного відставання та конкуренції альтернативних моделей цифрового управління. Фундаментальне напруження між наднаціональними амбіціями та міжурядовою реальністю зовнішньої політики ЄС проявляється також у цифровій дипломатії, де держави-члени зберігають значну автономію у веденні власної цифрової дипломатії, що може не завжди узгоджуватися з позицією та стратегіями рівня ЄС, створюючи проблеми coherence та ефективності спільного зовнішньополітичного представлення Союзу. Бйола стверджує, що подолання цього виклику вимагає не лише формальних координаційних механізмів, але й розвитку спільної strategic culture цифрової дипломатії, яка б об'єднувала різні актори навколо спільного розуміння

цілей, методів та пріоритетів цифрової зовнішньої політики ЄС [21, с. 412-415].

Перспективи розвитку нормативно-правової бази цифрової дипломатії ЄС визначаються динамікою геополітичного середовища, технологічних інновацій та внутрішньополітичних процесів в Союзі, що створює умови як для поглиблення існуючих підходів, так і для можливих парадигмальних зсувів. Оновлення Глобальної стратегії ЄС, очікуване в найближчі роки, може призвести до перегляду ролі та пріоритетів цифрової дипломатії в контексті зростаючої геополітичної конкуренції та необхідності забезпечення стратегічної автономії Союзу в усіх вимірах, включаючи цифровий, що може означати посилення *defensive* та *assertive* елементів цифрової дипломатії поряд з традиційним фокусом на нормативному лідерстві та *promotion* демократичних цінностей. Менор прогнозує, що майбутнє європейської цифрової дипломатії лежатиме в напрямку більшої інтеграції різних інструментів зовнішньої політики – від регуляції та санкцій до публічної дипломатії та розвиткової допомоги – в *coherent* стратегію використання цифрового виміру для досягнення геополітичних цілей Союзу [53, с. 445-448].

Узагальнюючи аналіз нормативно-правових та концептуальних основ цифрової дипломатії Європейського Союзу, доцільно констатувати, що ЄС розробив комплексну, хоча й фрагментовану систему стратегічних документів, регуляторних інструментів та інституційних механізмів, які в сукупності формують специфічну європейську модель цифрової дипломатії, що базується на поєднанні ліберальних цінностей, регуляторного активізму та багатостороннього підходу до глобального цифрового управління. Особливість цієї моделі полягає у тісній інтеграції внутрішньої цифрової політики та зовнішньої дипломатії, де регуляторна потужність ЇС у цифровій сфері перетворюється на інструмент зовнішньополітичного впливу через встановлення стандартів, формування норм та створення структурних умов функціонування глобального цифрового простору відповідно до європейських цінностей та інтересів. Водночас реалізація цієї моделі стикається з численними викликами, пов'язаними з інституційною складністю Союзу, обмеженими ресурсами, технологічною залежністю від іноземних провайдерів та

геополітичною конкуренцією альтернативних візій цифрового порядку, що вимагає постійної адаптації та вдосконалення нормативно-правової рамки цифрової дипломатії ЄС у відповідь на динамічні зміни технологічного та геополітичного середовища, зберігаючи при цьому вірність фундаментальним цінностям демократії, прав людини та верховенства права, які становлять основу європейської ідентичності та легітимності Союзу як глобального актора.

Висновки до розділу 1

Теоретичне осмислення феномену цифрової дипломатії в системі сучасних міжнародних відносин дозволяє концептуалізувати його як комплексну, багатовимірну систему практик, інструментів та стратегій, що трансформують традиційну дипломатію під впливом цифрових технологій, створюючи якісно нові можливості для міжнародної комунікації, просування національних інтересів та формування глобальних наративів, водночас породжуючи значні виклики, пов'язані з інформаційною безпекою, етичними дилемами та необхідністю адаптації дипломатичних інституцій до вимог цифрової епохи. Аналіз еволюції наукового дискурсу щодо цифрової дипломатії виявляє поступовий перехід від вузького інструментального розуміння як простого використання цифрових платформ до комплексної концептуалізації, що охоплює технологічні, комунікативні, інституційні, стратегічні та геополітичні виміри цього феномену, які у своїй сукупності формують цілісну екосистему цифрової дипломатичної діяльності сучасних міжнародних акторів.

Структурний аналіз цифрової дипломатії розкриває її функціональну багатогранність, що виходить за межі традиційної публічної дипломатії та охоплює широкий спектр активностей від інформаційного обміну та діалогу з громадськостями до формування міжнародного іміджу, консульських послуг, кризового реагування, протидії дезінформації та кібердипломатії, що вимагає від дипломатичних служб розвитку нових компетенцій, організаційних структур та стратегічних підходів. Трансформаційний вплив цифрових технологій на дипломатичну практику проявляється у демократизації міжнародної комунікації

через можливість прямого звернення до глобальних аудиторій, горизонталізації дипломатичної взаємодії через руйнування традиційних ієрархічних структур, прискоренні темпоральності дипломатичних процесів через вимогу миттєвого реагування на події та мультимодальності комунікації через інтеграцію текстових, візуальних, аудіо та відео форматів у цілісні дипломатичні повідомлення.

Методологічний аналіз підходів до дослідження цифрової дипломатії демонструє необхідність інтегрованої аналітичної рамки, яка поєднує інструментарій теорії міжнародних відносин, теорії комунікації, медіа-студій, соціології технологій та суміжних дисциплін для адекватного охоплення багатогранності цього феномену. Застосування різних теоретичних парадигм теорії міжнародних відносин до аналізу цифрової дипломатії виявляє їхні специфічні евристичні переваги та обмеження, де реалізм фокусується на конкурентному та силовому вимірі цифрової дипломатії, ліберальний інституціоналізм висвітлює роль інституцій та норм у структуруванні цифрової дипломатичної практики, а конструктивізм розкриває процеси конструювання смислів, ідентичностей та наративів через цифрову комунікацію, що обґрунтовує доцільність методологічного плюралізму та творчої комбінації різних підходів залежно від конкретних дослідницьких питань.

Емпіричне дослідження цифрової дипломатії потребує розробки адекватних методів збору та аналізу даних, що включають цифрову етнографію, контент-аналіз, дискурс-аналіз, аналіз соціальних мереж, аналіз великих даних та інші інструменти, які дозволяють систематично досліджувати цифрову дипломатичну практику різних акторів, виявляти патерни, тренди та ефективність різних стратегій, водночас усвідомлюючи методологічні виклики та обмеження, пов'язані з репрезентативністю даних, валідністю вимірювань, етичними дилемами та динамічним характером цифрового середовища. Інтердисциплінарний характер методології дослідження цифрової дипломатії відображає гібридну природу самого феномену, який перебуває на перетині політики, технології, комунікації та культури, вимагаючи від дослідників здатності інтегрувати концептуальні інструменти та аналітичні техніки з різних

дисциплінарних традицій у coherent дослідницьку стратегію.

Аналіз нормативно-правових та концептуальних основ цифрової дипломатії Європейського Союзу виявляє формування специфічної європейської моделі, що базується на поєднанні ліберальних цінностей, регуляторного підходу та багатостороннього інституціоналізму, відрізняючись як від американської моделі технологічного *laissez-faire*, так і від авторитарних моделей цифрового контролю. Нормативна рамка цифрової дипломатії ЄС характеризується фрагментованістю та розпорошеністю в численних стратегічних документах, регламентах та рішеннях, що охоплюють різні аспекти від кібербезпеки до протидії дезінформації, від стратегічних комунікацій до регулювання цифрових платформ, проте об'єднаних спільною логікою використання регуляторної потужності Союзу для формування глобальних норм та стандартів цифрового простору відповідно до європейських цінностей.

Інституційна архітектура цифрової дипломатії ЄС відображає складність інституційної структури Союзу через систему розподілених повноважень між EEAS, Європейською Комісією, державами-членами та спеціалізованими агенціями, що створює виклики координації та когерентності, проте водночас дозволяє мобілізувати різноманітні ресурси та експертизу для комплексного підходу до цифрових питань. Стратегічна рамка цифрової дипломатії ЄС еволюціонувала від фокусу на публічній комунікації до комплексного підходу, що інтегрує наступальні та оборонні елементи, публічну та традиційну дипломатію, регуляторні та комунікативні інструменти в цілісну стратегію використання цифрового виміру для досягнення зовнішньополітичних цілей Союзу та забезпечення його стратегічної автономії в умовах зростаючої геополітичної конкуренції.

Концепція цифрового суверенітету та стратегічної автономії в цифровій сфері відображає усвідомлення ЄС геополітичного виміру технологій та прагнення трансформувати регуляторну потужність у справжню стратегічну спроможність автономно діяти в цифровому просторі відповідно до європейських цінностей та інтересів, незалежно від іноземних технологічних провайдерів та цифрових платформ. Зовнішній вимір європейської цифрової

політики спрямований на просування багатостороннього, заснованого на правилах підходу до глобального інтернет-управління, захист прав людини в цифровому просторі, протидію авторитарному використанню технологій та підтримку цифрової трансформації країн-партнерів відповідно до європейських стандартів через дипломатичну взаємодію, міжнародні партнерства та розвиткову допомогу.

Виклики імплементації нормативно-правової рамки цифрової дипломатії ЄС пов'язані з інституційною складністю Союзу, обмеженими ресурсами порівняно з великими державами, технологічною залежністю від іноземних провайдерів, різницею в пріоритетах та підходах держав-членів та геополітичною конкуренцією альтернативних моделей цифрового управління, що вимагає постійної адаптації стратегій, вдосконалення координаційних механізмів та інвестицій у розвиток власних технологічних спроможностей. Водночас унікальна комбінація великого внутрішнього ринку, розвиненої регуляторної спроможності, нормативного авторитету та м'якої сили дозволяє ЄС відігравати значущу роль у формуванні глобального цифрового порядку, компенсуючи обмеження військової та технологічної могутності через структурну владу встановлення норм, стандартів та правил функціонування цифрового простору.

Теоретичне осмислення концептуальних основ цифрової дипломатії та аналіз специфіки європейської моделі створюють необхідну аналітичну рамку для подальшого емпіричного дослідження конкретних практик, інструментів та результатів цифрової дипломатії Європейського Союзу, що дозволить перейти від абстрактного теоретизування до детального аналізу того, як нормативні принципи та стратегічні документи трансформуються в конкретні дипломатичні дії, комунікативні кампанії та зовнішньополітичні результати, виявляючи розриви між декларованими амбіціями та реальними досягненнями, між стратегічними документами та практичною імплементацією, між нормативними цілями та прагматичними компромісами, що характеризують складну реальність цифрової дипломатії Європейського Союзу в умовах турбулентного геополітичного середовища та швидких технологічних трансформацій сучасного світу.

РОЗДІЛ 2. ІНСТИТУЦІЙНО-АНАЛІТИЧНИЙ ВИМІР ПОЛІТИКИ ЄС У СФЕРІ ЦИФРОВОЇ ДИПЛОМАТІЇ

2.1. Суб'єкти формування цифрової дипломатії Європейського Союзу

Інституційна архітектура формування та реалізації цифрової дипломатії Європейського Союзу відображає складну багаторівневу систему governance, характерну для політичної структури Союзу загалом, де повноваження розподілені між наднаціональними інституціями, міжурядовими органами та державами-членами, створюючи унікальну конфігурацію акторів з різним ступенем автономії, ресурсної забезпеченості та функціональної спеціалізації, що водночас генерує як синергетичний потенціал через мобілізацію різноманітної експертизи та ресурсів, так і координаційні виклики через множинність центрів прийняття рішень та можливу неузгодженість стратегічних пріоритетів. Розуміння специфіки інституційних суб'єктів цифрової дипломатії ЄС вимагає аналізу не лише формальних повноважень, закріплених у договорах та регламентах, але й практичної динаміки міжінституційної взаємодії, розподілу ресурсів, механізмів координації та неформальних патернів впливу, що формуються в процесі реальної діяльності цих інституцій у швидко еволюціонуючому цифровому дипломатичному просторі, де традиційні бюрократичні процедури часто стикаються з вимогами оперативності та гнучкості цифрового середовища.

Європейська служба зовнішніх дій посідає центральне місце в інституційній системі цифрової дипломатії ЄС як унікальна структура *sui generis*, створена Лісабонським договором для забезпечення когерентності та ефективності зовнішньої політики Союзу через об'єднання дипломатичних ресурсів інституцій ЄС та експертизи держав-членів у єдиній організаційній рамці під керівництвом Високого представника з питань зовнішньої політики та політики безпеки. Інституційна еволюція EEAS від її створення у 2010 році до сьогодення демонструє поступову адаптацію цієї служби до викликів цифрової епохи, що кульмінувало у створенні спеціалізованого підрозділу Digital Diplomacy Unit у структурі Strategic Communications and Information Analysis Division, який отримав мандат координувати цифрову дипломатичну діяльність

всієї мережі делегацій ЄС та забезпечувати стратегічне планування цифрової присутності Союзу в глобальному інформаційному просторі. Кармен та Заваттаро аналізують організаційну структуру EEAS крізь призму теорії інституційної адаптації, демонструючи, що створення Digital Diplomacy Unit стало відповіддю на зростаючий розрив між традиційними дипломатичними практиками та вимогами цифрового середовища, де швидкість реагування, візуальна комунікація та інтерактивність стають критичними факторами дипломатичної ефективності.

Функціональний мандат Digital Diplomacy Unit охоплює широкий спектр активностей від розробки стратегічних рамок цифрової комунікації та координації присутності EEAS у різних соціальних мережах до моніторингу та аналізу цифрового інформаційного простору, підготовки рекомендацій щодо цифрових кампаній та забезпечення навчання персоналу делегацій ЄС у сфері цифрової дипломатії, що відображає комплексне розуміння цифровізації дипломатії як процесу, який вимагає не лише технологічних інструментів, але й організаційної трансформації, розвитку нових компетенцій та культурних змін у дипломатичній практиці. Практична діяльність підрозділу включає управління офіційними акаунтами EEAS у провідних соціальних мережах, де станом на 2024 рік представництво охоплює платформи Twitter, Facebook, Instagram, LinkedIn та YouTube з загальною аудиторією понад п'ять мільйонів підписників, координацію цифрових кампаній з ключових питань зовнішньої політики ЄС від клімату та прав людини до міжнародної безпеки та підтримки партнерів, моніторинг глобального інформаційного простору для раннього виявлення дезінформаційних кампаній та інформаційних загроз європейським інтересам. Бйола та Менор наголошують, що ефективність Digital Diplomacy Unit значною мірою залежить від його здатності балансувати між централізованою координацією для забезпечення узгодженості повідомлень та децентралізованою гнучкістю, необхідною для адаптації комунікацій до специфіки різних регіональних та тематичних контекстів, що вимагає розробки складних систем внутрішньої комунікації та процедур узгодження між центральним офісом та мережею делегацій [21, с. 267-270].

Організаційна структура EEAS передбачає також функціонування регіональних Strategic Communications Task Forces, які забезпечують координацію стратегічних комунікацій та протидії дезінформації в специфічних географічних регіонах, де інформаційні загрози для європейських інтересів є особливо гострими, зокрема East StratCom Task Force для Східного сусідства та Росії, South Task Force для регіону Близького Сходу та Північної Африки, Western Balkans Task Force для країн Західних Балкан, що відображає визнання геополітичного виміру інформаційного протиборства та необхідності таргетованих регіональних стратегій цифрової дипломатії. Діяльність East StratCom Task Force, створеної у 2015 році як відповідь на російську дезінформаційну кампанію, стала найбільш видимим та контроверсійним елементом системи стратегічних комунікацій EEAS, що включає ведення платформи EUvsDisinfo для систематичного документування та спростування дезінформації, підтримку незалежних медіа у країнах Східного партнерства, проведення дослідницької та аналітичної роботи щодо наративів та методів інформаційного впливу. Горбатенко та Шедяков зазначають, що East StratCom демонструє еволюцію підходу ЄС до стратегічних комунікацій від pure defensive позиції спростування дезінформації до більш проактивного narrative engagement, що передбачає формування власних compelling наративів про європейську інтеграцію, демократичні цінності та переваги партнерства з ЄС [4, с. 156-159].

Європейська Комісія відіграє критично важливу роль у формуванні цифрової дипломатії ЄС через свої широкі повноваження у сферах внутрішнього ринку, цифрової економіки, регуляторної політики та міжнародної співпраці, де цифровий вимір набуває дедалі більшого значення для реалізації зовнішньополітичних цілей Союзу та просування його глобальних інтересів. Специфіка ролі Комісії полягає в тому, що вона поєднує функції законодавчої ініціативи, регуляторного органу та виконавчої інституції, що дозволяє їй впливати на цифрову дипломатію як через розробку нормативно-правової бази цифрового простору, так і через пряму реалізацію програм міжнародної цифрової співпраці, що створює синергію між внутрішньою та зовнішньою політикою у цифровій сфері. Генеральний директорат з питань комунікаційних

мереж, контенту та технологій (DG CONNECT) виступає ключовим актором формування зовнішнього виміру цифрової політики ЄС через координацію міжнародних цифрових партнерств, участь у багатосторонніх форумах з питань інтернет-управління, розробку програм цифрової допомоги третім країнам та просування європейських стандартів та норм у глобальному цифровому просторі. Матвієнко підкреслює, що DG CONNECT фактично перетворився на центр цифрової економічної дипломатії ЄС, де технічні стандарти, регуляторні рамки та цифрова інфраструктура стають інструментами геополітичного впливу та просування європейської моделі цифрового управління [10, с. 48-51].

Взаємодія між EEAS та Європейською Комісією у сфері цифрової дипломатії структурується через складну систему формальних та неформальних координаційних механізмів, що включають регулярні міжслужбові консультації, спільні робочі групи з ключових питань цифрової зовнішньої політики, координацію позицій у міжнародних форумах та узгодження комунікаційних кампаній, проте ця взаємодія не позбавлена інституційних напружень, зумовлених відмінностями в організаційних культурах, пріоритетах та підходах між дипломатичною службою та технократичним апаратом Комісії. Петренко аналізує динаміку міжінституційної координації крізь призму теорії інституційного раціонального вибору, демонструючи, що ефективність співпраці між EEAS та Комісією значною мірою залежить від персональних відносин між ключовими посадовцями, наявності спільних стратегічних інтересів у конкретних питаннях та механізмів вирішення конфліктів повноважень, що періодично виникають через розмитість меж між зовнішньою та внутрішньою політикою у цифровій сфері [14, с. 118-121].

Рада Європейського Союзу як головний міжурядовий орган, що визначає стратегічні напрямки політики Союзу та приймає ключові рішення у сфері зовнішньої політики та безпеки, формує загальну політичну рамку для цифрової дипломатії ЄС через схвалення стратегічних документів, надання мандатів для дипломатичних ініціатив та координацію позицій держав-членів з цифрових питань міжнародного порядку денного. Система робочих груп Ради, зокрема Working Party on Cyber Issues та Working Party on Information, охоплює різні

аспекти цифрової зовнішньої політики від кібербезпеки та кібердипломатії до стратегічних комунікацій та протидії дезінформації, забезпечуючи платформу для міждержавної координації національних підходів та вироблення спільних позицій ЄС у міжнародних переговорах з цифрових питань. Толстов зазначає, що консенсусний характер прийняття рішень у Раді створює виклики для оперативності та амбітності цифрової дипломатії ЄС, оскільки необхідність узгодження позицій двадцяти семи держав-членів з різними геополітичними пріоритетами, технологічними спроможностями та підходами до цифрових питань часто призводить до вибору найменшого спільного знаменника та розмивання радикальніших ініціатив [16, с. 162-165].

Європейський Парламент, хоча й не має прямих виконавчих повноважень у сфері зовнішньої політики, впливає на формування цифрової дипломатії ЄС через законодавчі функції в регулюванні цифрового простору, бюджетні повноваження щодо фінансування програм міжнародної цифрової співпраці, контрольні функції стосовно діяльності EEAS та Комісії та формування публічного дискурсу навколо цифрових питань міжнародної політики через резолюції, слухання та публічні дебати. Профільні комітети Парламенту, зокрема Committee on Foreign Affairs, Committee on Industry, Research and Energy та Subcommittee on Security and Defence, систематично розглядають питання цифрової зовнішньої політики, проводять експертні слухання, готують доповіді та рекомендації, що формують важливий елемент демократичного контролю та публічної легітимації цифрової дипломатії ЄС. Чекаленко та Воловик аргументують, що роль Парламенту в цифровій дипломатії ЄС не обмежується формальними інституційними функціями, а включає також символічний вимір як представника європейських громадян та європейських цінностей у дебатах про майбутнє глобального цифрового порядку, де парламентська дипломатія стає додатковим каналом просування європейських позицій [17, с. 21-23].

Держави-члени ЄС залишаються важливими суб'єктами формування цифрової дипломатії Союзу як через свою роль у прийнятті рішень в міждержавних інституціях ЄС, так і через власну національну цифрову дипломатичну діяльність, яка може як доповнювати та посилювати зусилля рівня

ЄС, так і створювати конкуренцію чи навіть суперечити загальноєвропейським пріоритетам залежно від ступеня узгодженості національних та європейських інтересів у конкретних питаннях. Гетерогенність держав-членів у цифровій дипломатичній спроможності, стратегічних пріоритетах та підходах до цифрових питань створює виклики для формування єдиної європейської лінії, де більші держави з розвиненими дипломатичними службами та значними ресурсами, такі як Франція, Німеччина або Швеція, часто ведуть власну активну цифрову дипломатію, що може затьмарювати присутність рівня ЄС у цифровому просторі. Яковюк наголошує на необхідності розробки механізмів забезпечення синергії між національним та європейським рівнями цифрової дипломатії через координацію повідомлень, обмін найкращими практиками, спільні цифрові кампанії та уникнення дублювання зусиль, що вимагає як формальних інституційних процедур, так і неформальної культури співпраці та солідарності [2, с. 97-100].

Спеціалізовані агенції та органи ЄС, включаючи Агенцію з кібербезпеки Європейського Союзу (ENISA), European Digital Innovation Hubs, EU Satellite Centre та інші технічні структури, забезпечують експертну та технологічну підтримку цифрової дипломатії через аналіз кіберзагроз, розробку технічних стандартів безпеки, надання даних супутникового спостереження для моніторингу міжнародних подій та інші форми технічної експертизи, що стають дедалі важливішими для ефективної цифрової дипломатичної діяльності в умовах зростаючої складності та технологічності міжнародних викликів. Камінський зазначає, що інтеграція технічної експертизи спеціалізованих агенцій у процес формування та реалізації цифрової дипломатії ЄС залишається неповною, оскільки існують організаційні бар'єри між технічними експертами та дипломатичними практиками, відмінності в інституційних культурах та недостатні механізми перекладу технічних знань у стратегічні дипломатичні рекомендації [6, с. 83-86].

Аналіз інституційної системи суб'єктів цифрової дипломатії ЄС виявляє парадоксальну ситуацію, де множинність акторів з різними повноваженнями, ресурсами та підходами створює як потенціал для комплексного та

багатовимірному підходу до цифрових викликів через мобілізацію різноманітної експертизи, так і ризики фрагментації, неузгодженості та неефективності через координаційні складнощі, інституційну конкуренцію та відсутність єдиного центру стратегічного керівництва цифровою дипломатією. Бебик та Головатий аргументують, що подолання цих викликів вимагає не стільки радикальної інституційної реформи, скільки розвитку горизонтальних механізмів координації, культури міжінституційної співпраці, чіткого розподілу функціональних ролей та створення платформ для регулярного діалогу між різними акторами цифрової дипломатії ЄС на всіх рівнях від стратегічного планування до операційної реалізації конкретних ініціатив [3, с. 208-211].

Узагальнюючи аналіз суб'єктів формування цифрової дипломатії Європейського Союзу, доцільно констатувати, що інституційна архітектура цієї сфери відображає загальну складність governance ЄС через поєднання наднаціональних та міжурядових елементів, множинність акторів з пересічними повноваженнями та необхідність постійної координації між різними рівнями та секторами політики, що створює як унікальні можливості для комплексного підходу, так і значні виклики для когерентності та ефективності. Центральна роль EEAS та її Digital Diplomacy Unit у координації цифрової дипломатичної діяльності поєднується з критично важливими функціями Європейської Комісії у сфері регуляторної дипломатії та міжнародної цифрової співпраці, стратегічним керівництвом Ради та демократичним контролем Парламенту, створюючи багатополосну систему, де ефективність залежить не стільки від формальних повноважень окремих інституцій, скільки від якості міжінституційної координації, особистих відносин між ключовими посадовцями та здатності виробляти спільне стратегічне бачення цифрової зовнішньої політики ЄС в умовах швидких технологічних змін та зростаючої геополітичної конкуренції. Розуміння цієї інституційної динаміки створює необхідну основу для аналізу конкретних інструментів реалізації цифрової дипломатії ЄС, через які абстрактні стратегічні цілі та інституційні мандати трансформуються в практичні дипломатичні дії, комунікативні кампанії та програми міжнародної співпраці, що становлять матеріальне втілення європейської цифрової

дипломатії в глобальному інформаційному просторі.

2.2. Інструменти реалізації цифрової дипломатії ЄС

Трансформація стратегічних цілей та інституційних мандатів у практичні результати цифрової дипломатії відбувається через систему конкретних інструментів, механізмів та програм, які становлять операційний рівень європейської цифрової зовнішньої політики та забезпечують матеріальне втілення абстрактних принципів у щоденній дипломатичній практиці взаємодії з глобальними аудиторіями, партнерськими державами та міжнародними організаціями. Інструментарій цифрової дипломатії ЄС характеризується різноманітністю форм, методів та технологій, що відображає комплексне розуміння цифровізації зовнішньої політики як багатовимірного процесу, який охоплює не лише комунікативні практики в соціальних мережах, але й технологічну співпрацю, розвиток спроможностей у третіх країнах, протидію дезінформації, кібердипломатію та інфраструктурні проекти, що створюють довгострокові умови для поширення європейської моделі цифрового управління. Аналіз цього інструментарію дозволяє виявити специфіку європейського підходу до цифрової дипломатії, що базується на поєднанні комунікативних, регуляторних, технологічних та розвиткових інструментів у цілісну систему впливу на глобальний цифровий порядок відповідно до цінностей та інтересів Європейського Союзу.

Механізми цифрових комунікацій становлять найбільш видиму та безпосередню форму цифрової дипломатичної активності ЄС, що охоплює систематичну присутність європейських інституцій у провідних соціальних мережах, розробку та поширення мультимедійного контенту, інтерактивну взаємодію з різноманітними аудиторіями та оперативне реагування на міжнародні події через цифрові канали комунікації. Стратегія присутності EEAS у соціальних мережах базується на багатоплатформному підході, що передбачає адаптацію контенту та комунікативних стратегій до специфіки різних платформ, їхніх аудиторій та функціональних можливостей, де Twitter використовується

переважно для оперативного реагування на події та офіційних заяв, Facebook для більш розгорнутих наративів та взаємодії з широкими аудиторіями, Instagram для візуальної комунікації та humanization дипломатії, LinkedIn для професійної аудиторії та policy-oriented контенту, а YouTube для довгоформатного відеоконтенту та документальних матеріалів про діяльність ЄС. Менор наголошує, що ефективність багатоплатформної стратегії залежить не від простої репродукції однакового контенту на різних платформах, а від розуміння унікальної комунікативної логіки кожної платформи та здатності створювати нативний контент, що резонує з очікуваннями та практиками користувачів конкретної соціальної мережі [61, с. 234-237].

Контент-стратегія цифрових комунікацій ЄС структурується навколо декількох тематичних pillar'ів, що відображають ключові пріоритети зовнішньої політики Союзу та прагнення формувати глобальні наративи з питань міжнародного порядку, прав людини, кліматичних змін, багатостороннього співробітництва та демократичних цінностей, водночас намагаючись персоналізувати та humanize європейську дипломатію через людські історії, візуальні наративи та емоційний резонанс, що створює виклик балансування між офіційним дипломатичним тоном та вимогами цифрового середовища до автентичності, неформальності та емоційності комунікації. Мультимедійний характер цифрового контенту EEAS включає широке використання візуальних елементів від інфографіки та фотографій до відеороликів та інтерактивних графіків, що відповідає візуально орієнтованій природі сучасного цифрового споживання інформації, де текстові повідомлення дедалі частіше виконують роль супроводу до візуальних наративів, а не навпаки. Литвин зазначає, що візуальна комунікація в цифровій дипломатії ЄС поступово еволюціонує від формальних офіційних фотографій та стандартизованої графіки до більш креативних, емоційних та narrative-driven візуальних форматів, що відображає усвідомлення необхідності конкурувати за увагу аудиторій у перенасиченому інформаційному середовищі [7, с. 37-39].

Платформні рішення для управління цифровою присутністю та координації комунікацій між численними акаунтами європейських інституцій та

делегацій ЄС у різних країнах становлять критично важливу технологічну інфраструктуру, що забезпечує можливість централізованого моніторингу, планування контенту, аналізу ефективності та оперативного реагування на події в режимі реального часу через єдину систему управління множинними соціальними мережами. EEAS використовує спеціалізовані платформи для social media management, які дозволяють координувати публікації, відстежувати згадки ЄС у цифровому просторі, аналізувати sentiment аудиторій, ідентифікувати emerging trends та потенційні кризи, що вимагають дипломатичного реагування, а також вимірювати performance різних типів контенту для continuous optimization комунікативних стратегій на основі data-driven підходу. Пашковська підкреслює, що технологічна інфраструктура цифрової дипломатії не є нейтральним інструментом, а активно формує можливості та обмеження дипломатичної практики через свої функціональні характеристики, інтерфейс користувача та вбудовані метрики успішності, що потенційно може призводити до надмірної орієнтації на кількісні показники engagement на шкоду якісним цілям дипломатичного впливу [12, с. 151-154].

Програма EUvsDisinfo становить флагманську ініціативу ЄС у сфері протидії дезінформації, що функціонує під егідою East StratCom Task Force та забезпечує систематичне документування, аналіз та спростування дезінформаційних наративів, спрямованих на підрив європейських інтересів та дискредитацію демократичних цінностей переважно у просторі Східного партнерства, але з поступовим розширенням географічного охоплення на інші регіони, де виявляються схожі патерни координованого інформаційного впливу. Методологія роботи EUvsDisinfo базується на чітких критеріях ідентифікації дезінформації, що включають фактичну неправдивість твердження, очевидність навмисного характеру поширення неправдивої інформації та потенціал шкоди суспільним інтересам, що відрізняє дезінформацію від помилок, неточностей чи легітимних відмінностей в інтерпретаціях подій, дозволяючи уникати обвинувачень у цензурі чи обмеженні свободи слова. Мартинов аналізує еволюцію підходу EUvsDisinfo від pure fact-checking моделі, зосередженої на спростуванні конкретних фейків, до більш комплексної стратегії, що включає

аналіз дезінформаційних наративів, виявлення координованих кампаній, дослідження інфраструктури поширення дезінформації та розробку позитивних контрнарративів, здатних конкурувати з дезінформацією за увагу та довіру аудиторій [9, с. 70-72].

База даних EUvsDisinfo станом на початок 2024 року містить понад шістнадцять тисяч випадків дезінформації, систематизованих за тематикою, географією, джерелами та наративами, що становить унікальний емпіричний ресурс для дослідження patterns та evolution дезінформаційних кампаній, дозволяючи виявляти recurring наративи, адаптацію тактик маніпуляції до змін медіа-ландшафту та координацію між різними каналами поширення дезінформації. Публічна доступність цієї бази даних через веб-платформу euvsdisinfo.eu забезпечує прозорість методології, можливість верифікації висновків та створює ресурс для журналістів, дослідників, громадянського суспільства та широкої публіки, що посилює ефект протидії дезінформації через crowd-sourced vigilance та суспільну resilience до маніпулятивних наративів. Романюк зазначає, що публічна дипломатія протидії дезінформації через EUvsDisinfo виконує подвійну функцію, де спростування конкретних фейків поєднується з більш стратегічною метою формування critical media literacy та скептицизму стосовно інформації з ненадійних джерел, що становить форму когнітивної вакцинації аудиторій проти майбутніх спроб маніпуляції [15, с. 105-107].

Ініціатива Digital4Development втілює підхід ЄС до використання цифрової співпраці як інструменту зовнішньої політики та розвиткової допомоги, що спрямована на підтримку цифрової трансформації країн-партнерів через передачу технологій, розбудову capacity, підтримку регуляторних реформ та інвестиції в цифрову інфраструктуру відповідно до європейських стандартів та принципів human-centric цифровізації. Програма охоплює широкий спектр активностей від технічної допомоги у розробці національних цифрових стратегій та регуляторних рамок до фінансування проєктів розбудови широкосмугового доступу в сільських районах, підтримки цифрових стартапів, навчання цифровим навичкам та сприяння електронному урядуванню, що відображає комплексне

розуміння цифрового розвитку як multidimensional процесу, який вимагає синхронізованих втручань на рівні інфраструктури, регулювання, освіти та інновацій. Горбатенко та Шедяков аргументують, що Digital4Development являє собою форму структурної влади ЄС через формування траєкторій цифрового розвитку країн-партнерів у напрямку, сумісному з європейською моделлю, створюючи довгострокові умови для alignment регуляторних підходів, технологічних стандартів та нормативних рамок [4, с. 201-204].

Географічний фокус Digital4Development включає країни Африки, Карибського басейну та Тихого океану, Східного та Південного сусідства, Азії та Латинської Америки, з особливим акцентом на найменш розвинених країнах та fragile states, де цифрова трансформація може мати найбільший трансформативний вплив на економічний розвиток, соціальну інклюзію та демократичне governance, водночас створюючи виклики через обмежену інституційну спроможність, недостатню інфраструктуру та ризики цифрової колонізації через залежність від іноземних технологій та платформ. Програма включає також компонент digital diplomacy capacity building для дипломатичних служб країн-партнерів, що передбачає навчання, обмін досвідом та технічну підтримку розвитку їхніх власних спроможностей цифрової дипломатії, що відображає визнання важливості багатостороннього підходу до формування глобального цифрового порядку та необхідності empowerment партнерів як суб'єктів, а не лише об'єктів європейської цифрової дипломатії. Кобзар підкреслює, що успішність Digital4Development залежить від здатності ЄС уникати неоколоніальних патернів технологічної допомоги та забезпечувати genuine partnership, що поважає пріоритети та контекстуальну специфіку країн-партнерів, дозволяючи їм робити власні вибори щодо моделей цифрового розвитку в рамках pluralistic глобального цифрового порядку [9, с. 75-77].

East StratCom Task Force як спеціалізований інструмент стратегічних комунікацій у Східному сусідстві поєднує defensive функції протидії дезінформації з proactive формуванням позитивних наративів про ЄС, його політику Східного партнерства та переваги європейської інтеграції для країн регіону, що вимагає тонкого балансування між критикою деструктивного

інформаційного впливу та *constructive engagement* з локальними аудиторіями на основі їхніх реальних потреб, прагнень та *cultural codes*. Діяльність Task Force включає не лише моніторинг та спростування дезінформації через платформу EUvsDisinfo, але й підтримку незалежних медіа у країнах Східного партнерства через грантові програми, технічну допомогу та *capacity building*, що спрямовані на зміцнення *media ecosystem* та створення альтернативних джерел якісної інформації, здатних конкурувати з дезінформаційними *outlets* за аудиторію. Толстов зазначає, що підтримка незалежних медіа становить стратегічно важливіший інструмент довгострокової *resilience* до дезінформації порівняно з *reactive fact-checking*, оскільки створює структурні умови для функціонування вільного та плюралістичного медіа-простору, проте вимагає терпіння та тривалих інвестицій без гарантії швидких вимірюваних результатів [16, с. 167-169].

Комунікативна стратегія East StratCom базується на розробці та просуванні *affirmative narratives* про європейську інтеграцію, демократичні цінності, економічні можливості асоціації з ЄС та *success stories* реформ у країнах Східного партнерства, що мають резонувати з локальними аудиторіями через *authentic stories*, *relatable characters* та *emotional appeal*, уникаючи абстрактних бюрократичних формулювань та *eurocentrism*, що часто характеризує офіційну комунікацію європейських інституцій. Виклик полягає в тому, що позитивні наративи про повільні інституційні реформи та довгострокові структурні трансформації важко конкурують за увагу з емоційно зарядженими конспірологічними та апокаліптичними наративами дезінформації, що експлуатують страхи, обурення та ностальгію, володіючи *significant advantage* в *attention economy* цифрового інформаційного простору. Матвієнко аналізує спроби East StratCom адаптувати техніки *emotional storytelling* та *visual communication* для *affirmative narratives*, що включають використання відеосвідчень реальних людей, чиє життя покращилося завдяки реформам підтримуваним ЄС, інфографіку про *concrete benefits* європейської співпраці та *humanization* європейської присутності через особисті історії представників ЄС у регіоні [10, с. 51-53].

Ініціатива Global Gateway, запущена у 2021 році як відповідь ЄС на китайську Ініціативу Пояса та Шляху, становить амбітну програму інфраструктурних інвестицій у країнах-партнерах з особливим акцентом на цифровій інфраструктурі, що включає підтримку розбудови широкосмугових мереж, підводних кабелів, дата-центрів, цифрових платформ та інших елементів цифрової connectivity, необхідної для participation у глобальній цифровій економіці та забезпечення digital sovereignty країн-партнерів. Стратегічна логіка Global Gateway базується на позиціонуванні ЄС як альтернативного партнера для інфраструктурного розвитку, що пропонує values-based підхід з акцентом на фінансову стійкість проєктів, екологічну сталість, високі соціальні та трудові стандарти, прозорість procurement та local ownership, що контрастує з debt-trap diplomacy та непрозорими практиками, часто асоційованими з китайськими інфраструктурними проєктами. Сагайдак та Ісаєнко стверджують, що Global Gateway являє собою спробу ЄС перетворити свою нормативну силу та фінансову потужність у геополітичний вплив через інфраструктурну дипломатію, де інвестиції в цифрову connectivity стають інструментом формування довгострокових партнерств та alignment інтересів відповідно до європейської моделі globalization [14с. 238-240].

Цифровий компонент Global Gateway включає конкретні показові (флагманські) проєкти, такі як розбудова безпечної широкосмугової інфраструктури у країнах Африки, підтримка підводних кабельних систем для покращення зв'язності міжконтинентами, інвестиції в зелені дата-центри на основі відновлюваної енергії та розвиток цифрових навичок через освітні програми та центри цифрових інновацій, що створюють комплексну екосистему цифрової трансформації в країнах-партнерах. Фінансування Global Gateway передбачає мобілізацію як публічних ресурсів через бюджет ЄС, Європейський інвестиційний банк та фінансові інструменти держав-членів, так і приватних інвестицій через гарантійні механізми та інструменти змішаного фінансування (blending), що дозволяє досягти значного ефекту фінансового важеля та залучити комерційний капітал до проєктів, які мають як розвитковий, так і комерційний потенціал. Троян та Гончарук наголошують, що реалізація амбіцій Global

Gateway вимагає від ЄС подолання традиційних обмежень європейської зовнішньої політики, включаючи повільність процедур прийняття рішень, фрагментацію між різними фінансовими інструментами та інституціями, недостатню координацію з державами-членами та обмежену присутність на місцях для ефективної реалізації проєктів та моніторингу [24, с. 61–63].

Кібердипломатичний інструментарій ЄС охоплює широкий спектр механізмів – від участі у багатосторонніх переговорах з питань кібербезпеки та інтернет-урядування до двосторонніх кібердіалогів з ключовими партнерами, від розробки та просування міжнародних норм відповідальної поведінки держав у кіберпросторі до застосування цільових рестриктивних заходів проти акторів, відповідальних за шкідливі кібероперації. Це відображає комплексний підхід до кібербезпеки як багатовимірного виклику, що вимагає поєднання технічних, правових, дипломатичних та політичних інструментів. Режим кібердипломатичних санкцій ЄС, запроваджений у 2017 році та посилений у наступні роки, дозволяє накладати цільові обмежувальні заходи проти фізичних осіб та організацій, відповідальних за кібератаки, що порушують територіальну цілісність, суверенітет чи незалежність держав, спричиняють значні економічні втрати чи становлять загрозу критичній інфраструктурі. Це є формою дипломатичного примусу у цифровому просторі та сигналізує про неприйнятність певних типів кіберповедінки. Камінський аналізує виклики ефективної імплементації кібердипломатичних санкцій, що включають труднощі технічної атрибуції кібератак із достатнім рівнем упевненості для публічного приписування відповідальності, політичну чутливість публічного звинувачення держав у кіберагресії та обмежений стримувальний ефект санкцій щодо акторів, які вже перебувають під дією інших санкційних режимів або працюють з територій, недоступних для європейської юрисдикції [6, с. 88–90].

Узагальнюючи аналіз інструментів реалізації цифрової дипломатії ЄС, доцільно констатувати, що європейський підхід характеризується різноманітністю та комплексністю інструментарію, який охоплює весь спектр – від безпосередньої цифрової комунікації в соціальних мережах до довгострокових інфраструктурних інвестицій, від протидії дезінформації до

нарощування потенціалу (capacity building) у країнах-партнерах, від регуляторної дипломатії до кібербезпекових санкцій. Це відображає розуміння цифровізації зовнішньої політики як багатовимірного процесу, який не може бути зведений до однієї форми активності чи одного типу інструментів. Специфіка європейського інструментарію полягає в акценті на нормативних, регуляторних та інструментах нарощування спроможностей, що доповнюють комунікативні засоби та відображають прагнення ЄС формувати структурні умови глобального цифрового порядку відповідно до європейських цінностей і стандартів, компенсуючи обмеження військової сили та технологічного лідерства за допомогою регуляторної потуги та співпраці у сфері розвитку як форм довгострокового впливу. Водночас виклики ефективної імплементації цих інструментів, пов'язані з бюрократичними процедурами, обмеженими ресурсами, прогалинами координації між різними програмами та інституціями та конкуренцією з геополітичними суперниками, що володіють потужнішими ресурсами та меншими нормативними обмеженнями, вимагають постійного вдосконалення підходів і адаптації інструментарію до динамічних змін технологічного та геополітичного середовища. Розуміння можливостей та обмежень цього інструментарію створює основу для аналізу практичних результатів цифрової дипломатії ЄС у глобальному та регіональному вимірах, що дозволяє оцінити ефективність європейського підходу на основі конкретних кейсів співпраці з партнерами та його впливу на формування цифрового глобального порядку.

2.3. Цифрова дипломатія ЄС у глобальному та регіональному вимірах

Оцінка практичних результатів цифрової дипломатії Європейського Союзу вимагає переходу від аналізу інституційних структур та інструментів до емпіричного дослідження конкретних досягнень, впливів та ефектів європейської цифрової зовнішньої політики у різних географічних контекстах та тематичних сферах, що дозволяє верифікувати відповідність між декларованими амбіціями, стратегічними документами та реальними результатами

дипломатичної активності у цифровому просторі. Методологічна складність вимірювання ефективності цифрової дипломатії полягає в тому, що багато її цілей мають довгостроковий та якісний характер, зокрема формування міжнародних норм, зміну сприйняття та установок, розбудову партнерств і створення сприятливого середовища для просування європейських цінностей, що важко піддаються простій квантифікації через метрики соціальних мереж чи підрахунок дипломатичних угод. Це вимагає більш комплексних та вдосконалених підходів до оцінювання, які поєднують кількісні індикатори з якісним аналізом процесів, контекстів та причинно-наслідкових механізмів. Водночас конкретні приклади співпраці з державами-партнерами, участь у формуванні глобальних стандартів кібербезпеки, результати протидії дезінформації та вплив на цифрову трансформацію третіх країн дають змогу емпірично оцінити реальний вплив європейської цифрової дипломатії на міжнародні процеси та верифікувати гіпотези про роль ЄС як глобального формувальника цифрового порядку.

Трансатлантичне цифрове партнерство між Європейським Союзом та Сполученими Штатами Америки становить стратегічно найважливіший вимір цифрової дипломатії ЄС, оскільки попри існуючі регуляторні відмінності та комерційні суперечності між двома найбільшими демократичними економіками світу, їхня співпраця є критично важливою для формування глобального цифрового порядку, заснованого на демократичних цінностях, верховенстві права та захисті прав людини в умовах зростаючого виклику з боку авторитарних режимів, що просувають альтернативні моделі цифрового управління на основі державного контролю та технологічного суверенітету. Створення Ради з торгівлі та технологій (Trade and Technology Council, TTC) у червні 2021 року ознаменувало якісний прорив у трансатлантичній цифровій співпраці через інституціоналізацію регулярного діалогу на високому рівні з ключових питань технологічної політики, торгівлі та безпеки, що об'єднує десять робочих груп із тематики – від штучного інтелекту та управління даними до експортного контролю технологій подвійного призначення та перевірки іноземних інвестицій у критичні сектори. Бйола та Холмс аргументують, що TTC є спробою

інституціоналізувати узгодження трансатлантичних підходів до цифрового регулювання та технологічних стандартів з метою формування критичної маси нормативної влади, здатної конкурувати з китайською моделлю та встановлювати фактичні глобальні правила через «брюссельсько-вашингтонський ефект», аналогічний до «брюссельського ефекту» попередніх десятиліть [21, с. 378–381].

Конкретні досягнення ТТС включають узгодження підходів до регулювання штучного інтелекту через спільні принципи довірчого (надійного) штучного інтелекту, координацію позицій щодо безпеки ланцюгів постачання напівпровідників для зменшення залежності від авторитарних постачальників критичних компонентів, розробку механізмів співпраці у сфері перевірки іноземних інвестицій у чутливі технології для захисту від технологічного трансферу до геополітичних суперників та спільні ініціативи з підтримки свободи Інтернету та протидії цифровому авторитаризму у третіх країнах. Це демонструє здатність подолати традиційні трансатлантичні суперечності щодо захисту даних та антимонопольного регулювання заради стратегічного узгодження у протистоянні спільним викликам. Водночас залишаються значні розбіжності щодо екстратериторіального застосування американського законодавства, доступу американських спецслужб до даних європейських громадян, позицій великих американських технологічних корпорацій на європейському ринку та компромісів між захистом даних і вимогами національної безпеки, що створює постійне напруження в трансатлантичних відносинах та потребує постійної дипломатичної взаємодії для управління цими суперечностями. Менор зазначає, що ТТС демонструє еволюцію від «гри з нульовою сумою» між європейською та американською моделями цифрового регулювання до більш прагматичного визнання необхідності співпраці та зближення принаймні у базових питаннях задля збереження ліберально-демократичної моделі цифрового порядку перед обличчям авторитарного технологічного виклику [61, с. 389–392].

Цифрова співпраця між ЄС та Японією втілює модель партнерства між економіками з високим рівнем технологічного розвитку та спільними

демократичними цінностями, які прагнуть координувати підходи до цифрового регулювання, кібербезпеки та технологічних стандартів для формування альтернативи китайськоцентричній моделі цифровізації в Індо-Тихоокеанському регіоні та у глобальному вимірі. Цифрове партнерство ЄС–Японія (EU–Japan Digital Partnership), оформлене у 2022 році, структурує співпрацю навколо чотирьох напрямів, що включають узгодження регуляторних підходів до новітніх технологій, співпрацю у сфері кібербезпеки та захисту критичної інфраструктури, спільні ініціативи з просування концепції «вільного потоку даних із довірою» у багатосторонніх форумах та співробітництво у розробці міжнародних стандартів для 5G, Інтернету речей та інших передових технологій. Це відображає прагнення створити коаліцію демократичних, технологічно розвинених економік, здатних задавати стандарти. Горбатенко та Шедяков підкреслюють, що цифрове партнерство ЄС–Японія має особливе значення завдяки ролі Японії як технологічного лідера та впливового актора в Азійсько-Тихоокеанському регіоні, де її партнерство з ЄС може врівноважити китайський вплив і запропонувати країнам регіону альтернативну модель цифрового розвитку, засновану на відкритості, взаємодії та повазі до прав людини [4, с. 234–237].

Практичні результати цифрового партнерства ЄС–Японія включають угоди про взаємне визнання рамок захисту даних, які полегшують транскордонні потоки даних між двома юрисдикціями, водночас зберігаючи високі стандарти захисту приватності; спільні дослідницькі проєкти зі штучного інтелекту та квантових обчислень у межах програми Horizon Europe та японських схем фінансування досліджень; координацію позицій у міжнародних організаціях із питань інтернет-урядування та норм кібербезпеки; а також двосторонні кібердіалоги для обміну розвідданими щодо кіберзагроз і найкращими практиками захисту критичної інфраструктури. Особливої уваги заслуговує співпраця у просуванні концепції «вільного потоку даних із довірою» (Data Free Flow with Trust) у G7 та інших багатосторонніх форумах, що прагне узгодити європейський акцент на захисті даних з японським та американським пріоритетом сприяння транскордонним потокам даних для економічної

ефективності. Такий підхід пропонує проміжний варіант між «протекціонізмом даних» та регуляторною «гонкою донизу» через встановлення високих базових стандартів із забезпеченням взаємосумісності регуляторних режимів. Кобзар аналізує цифрове партнерство ЄС–Японія як приклад успішної мінілатеральної дипломатії, коли двостороння співпраця між партнерами зі спільними поглядами створює підґрунтя для ширших коаліцій та вироблення норм у глобальному масштабі, демонструючи альтернативу застарілим багатостороннім інституціям, що потерпають від паралічу через геополітичні розколи [8, с. 79–81].

Цифрова дипломатія ЄС щодо України набула особливого значення після повномасштабного російського вторгнення у лютому 2022 року, коли інформаційний вимір конфлікту став критично важливим компонентом гібридної війни, а цифрова стійкість України перетворилася на стратегічний пріоритет для європейської безпеки та підтримки опору українського народу проти агресії. Підтримка ЄС охоплює широкий спектр дій: від протидії російській дезінформації через скоординоване спростування неправдивих повідомлень і посилення поширення української позиції до технічної допомоги у захисті критичної цифрової інфраструктури від кібератак; від фінансування незалежних українських медіа до нарощування спроможностей українських структур стратегічних комунікацій, що відображає комплексне розуміння цифрового виміру конфлікту як багатогранного виклику, який вимагає інтегрованої відповіді. Матвієнко підкреслює, що масштаб і інтенсивність російських кібератак та дезінформаційних кампаній проти України перетворили країну на «передову цифрової битви», де відпрацьовуються тактики й технології гібридної війни, які можуть бути згодом застосовані проти інших європейських цілей. Це робить підтримку цифрової стійкості України питанням не лише солідарності, а й превентивного самозахисту європейської безпекової спільноти [10, с. 54–56].

Конкретні форми цифрової підтримки України з боку ЄС включають розгортання команд швидкого кіберреагування ЄС (EU Cyber Rapid Response Teams) для надання технічної експертизи у відбитті та відновленні після масштабних кібератак на критичну інфраструктуру; фінансування через

програми Східного партнерства проєктів зі створення безпечних систем зв'язку для українського уряду та військових структур; координацію з технологічними компаніями для запобігання використанню їхніх платформ для російської пропаганди та дезінформаційних кампаній; підтримку ініціатив із фактчекінгу та незалежних медіа через гранти й технічну допомогу; а також адвокацію в міжнародних форумах для викриття російських інформаційних операцій і мобілізації міжнародної підтримки України в інформаційному просторі. Група East StratCom Task Force значно розширила охоплення України у своєму моніторингу дезінформації, систематично документуючи російські наративи та тактики дезінформації, що застосовуються як проти України, так і для підриву європейської підтримки українського опору, формуючи доказову базу для дипломатичних демаршів, санкційних рішень та кампаній публічного викриття. Петренко зазначає, що інтенсивність цифрової підтримки України з боку ЄС після повномасштабного вторгнення демонструє здатність європейської цифрової дипломатії до швидкого масштабування та адаптації у кризових ситуаціях, хоча також виявляє структурні обмеження у вигляді бюрократичних процедур, нестачі фінансування та координаційних труднощів між різними інструментами ЄС та двосторонньою допомогою держав-членів [13, с. 123–126].

Довгостроковий вимір цифрової співпраці ЄС–Україна охоплює підтримку цифрової трансформації України в контексті європейської інтеграції через гармонізацію регуляторних рамок із правовими нормами ЄС у цифровій сфері, включно із захистом даних, кібербезпекою, електронними комунікаціями та електронною комерцією. Це є частиною ширшого процесу наближення в межах Угоди про асоціацію та статусу кандидата на вступ до ЄС. Програма Digital4Development забезпечує фінансування та технічну експертизу для модернізації цифрової інфраструктури, розвитку цифрових навичок, підтримки ІТ-сектору та впровадження рішень електронного врядування, які мають трансформаційний потенціал для економічного розвитку та покращення надання публічних послуг у контексті післявоєнної відбудови, де цифрові технології можуть прискорювати процеси відновлення та допомагати «перестрибнути» традиційні етапи розвитку. Литвин аргументує, що цифрова співпраця стала

одним із найбільш динамічних та успішних вимірів відносин між ЄС та Україною, де прогрес у цифровій трансформації може слугувати демонстраційним ефектом переваг європейської інтеграції та створювати імпульс для реформ в інших секторах, використовуючи відносну відкритість українського суспільства до цифрових інновацій і сильний ІТ-сектор як порівняльні переваги [7, с. 41–43].

Роль ЄС у протидії дезінформації на глобальному рівні виходить за межі двосторонніх партнерств і включає лідерство в розробці міжнародних норм, стандартів та механізмів протидії іноземним інформаційним маніпуляціям та втручанням (foreign information manipulation and interference, FIMI) через багатосторонні форуми та органи зі встановлення стандартів. Це спрямовано на інституціоналізацію визначень, таксономій та рамок реагування для колективного захисту від систематичних дезінформаційних кампаній, які підривають демократичні процеси та суспільну згуртованість. Кодекс практики ЄС щодо дезінформації, започаткований у 2018 році та посилений у 2022 році, став новаторською саморегуляторною рамкою, що встановлює зобов'язання великих цифрових платформ щодо прозорості політичної реклами, маркування ботів, демонетизації дезінформації, співпраці з фактчекерами та підвищення спроможності користувачів через вдосконалені алгоритми та політики модерації контенту. Він слугує моделлю для аналогічних ініціатив в інших юрисдикціях і демонструє регуляторну силу ЄС у формуванні глобального цифрового врядування завдяки важелю великого внутрішнього ринку. Мартинов підкреслює, що еволюція від добровільного Кодексу до більш обов'язкових вимог у межах Digital Services Act демонструє процес навчання та поступове посилення регуляторного підходу ЄС у відповідь на недостатнє виконання платформами своїх зобов'язань та тривалі виклики у дезінформаційній екосистемі, що потребує поєднання інструментів «твердого» та «м'якого» права для ефективного врядування цифрових платформ [9, с. 73–75].

Адвокація ЄС у міжнародних форумах, зокрема в ООН, ОБСЄ, Раді Європи та інших багатосторонніх майданчиках, спрямована на просування комплексного підходу до протидії дезінформації, який поєднує імперативи

безпеки з основоположними правами на свободу вираження поглядів, медійнуpluralism та доступ до інформації, уникаючи авторитарних моделей цензури та державного контролю над інформаційними потоками під приводом боротьби з фейковими новинами. Європейська служба зовнішніх дій координує позиції держав-членів ЄС і здійснює лобіювання ухвалення резолюцій, декларацій та планів дій, які визнають загрозу іноземних інформаційних маніпуляцій, закріплюють норми відповідальної поведінки держав в інформаційному просторі та просувають прозорість, медіаграмотність і підтримку незалежної журналістики як структурні засоби зменшення вразливості до дезінформації. Романюк аналізує напруженість між різними підходами членів міжнародної спільноти, де ЄС виступає за модель, засновану на правах людини, авторитарні режими прагнуть використати порядок денний боротьби з дезінформацією для легітимізації цензури та контролю, а США наголошують на саморегуляції платформ і проблематиці, пов'язаній з Першою поправкою. Це ускладнює вироблення по-справжньому універсальних норм і рамок, змушуючи ЄС вибудовувати коаліції з демократичними країнами-однодумцями для створення критичної маси нормативного впливу [15, с. 108–110].

Формування стандартів кібербезпеки становить ще один критично важливий вимір практичних результатів цифрової дипломатії ЄС, у межах якого Союз прагне поєднати внутрішню регуляторну гармонізацію через директиви та регламенти з зовнішнім просуванням європейських підходів та стандартів у двосторонньому й багатосторонньому контекстах. Оновлена Директива NIS2, яка модернізує європейську систему мережевої та інформаційної безпеки, встановлює високі вимоги до кіберзахисту для критичної інфраструктури, основних послуг і постачальників цифрових сервісів. Через «брюссельський ефект» та вимоги доступу до ринку ЄС ця директива стимулює дотримання стандартів також і неєвропейськими компаніями, які працюють на європейському ринку або надають послуги європейським клієнтам, фактично поширюючи європейські правила та практики за межі Союзу. Як підкреслює Толстов [16, с. 170–172], саме регуляторна дипломатія у сфері кібербезпеки

дозволяє ЄС використовувати економічні важелі для впливу на глобальні практики попри відсутність військової потужності чи технологічної домінації. Це, у свою чергу, перетворює внутрішні стандарти ЄС на дієвий геополітичний інструмент, а економічну взаємозалежність – на засіб формування більш безпечного та стійкого глобального кіберпростору, що відповідає довгостроковим інтересам Євросоюзу.

Участь ЄС у формуванні міжнародних норм кібербезпеки через Групу урядових експертів ООН (UN GGE) та Робочу групу відкритого складу (OEWG) спрямована на кодифікацію правил відповідальної поведінки держав у кіберпросторі, включно із заборонаю атак на критичну цивільну інфраструктуру, підвищенням прозорості процедур розкриття вразливостей, посиленням співпраці в протидії кіберзлочинності та утвердженням поваги до прав людини онлайн. Попри те, що механізми виконання цих норм залишаються слабкими через відсутність обов'язкового міжнародного договору, вони створюють базу для формування глобального режиму підзвітності та стримування шкідливих кібероперацій. У цьому контексті «Кібердипломатичний інструментарій ЄС», який включає дипломатичні демарші, публічне приписування відповідальності та застосування обмежувальних заходів, демонструє готовність Союзу накладати політичні й економічні витрати на акторів, що порушують усталені норми. Як зазначає Камінський [6, с. 91–93], ефективність цього підходу залежить від достовірності технічної атрибуції, узгодженості позицій держав-членів та координації з партнерами-однодумцями. У підсумку поєднання нормативної діяльності, дипломатичного тиску та партнерських механізмів дозволяє ЄС посилювати свій вплив у глобальній кіберполітиці та просувати більш відповідальну та безпечну модель міжнародного кіберпростору.

Нарощування спроможностей (capacity building) у сфері кібербезпеки для країн-партнерів є важливим доповненням до регуляторних та дипломатичних інструментів, оскільки дає змогу усувати структурні вразливості та формувати місцеву стійкість до кіберзагроз. Це приносить вигоду не лише країнам-партнерам, а й самому Європейському Союзу, зменшуючи ризики поширення кіберінцидентів та сприяючи створенню безпечнішого глобального

кіберпростору. Програми ЄС із нарощування кіберспроможностей забезпечують технічну допомогу, навчання, обладнання та експертну підтримку для країн Східного партнерства, Західних Балкан, Африки та інших регіонів з метою посилення національних систем кібербезпеки, створення команд реагування на комп'ютерні надзвичайні події (CERT), розроблення стратегій і законодавства у сфері кіберзахисту, а також підготовки фахівців із кібероборони та реагування на інциденти. Як підкреслює Пашковська [12, с. 156–158], кіберспроможнісна підтримка має не лише технічний вимір, а й нормативний, оскільки передбачає передання європейських цінностей і підходів до поєднання безпеки та прав людини, просування багатостейкхолдерних моделей врядування та зміцнення демократичних інституцій перед гібридними загрозами. У підсумку така діяльність стає невід'ємною частиною ширшої стратегії цифрової дипломатії ЄС, спрямованої на формування більш передбачуваного та стабільного глобального цифрового порядку.

Регіональний вимір практичних результатів цифрової дипломатії ЄС демонструє диференційовані підходи та різний рівень успішності залежно від географічного контексту, політичної динаміки та готовності місцевих акторів до взаємодії з ЄС. Країни Східного партнерства загалом демонструють високий рівень співпраці та зацікавленість у наближенні до цифрових стандартів ЄС; держави Західних Балкан прагнуть прискорити цифрову трансформацію в рамках підготовки до вступу в ЄС; африканські партнери все частіше розглядають підтримку Євросоюзу як можливість розвинути власні цифрові екосистеми, уникаючи залежності від недемократичних постачальників технологій; тоді як азійські та латиноамериканські контексти характеризуються складнішою динамікою суперництва зовнішніх впливів і різноманіттям політичних систем. Бебик та Головатий [3, с. 213–216] аналізують ці регіональні відмінності через призму контекстуальних факторів — історичних зв'язків, економічної взаємозалежності, типу політичного режиму, рівня технологічного розвитку та присутності зовнішніх конкурентних акторів — що робить неможливими універсальні підходи та потребує адаптованих рішень. У підсумку найбільш ефективною є стратегія, що ґрунтується на врахуванні місцевої

специфіки, підтримці локальної відповідальності, культурній чутливості та довгостроковій залученості, а не на прагненні швидких результатів, що забезпечує реалістичність і сталість впливу цифрової дипломатії ЄС.

Узагальнюючи аналіз практичних результатів цифрової дипломатії ЄС, доцільно констатувати, що Європейський Союз досяг відчутних успіхів у формуванні партнерств із ключовими демократичними союзниками, просуванні регуляторних стандартів і норм у глобальному цифровому просторі, підтримці цифрової стійкості країн-партнерів перед гібридними загрозами та утвердженні себе як впливового учасника дискусій щодо майбутнього глобального цифрового порядку. Це демонструє здатність ЄС трансформувати свою регуляторну потужність, економічні важелі та нормативну привабливість у реальний дипломатичний вплив навіть за відсутності військової сили чи технологічної домінації, характерних для традиційних великих держав. Водночас ЄС стикається зі значними викликами у вигляді обмежених ресурсів порівняно з геополітичними конкурентами, повільних процедур ухвалення рішень, притаманних інституційній архітектурі Союзу, розривів між амбітними стратегічними документами та їхньою операційною реалізацією, а також труднощів координації між загальноєвропейським рівнем і державами-членами. До цього додається фундаментальна напруга між ціннісним підходом ЄС та реалістичною логікою боротьби за вплив з авторитарними режимами, які не обмежені подібними нормативними зобов'язаннями. Оцінювання ефективності цифрової дипломатії потребує реалістичного розуміння того, що ця сфера є за своєю суттю довгостроковою діяльністю, де структурні зміни в інституційних рамках, регуляторних середовищах та нормативних контекстах часто є більш суттєвими, ніж миттєві видимі результати. Порівняльні переваги ЄС полягають не у швидких жестах чи миттєвих реакціях, а у послідовному інституційному розбудовуванні, формуванні стандартів і створенні довготривалих партнерств, заснованих на спільних цінностях та взаємній зацікавленості. Саме така стратегія, що передбачає тривалу відданість та стратегічну терплячість, забезпечує найбільш сталі й глибокі результати для глобального цифрового порядку.

Висновки до розділу 2

Проведене дослідження інституційно-аналітичного виміру політики Європейського Союзу у сфері цифрової дипломатії свідчить, що ЄС сформував унікальну модель цифрової зовнішньої політики, яка значно відрізняється від підходів національних держав. Її специфіка полягає у багаторівневій архітектурі управління, поєднанні наднаціональних і міжурядових елементів та комбінуванні регуляторних, комунікативних і розвиткових інструментів. Ця модель відображає не просто адаптацію дипломатії до цифрової епохи, а трансформацію самої логіки зовнішньополітичного впливу, коли економічна вага внутрішнього ринку та нормативна спроможність Союзу перетворюються на геополітичні інструменти через поширення стандартів і норм за межі ЄС.

Аналіз суб'єктної структури цифрової дипломатії демонструє подвійність: інституційна множинність акторів одночасно посилює ЄС через різноманіття експертизи та ресурсів і створює координаційні труднощі, що загрожують фрагментацією зовнішньополітичної позиції. Європейська служба зовнішніх дій, формально відповідальна за координацію, діє в умовах напруженого розподілу компетенцій із Європейською Комісією. Це створює не стільки дисфункціональність, скільки специфічну продуктивну невизначеність, яка дозволяє ситуативно використовувати різні інструменти залежно від контексту. Успішність цифрової дипломатії в таких умовах визначається не стільки бюрократичною узгодженістю, скільки здатністю до прагматичної координації та стратегічної гнучкості.

Особливе значення має діяльність Підрозділу цифрової дипломатії в структурі Європейської служби зовнішніх дій, який виступає насамперед координаційним центром. Його роль полягає у забезпеченні горизонтальної взаємодії між підрозділами, делегаціями та іншими інституціями, обміні практиками та підтримці мережевої форми співпраці. Така організаційна логіка відповідає децентралізованій природі цифрового середовища й демонструє інституційне навчання ЄС, який відмовляється від жорсткої централізації та натомість формує механізми узгодження дій численних учасників.

Інструментарій цифрової дипломатії ЄС інтегрує три взаємодоповнюючі

підходи: комунікативну дипломатію через соціальні мережі та залучення аудиторій; структурну дипломатію через регуляторний вплив і встановлення стандартів; дипломатію розбудови спроможностей через довгострокову підтримку цифрової трансформації партнерських держав. Таке поєднання ґрунтується на розумінні, що стійкий вплив на глобальний цифровий порядок неможливий лише через інформаційні кампанії, а потребує глибшої трансформації інституційного середовища та нормативних рамок у країнах-партнерах.

Європейська програма протидії дезінформації демонструє перехід від реактивного спростування фейків до побудови стійкості інформаційного простору. Її діяльність охоплює документування маніпуляцій, підтримку незалежних медіа та розвиток критичного мислення аудиторій. Програма виявила фундаментальну асиметрію між складністю створення якісного контенту і легкістю поширення дезінформації, що підкреслює потребу в системних змінах медіа-екосистеми, включно з розвитком незалежної журналістики, медіаграмотності та альтернативних економічних моделей.

Розвиткові ініціативи цифрової дипломатії, зокрема Digital4Development та «Глобальний шлюз», спрямовані на формування траєкторій цифрового розвитку партнерських країн відповідно до європейських стандартів. Таким чином ЄС використовує свою економічну вагу для створення довгострокових інституційних залежностей та сумісності систем. Водночас реалізація цих ініціатив ускладнюється повільністю процедур, фрагментованістю фінансування та недостатньою польовою присутністю, що потребує додаткових організаційних рішень для підвищення ефективності.

У глобальному та регіональному вимірах ефективність цифрової дипломатії ЄС суттєво різниться. Співпраця з демократичними партнерами, зокрема зі США та Японією, демонструє значні результати у формуванні спільних стандартів і позицій у багатосторонніх інституціях. Натомість у регіонах гострої геополітичної конкуренції вплив ЄС обмежений через ресурсну асиметрію та готовність конкурентів ігнорувати нормативні обмеження європейської моделі.

Підтримка цифрової стійкості України після 2022 року стала показником здатності ЄС до швидкої мобілізації ресурсів і гнучкого використання інструментів у кризових умовах. Водночас цей досвід виявив потребу у спрощенні процедур кризового реагування та посиленні координації між інституціями та державами-членами.

Узагальнюючи результати, можна стверджувати, що ефективність цифрової дипломатії ЄС визначається не обсягом ресурсів чи наявністю військових спроможностей, а здатністю перетворювати нормативну силу, регуляторну спроможність та мережу партнерств на стійкий структурний вплив. Для збереження та посилення цієї моделі необхідні подальше подолання координаційних викликів, забезпечення достатніх ресурсів та формування спільної стратегічної культури цифрової дипломатії, здатної об'єднати багатоманітних акторів навколо бачення демократичного та безпечного глобального цифрового порядку.

РОЗДІЛ 3. ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОЇ ДИПЛОМАТІЇ ЄС ТА ЇЇ СПІВПРАЦЯ З УКРАЇНОЮ

3.1. Цифрова дипломатія як складова зовнішньої політики розширення ЄС

Трансформація цифрової дипломатії з інструменту публічної комунікації та стратегічного наративного впливу у структурний компонент політики розширення Європейського Союзу відображає фундаментальну зміну розуміння процесів європейської інтеграції, де цифровізація перестає бути суто технічним питанням модернізації економіки та державного управління, натомість набуває характеру стратегічного геополітичного виміру, що визначає здатність країн-кандидатів до повноцінної участі у європейському проєкті та їхню стійкість перед обличчям гібридних загроз, інформаційного маніпулювання та технологічної залежності від авторитарних режимів. Інтеграція цифрової дипломатії у політику розширення передбачає не просто додавання нового тематичного блоку до традиційних критеріїв копенгагенського набуття, а радикальне переосмислення самої логіки європейської інтеграції в умовах, коли цифрова інфраструктура, кібербезпека, захист персональних даних, протидія дезінформації та цифрові компетенції населення стають критичними факторами національної безпеки, економічної конкурентоспроможності та демократичної стабільності, що вимагає від країн-аспірантів не лише формальної імплементації регуляторних норм, але й глибинної трансформації інституційних структур, технологічних систем та суспільних практик відповідно до європейської моделі цифрового розвитку.

Політика Східного партнерства, запущена у 2009 році як рамкова ініціатива для поглиблення відносин ЄС з шістьма країнами пострадянського простору, поступово еволюціонувала від переважно економічно-орієнтованого підходу до комплексної стратегії, що визнає критичну важливість цифрового виміру для трансформації партнерських країн та їхнього зближення з європейськими стандартами, що особливо актуалізувалося після 2014 року у контексті російської агресії проти України та масштабних інформаційних кампаній, спрямованих на дестабілізацію східноєвропейських суспільств і

підкрив їхньої проєвропейської орієнтації. Самміт Східного партнерства 2017 року в Брюсселі ознаменував якісний зсув через визнання цифрової економіки одним із чотирьох ключових пріоритетів партнерства поряд з економічним розвитком, врядуванням, сполученістю та суспільством, що відобразилося у запуску флагманської ініціативи EU4Digital, призначеної для підтримки цифрової трансформації країн Східного партнерства через гармонізацію регуляторних рамок, розбудову цифрової інфраструктури, розвиток цифрових навичок та інтеграцію у єдиний цифровий ринок ЄС. Горбатенко та Шедяков аналізують цю трансформацію як відповідь на усвідомлення ЄС геополітичного виміру цифровізації, де цифрова модернізація східноєвропейських партнерів стає інструментом не лише економічного розвитку, але й стратегічного закріплення цих країн до європейського простору та зменшення їхньої технологічної та інформаційної вразливості перед російським впливом [2, с. 145-148].

Концептуальна рамка цифрового виміру Східного партнерства базується на визнанні, що цифрова трансформація є наскрізним питанням, що перетинає всі сектори та тематичні опори партнерства від торгівлі та економічного розвитку до демократичного врядування, від енергетики до транспортної сполученості, від освіти до охорони здоров'я, вимагаючи інтегрованого підходу, який би забезпечував синергію між різними ініціативами та програмами, уникаючи фрагментації зусиль та дублювання втручань. Стратегічний документ «Східне партнерство після 2020: Час для нових амбіцій», представлений у березні 2020 року напередодні наступного саміту, що так і не відбувся через пандемію COVID-19, артикулював бачення стійкого, сталого та інтегрованого регіону Східного партнерства, де цифрова сполученість та цифровізація відіграють центральну роль у досягненні всіх стратегічних цілей від економічного процвітання до екологічної сталості, від підзвітного врядування до стійкого суспільства. Кобзар підкреслює, що амбітна риторика стратегічних документів контрастує з обмеженими ресурсами, виділеними на реалізацію цифрових ініціатив порівняно з масштабом викликів та потреб країн-партнерів, що створює розрив між очікуваннями та реалізацією, підриває довіру до

європейських зобов'язань та відкриває простір для альтернативних пропозицій від геополітичних конкурентів, що пропонують суттєве фінансування без нормативних умовностей [4, с. 82-85].

Операціоналізація цифрового виміру Східного партнерства відбувається через складну систему програм, проєктів та ініціатив, що охоплюють різні аспекти цифрової трансформації від розбудови широкосмугової інфраструктури в сільських районах до гармонізації законодавства про електронну комерцію, від розбудови спроможностей у кібербезпеці до підтримки цифрового підприємництва, від розвитку платформ електронного урядування до навчання цифровим навичкам, що вимагає координації між множиною інструментів фінансування ЄС, національними програмами держав-членів, міжнародними фінансовими інституціями та приватним сектором для забезпечення взаємодоповнюваності та максимізації впливу обмежених ресурсів. Програма EU4Digital, запущена у 2019 році з бюджетом приблизно тридцять мільйонів євро на перші чотири роки впровадження, структурована навколо п'яти тематичних областей, що включають широкосмугову сполученість, цифрові навички та робочі місця, сприяння цифровій торгівлі, цифрову довіру та безпеку, та електронну охорону здоров'я, кожна з яких передбачає комбінацію технічної допомоги, політичного діалогу, пілотування інноваційних рішень та поширення кращих практик для підтримки країн-партнерів у їхніх національних порядках денних цифрової трансформації. Матвієнко зазначає, що відносно скромний бюджет EU4Digital порівняно з амбітними цілями та масштабом потреб цифрового розвитку у регіоні вимагає стратегічного фокусування на областях з найвищим потенціалом впливу, де підтримка ЄС може каталізувати ширші трансформації та залучити додаткові інвестиції від інших донорів та приватного сектору, пріоритизуючи регуляторну гармонізацію та розбудову інституцій над прямим фінансуванням інфраструктури, яке вимагає суттєво більших ресурсів [8, с. 167-170].

Регуляторна гармонізація становить центральний елемент цифрового виміру Східного партнерства через прагнення створити розширений єдиний цифровий ринок, що охоплює країни-партнери через наближення їхнього

законодавства з цифровим набуттям ЄС, включаючи Загальний регламент про захист даних, Директиву про мережеву та інформаційну безпеку, Кодекс електронних комунікацій, Акт про цифрові послуги та інші ключові регуляторні рамки, що регулюють функціонування цифрового простору в ЄС. Процес наближення передбачає не просто транспонування європейських правових текстів у національне законодавство партнерських країн, але глибинну інституційну трансформацію для забезпечення ефективного виконання нових правил через створення незалежних регуляторних органів з адекватними повноваженнями та ресурсами, розвиток технічної експертизи для нагляду за складними цифровими ринками, встановлення механізмів для транскордонного співробітництва у виконанні, та сприяння регуляторній культурі, що балансує просування інновацій із захистом фундаментальних прав та суспільних інтересів. Петренко аналізує напруження між амбіціями швидкої регуляторної конвергенції та реальними інституційними спроможностями партнерських країн для ефективного впровадження складних регуляцій ЄС, що розроблялися для набагато більш розвинених регуляторних екосистем з сильними судовими системами, незалежними наглядовими органами та досконалими адміністративними спроможностями, аргументуючи, що механічне транспонування без адекватної розбудови спроможностей може призвести до регуляторного фасаду, де формальні правила існують на папері, але не функціонують ефективно на практиці [10, с. 201-204].

Цифрова дипломатія у контексті Східного партнерства охоплює не лише традиційні активності публічної дипломатії такі як комунікаційні кампанії та культурні обміни, але також стратегічні комунікації, спрямовані на протидію дезінформації, підтримку незалежних медіа, просування медіаграмотності та розбудову суспільної стійкості проти інформаційної маніпуляції, що стало особливо критичним після 2014 року, коли систематичні російські дезінформаційні кампанії проти України та інших країн Східного партнерства досягли безпрецедентного масштабу та інтенсивності, використовуючи традиційні медіа, соціальні мережі та альтернативні інформаційні платформи для поширення маніпулятивних наративів, підриву довіри до демократичних

інституцій та створення суспільних розколів. Оперативна група зі стратегічних комунікацій для Східного сусідства, створена EEAS у 2015 році, стала інституційним втіленням цього оборонного виміру цифрової дипломатії ЄС у регіоні через систематичний моніторинг, документування та спростування дезінформаційних наративів через платформу EUvsDisinfo, водночас надаючи підтримку місцевим медіа та громадянському суспільству у розвитку спроможності для ідентифікації та протидії інформаційній маніпуляції. Сагайдак та Ісаєнко підкреслюють, що ефективність цих зусиль обмежується структурною асиметрією між складністю створення якісного верифікованого контенту та легкістю виробництва і вірусного поширення емоційно зарядженої дезінформації, що вимагає переходу від суто реактивних підходів спростування конкретних фейків до більш проактивних стратегій формування альтернативних наративів та розбудови структурної стійкості інформаційних екосистем через підтримку якісної журналістики, медіаосвіти та диверсифікації джерел інформації [13, с. 245-248].

Вплив цифрових стратегій на зовнішню політику ЄС після 2022 року характеризується радикальною переоцінкою пріоритетів та підходів у відповідь на повномасштабне російське вторгнення в Україну, що не лише актуалізувало питання цифрової безпеки, інформаційної стійкості та протидії дезінформації, але й фундаментально змінило геополітичний контекст європейської цифрової дипломатії, де питання технологічного суверенітету, кібербезпеки критичної інфраструктури та цифрового виміру гібридної війни набули екзистенційного значення для безпеки та стабільності європейського континенту. Російське військове вторгнення супроводжувалося масштабними кібератаками на українську критичну інфраструктуру, державні установи та комунікаційні мережі, паралельними дезінформаційними кампаніями безпрецедентного масштабу в глобальному інформаційному просторі, спрямованими на виправдання агресії, делегітимізацію українського опору та підрив міжнародної підтримки України, що продемонструвало критичну важливість цифрового виміру сучасних конфліктів та необхідність комплексної відповіді, що інтегрує військову, дипломатичну, економічну та інформаційну складові. Толстов

аналізує, як російська агресія каталізувала прискорення європейської цифрової дипломатії та розширення її мандату від переважно комунікативних та розвиткових функцій до більш операційного залучення у підтримці кібероборони партнерів, координації міжнародної відповіді на інформаційні операції та мобілізації технологічного сектору для підтримки цифрової стійкості країн під загрозою [14, с. 178-181].

Стратегічний компас для безпеки та оборони, схвалений Радою ЄС у березні 2022 року, вперше експліцитно включив цифровий вимір як інтегральний компонент європейської безпекової політики, визнаючи, що гібридні загрози, кібератаки, дезінформація та інформаційне маніпулювання становлять не периферійні виклики, а центральні загрози європейській безпеці, що вимагають адекватних спроможностей, ресурсів та інституційних механізмів для ефективної відповіді як на превентивному, так і на реактивному рівнях реагування. Документ передбачає посилення спроможностей кіберзахисту, розвиток швидких реагувальних кіберкоманд ЄС для надання оперативної допомоги державам-членам та партнерам під кібератакою, покращення систем обміну інформацією про загрози та координації атрибуції кіберінцидентів, розширення використання режиму кібердипломатичних санкцій проти відповідальних за шкідливі кіберактивності, та інтеграцію кіберіміру у всі аспекти спільної безпекової та оборонної політики від планування місій до навчань та операцій. Чекаленко та Воловик підкреслюють, що імплементація амбітних зобов'язань Стратегічного компасу вимагає суттєвого збільшення ресурсів, інституційних реформ для прискорення процесів прийняття рішень, подолання стійких розбіжностей між державами-членами щодо ступеня інтеграції у кібербезпекових питаннях, та розвитку справжньої стратегічної культури, що визнає кіберпростір як легітимний простір військового та дипломатичного протистояння, що вимагає відповідних спроможностей та готовності їх використовувати [16, с. 189-192].

Глобальна стратегія цифрової дипломатії ЄС, оновлена у 2023 році з урахуванням уроків від російської агресії та трансформацій глобального геополітичного ландшафту, артикулює більш наполегливий та геополітично

усвідомлений підхід порівняно з попередніми документами, експліцитно визнаючи, що цифрова сфера стала ареною інтенсивної геополітичної конкуренції між демократичними та авторитарними моделями врядування, де ЄС має не *merely* регулювати та комунікувати, але активно боротися за формування глобального цифрового порядку відповідно до своїх цінностей та інтересів. Стратегія визначає три взаємопов'язані стратегічні цілі: по-перше, посилення цифрової стійкості ЄС та його партнерів через розбудову спроможностей кіберзахисту, протидії дезінформації та захисту критичної цифрової інфраструктури; по-друге, просування на глобальному рівні європейської моделі цифрового управління, заснованої на правах людини, демократичних цінностях та верховенстві права; по-третє, забезпечення цифрового суверенітету через зменшення технологічної залежності від геополітичних конкурентів та розвиток власних європейських цифрових спроможностей у критичних технологіях від штучного інтелекту до квантових обчислень, від напівпровідників до хмарних сервісів. Яковюк аналізує цей стратегічний поворот як запізнілу, але необхідну відповідь на зростаючу технологічну біполярність між США та Китаєм, де ЄС ризикує залишитися регуляторною силою без технологічних спроможностей для забезпечення власного суверенітету та захисту своїх інтересів, що вимагає радикального збільшення інвестицій у дослідження та інновації, створення сприятливого екосистему для європейських технологічних лідерів та стратегічних партнерств з демократичними союзниками для формування критичної маси технологічної та нормативної влади [17, с. 256-259].

Інституційна реорганізація EEAS після 2022 року включає посилення Підрозділу стратегічних комунікацій через додаткові людські ресурси та фінансування, розширення мандату Підрозділу цифрової дипломатії для охоплення більш операційних функцій у підтримці кіберзахисту партнерів, створення координаційних механізмів для швидкого реагування на інформаційні кризи через залучення експертизи різних інституцій ЄС, держав-членів та приватного сектору, та поглиблення співпраці з НАТО у кібербезпекових та стратегічних комунікаційних питаннях для уникнення дублювання та забезпечення взаємодоповнюваності зусиль двох організацій у відповідь на

спільні загрози. Створення спеціальної посади надзвичайного та повноважного посла з цифрових питань у деяких державах-членах, таких як Данія та Нідерланди, стимулювало дискусії про доцільність подібної структури на рівні ЄС для забезпечення увагу високого політичного рівня до цифрових питань зовнішньої політики та покращення координації між різними тематичними напрямками цифрової дипломатії від торгівлі та економічного співробітництва до безпеки та прав людини. Бебик та Головатий зазначають, що організаційні інновації самі по собі недостатні без справжньої політичної волі держав-членів надавати адекватні ресурси, делегувати необхідні повноваження на європейський рівень та приймати колективну дисципліну у питаннях, що традиційно вважалися національними прерогативами, що вимагає не лише технічних коригувань інституційних структур, але фундаментального зсуву у стратегічній культурі європейської зовнішньої політики від уникнення ризиків та пошуку консенсусу до більш рішучої та наполегливої позиції, готової використовувати доступні інструменти впливу навіть за ціною короткострокових економічних витрат чи дипломатичного тертя [2, с. 267-270].

Партнерства з демократичними союзниками набули нового стратегічного пріоритету після 2022 року через визнання, що ізольований європейський підхід недостатній для формування глобального цифрового порядку в умовах інтенсивної геополітичної конкуренції, що вимагає формування коаліцій з однодумцями для створення критичної маси нормативної та економічної влади. Трансатлантична Рада з торгівлі та технологій набула нового поштовху після російського вторгнення через усвідомлення нагальної потреби координації підходів до контролю експорту технологій, перевірки іноземних інвестицій у критичні сектори, стійкості ланцюгів постачання та протидії авторитарним цифровим моделям, що каталізувало прогрес у областях, що попередньо стагнували через стійкі трансатлантичні розбіжності з приводу управління даними та регулювання великих технологічних платформ. Цифрове партнерство з Японією, подібні угоди з Південною Кореєю, Сінгапуром та іншими технологічно розвиненими демократіями формують мережу партнерств, що прагнуть координувати підходи до критичних технологій, гармонізувати

стандарти та спільно просувати демократичні цінності у глобальному цифровому просторі як альтернативу китайським ініціативам, що пропонують суттєві ресурси без умовностей щодо врядування. Литвин аргументує, що ефективність цих партнерств залежить від здатності рухатися за межі декларативних зобов'язань до конкретних колаборативних проєктів з відчутними результатами, що демонструють додану вартість коаліційного підходу порівняно з односторонніми діями чи двосторонніми угодами з авторитарними силами, вимагаючи стратегічного терпіння для розбудови довіри, розвитку спільного розуміння та узгодження регуляторних підходів через ітераційний процес діалогу та практичного співробітництва [6, с. 123-126].

Узагальнюючи аналіз цифрової дипломатії як складової зовнішньої політики розширення ЄС, доцільно констатувати, що цифровий вимір трансформувався з периферійного технічного питання у центральний стратегічний пріоритет європейської інтеграційної політики, що відображає фундаментальну зміну природи сучасної геополітики, де технологічні спроможності, кіберстійкість, цілісність інформаційної екосистеми та цифровий суверенітет стають критичними факторами національної безпеки та геополітичного впливу. Східне партнерство демонструє еволюцію від фокусу на економічному співробітництві до комплексного підходу, що визнає взаємозалежність між цифровою трансформацією, демократичним врядуванням, економічним процвітанням та геополітичною орієнтацією партнерських країн, хоча стійкий розрив між амбітною риторикою стратегічних документів та обмеженими ресурсами, виділеними для імплементації, підриває довіру до європейських зобов'язань та створює вразливості, що можуть бути використані геополітичними конкурентами через альтернативні пропозиції. Вплив російської агресії проти України каталізував парадигмальний зсув у європейській цифровій дипломатії від переважно підходу м'якої сили до більш інтегрованої стратегії, що поєднує комунікативні, регуляторні, розбудови спроможностей та операційної підтримки елементи у комплексній відповіді на гібридні загрози, водночас експонуючи стійкі обмеження інституційних структур, процесів прийняття рішень та механізмів розподілу ресурсів ЄС для ефективних дій у швидко

еволюціонуючих кризових ситуаціях. Перспективи подальшого розвитку цифрової дипломатії ЄС у контексті розширення залежать від здатності трансформувати уроки, вивчені з українського досвіду, у системні покращення інституційних рамок, справжнє збільшення ресурсів відповідно до декларованих амбіцій, та розвитку автентичної стратегічної культури, що визнає цифровий простір як легітимний простір геополітичної конкуренції, що вимагає не лише нормативного лідерства, але також операційних спроможностей та політичної волі їх використовувати у захисті європейських інтересів та цінностей, що становить необхідну передумову для аналізу конкретного досвіду та напрямків цифрової взаємодії між ЄС та Україною як тестового випадку нового підходу до цифрового виміру європейської інтеграційної політики.

3.2. Напрями цифрової взаємодії ЄС та України

Цифрова взаємодія між Європейським Союзом та Україною набула якісно нового значення після 2014 року, коли анексія Криму та початок збройної агресії Росії на Донбасі актуалізували питання цифрової стійкості, кібербезпеки та протидії дезінформації як критичних компонентів національної безпеки та державного суверенітету, що трансформувало цифрове співробітництво з технічної сфери модернізації економіки у стратегічний вимір європейської інтеграції України та її здатності протистояти гібридним загрозам авторитарної агресії. Повномасштабне російське вторгнення у лютому 2022 року радикально прискорило та поглибило цифрову співпрацю, де Україна перетворилася на передову лінію не лише фізичного військового протистояння, але й цифрового та інформаційного протиборства, що вимагало від ЄС переходу від традиційних форматів довгострокової розвиткової допомоги до оперативної підтримки критичної цифрової інфраструктури, кібероборони та стратегічних комунікацій в умовах активного конфлікту, демонструючи як спроможність європейських інституцій до швидкої адаптації у кризових ситуаціях, так і структурні обмеження бюрократичних процедур та координаційних механізмів для ефективного реагування на динамічні виклики гібридної війни. Аналіз досвіду та

напрямків цифрової взаємодії між ЄС та Україною дозволяє не лише оцінити ефективність конкретних програм та ініціатив, але й виявити системні патерни європейського підходу до підтримки цифрової трансформації та стійкості партнерських країн під гібридними загрозами, що має ширші імплікації для формування майбутньої політики розширення та сусідства ЄС у цифровій сфері.

Програма EU4Digital становить центральну рамкову ініціативу цифрової співпраці між ЄС та Україною у контексті Східного партнерства, що охоплює широкий спектр активностей від гармонізації регуляторних рамок до розбудови широкосмугової сполученості, від розвитку цифрових навичок до просування електронної комерції, від кібербезпеки до електронної охорони здоров'я, створюючи комплексну систему підтримки для наближення України до стандартів єдиного цифрового ринку ЄС та інтеграції у європейський цифровий простір. Запущена у 2019 році з початковим бюджетом приблизно тридцять мільйонів євро для всіх країн Східного партнерства, програма структурована навколо п'яти тематичних опор, кожна з яких передбачає комбінацію політичного діалогу для узгодження стратегічних підходів, технічної допомоги для розбудови інституційних спроможностей, фінансування для пілотних проєктів та інфраструктурних інвестицій, та обміну знаннями для поширення кращих практик між партнерськими країнами. Горбатенко та Шедяков підкреслюють, що ефективність EU4Digital для України значною мірою залежить від координації з національними програмами цифровізації, узгодження з пріоритетами, визначеними у Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та наступних стратегічних документах, та спроможності української сторони засвоювати технічну допомогу через адекватні інституційні структури та кваліфікований персонал, що не завжди відповідало амбіціям програми через обмежені адміністративні спроможності, плинність кадрів у державних інституціях та конкуруючі пріоритети в умовах триваючого конфлікту [2, с. 178-181].

Компонент широкосмугової сполученості програми EU4Digital спрямований на розширення доступу до високошвидкісного інтернету в сільських та віддалених регіонах України через підтримку розбудови фізичної

інфраструктури, гармонізацію регуляторних рамок для стимулювання приватних інвестицій у телекомунікаційний сектор, та розробку національної стратегії широкосмугового доступу, узгодженої з європейськими цілями гігабітного суспільства до 2025 року, що передбачають універсальне покриття населених пунктів сполученістю з швидкістю щонайменше сто мегабітів на секунду з можливістю покращення до гігабітних швидкостей. Конкретні досягнення включають прийняття Закону України «Про електронні комунікації» у грудні 2022 року, що наближує українське законодавство до Європейського кодексу електронних комунікацій, створення регуляторної рамки для розгортання мереж п'ятого покоління, та пілотні проекти розбудови волоконно-оптичних мереж у селах Львівської та Івано-Франківської областей, що демонструють можливість та економічну доцільність розширення широкосмугового доступу до недостатньо забезпечених спільнот. Кобзар зазначає, що прогрес у компоненті широкосмугової сполученості повільніший порівняно з іншими опорами програми через капіталомістку природу інфраструктурних інвестицій, що вимагають суттєво більших фінансових ресурсів ніж доступні через EU4Digital, що потребує мобілізації додаткового фінансування від міжнародних фінансових інституцій, національного бюджету та приватного сектору, що ускладнюється в умовах війни та конкуруючих пріоритетів відновлення критичної інфраструктури, зруйнованої російськими атаками [4, с. 156-159].

Опора цифрових навичок та робочих місць фокусується на розвитку цифрових компетенцій українського населення через реформування освітньої системи для інтеграції цифрової грамотності у навчальні програми всіх рівнів освіти, підтримку програм професійної підготовки у пріоритетних областях як розробка програмного забезпечення, кібербезпека, аналіз даних та цифровий маркетинг, сприяння навчанню дорослих та ініціативам перекваліфікації для адаптації робочої сили до вимог цифрової економіки, та просування участі жінок у технологічних секторах для подолання гендерного розриву у галузях природничих наук, технологій, інженерії та математики. Конкретні ініціативи включають розробку Національної рамки цифрових компетенцій для України, узгодженої з Європейською рамкою цифрових компетенцій, впровадження

програми підготовки вчителів з цифрових навичок через мережу регіональних центрів підвищення кваліфікації, запуск онлайн-платформи безкоштовних курсів з базових та просунутих цифрових навичок, доступних для всіх громадян незалежно від віку, географічного розташування чи соціально-економічного статусу, та підтримку бізнес-інкубаторів для цифрових стартапів у регіональних центрах для стимулювання місцевого цифрового підприємництва. Матвієнко підкреслює, що розвиток цифрових навичок представляє довгостроковий структурний виклик, що вимагає стійкого зобов'язання та інвестицій протягом років чи навіть десятиліть для досягнення фундаментального зсуву у цифровій грамотності населення, де короткострокові проєктні втручання можуть мати лише обмежений вплив без системних реформ освітньої системи та безперервного оновлення навчальних програм відповідно до швидко еволюціонуючого технологічного ландшафту [8, с. 189-192].

Компонент сприяння цифровій торгівлі спрямований на зменшення регуляторних бар'єрів для транскордонної електронної комерції через гармонізацію законодавства про електронні підписи, електронну ідентифікацію та довірчі послуги з регламентом Європейського Союзу, спрощення митних процедур для онлайн-торгівлі через впровадження електронних декларацій та систем управління ризиками, розвиток логістичної інфраструктури для підтримки зростання обсягів посилкової торгівлі, та захист прав споживачів у цифровому середовищі через адаптацію законодавства про захист прав споживачів до специфіки онлайн-транзакцій. Прийняття Закону України «Про електронні довірчі послуги» у листопаді 2021 року створило правову основу для визнання електронних підписів та інших довірчих послуг, що є критичною передумовою для розвитку безпечної електронної комерції та електронного урядування, водночас інтеграція українських систем електронної ідентифікації з європейською інфраструктурою довірчих послуг залишається триваючим процесом, що вимагає технічної гармонізації та двосторонніх угод про визнання для забезпечення сумісності систем. Петренко аналізує напруження між амбіціями швидкої лібералізації електронної комерції для стимулювання економічного зростання та необхідністю адекватних рамок захисту споживачів,

особливо у контексті зростаючої поширеності онлайн-шахрайства, фейкових платформ електронної комерції та транскордонних суперечок, що вимагає балансування сприяння легітимній торгівлі з механізмами примусового виконання проти зловживань, особливо складного в умовах обмежених ресурсів регуляторних органів та судової системи для ефективного нагляду за швидко розширюваним онлайн-ринком [10, с. 223-226].

Опора цифрової довіри та безпеки охоплює широкий спектр активностей від розбудови національних спроможностей кібербезпеки до гармонізації законодавства про захист персональних даних, від створення системи реагування на кіберінциденти до сертифікації критичної інформаційної інфраструктури, від підготовки кібербезпекових фахівців до підвищення обізнаності населення про цифрові ризики та безпечну поведінку онлайн. Прийняття Закону України «Про захист персональних даних» у червні 2010 року та його подальші поправки наближують українську рамку захисту даних до стандартів Загального регламенту про захист даних Європейського Союзу, хоча повна відповідність залишається триваючим процесом, що вимагає не лише законодавчих коригувань але також інституційного зміцнення Уповноваженого з захисту персональних даних, розвитку судової практики у спрах про захист даних, та сприяння культурі обізнаності про приватність серед як бізнесу так і громадян. Створення Державної служби спеціального зв'язку та захисту інформації як центрального органу виконавчої влади з питань кібербезпеки, реорганізація національної системи кіберзахисту після 2014 року, та створення Ситуаційного центру забезпечення кібербезпеки для координації реагування на кіберінциденти демонструють інституційний прогрес у розбудові національної архітектури кібербезпеки, водночас стійкі виклики включають дефіцит кваліфікованих кібербезпекових професіоналів, обмежені бюджети для придбання передових технологій та інструментів, фрагментацію відповідальності між множиною агенцій, та недостатнє залучення приватного сектору у національні зусилля з кібербезпеки. Сагайдак та Ісаєнко підкреслюють, що повномасштабне російське вторгнення драматично оголило вразливості української кіберінфраструктури через безпрецедентний масштаб та складність кібератак на критичну

інфраструктуру, державні установи, фінансові системи та комунікаційні мережі, водночас також каталізувало міжнародну підтримку для посилення української кібероборони через надання передових технологій, технічної експертизи, обміну розвідувальними даними та допомоги у розбудові спроможностей від ЄС, США, НАТО та окремих країн-партнерів [13, с. 267-270].

Програма Цифрова Європа представляє більш новітню рамку цифрової співпраці між ЄС та Україною, запущену у 2021 році як флагманський інструмент фінансування Європейської Комісії для прискорення цифрової трансформації економіки та суспільства з бюджетом сім мільярдів євро для періоду 2021-2027 років, що фокусується на п'яти стратегічних напрямках: суперкомп'ютерні обчислення, штучний інтелект, кібербезпека, просунуті цифрові навички, та забезпечення широкого використання цифрових технологій в економіці та суспільстві. Україна отримала можливість участі у певних компонентах програми Цифрова Європа як асоційована країна через механізми Східного партнерства та у контексті статусу кандидата на членство в ЄС, що відкриває доступ до можливостей фінансування, спільних проєктів та мереж європейських центрів цифрових інновацій, хоча повноцінна участь вимагає суттєвого співфінансування від української сторони та дотримання програмних правил та процедур, що може бути викликом враховуючи обмежені бюджетні ресурси та конкуруючі пріоритети в умовах війни. Конкретні напрямки участі України включають Європейську мережу компетенцій з кібербезпеки для розвитку дослідницьких та інноваційних спроможностей у кібербезпеці, мережу Європейських центрів цифрових інновацій для підтримки малих та середніх підприємств у процесах цифрової трансформації, та програми розвитку просунутих цифрових навичок для підготовки фахівців у критичних технологічних областях від штучного інтелекту до квантових обчислень. Толстов зазначає, що участь України у програмі Цифрова Європа становить важливий крок до глибшої інтеграції у європейський дослідницький та інноваційний простір, водночас реальна ефективність цієї участі залежатиме від спроможності українських інституцій, підприємств та дослідницьких організацій конкурувати за проєктне фінансування у високо конкурентному середовищі, де

вони змагаються з набагато більш ресурсно забезпеченими та досвідченими акторами з держав-членів ЄС, що вимагає цільової підтримки для розбудови спроможностей українських заявників та сприяння їхній участі у консорціумах з європейськими партнерами [14, с. 198-201].

Кібердіалог між ЄС та Україною становить спеціалізований формат двосторонньої взаємодії з питань кібербезпеки, що охоплює обмін інформацією про кіберзагрози, координацію відповідей на кіберінциденти, гармонізацію законодавства та політик у сфері кібербезпеки, співпрацю у розслідуванні кіберзлочинів, та спільні навчання і вправи для підготовки до кіберкризових ситуацій, створюючи інституційну рамку для системного діалогу та практичного співробітництва між відповідними установами обох сторін. Перший раунд кібердіалогу відбувся у жовтні 2014 року у відповідь на зростаючі кіберзагрози, з якими зіткнулася Україна після початку російської агресії, коли систематичні кібератаки на українську критичну інфраструктуру, державні установи та фінансові системи продемонстрували нагальну потребу міжнародної підтримки для посилення національної кібероборони. Наступні раунди кібердіалогу відбувалися регулярно, фокусуючись на різних аспектах від законодавчого наближення до операційного співробітництва, від розбудови спроможностей до спільних кібернавчань, поступово розширюючи обсяг та поглиблюючи залучення між європейськими та українськими кібербезпековими спільнотами. Чекаленко та Воловик підкреслюють, що кібердіалог забезпечує не лише формальну платформу для дипломатичних обмінів, але й практичні механізми для швидкого реагування на кіберкризи через гарячі лінії між командами реагування на кіберінциденти, регулярний обмін розвідувальними даними про нові загрози та скоординовану атрибуцію кібератак відповідальним акторам, що було особливо критичним після лютого 2022 року, коли українська кіберінфраструктура зазнала безпрецедентних спроб злому паралельно з військовим вторгненням [16, с. 212-215].

Повномасштабне російське вторгнення каталізувало якісний стрибок у кібербезпековій співпраці між ЄС та Україною через розгортання швидких реагувальних кіберкоманд ЄС для надання оперативної технічної допомоги

українським установам під кібератакою, надання передових технологій та інструментів кібербезпеки від європейських компаній та держав-членів, обмін розвідувальними даними про кіберзагрози у режимі реального часу для раннього виявлення та запобігання атакам, та скоординовану публічну атрибуцію російських кіберопераций для міжнародного викриття та засудження відповідальних акторів. Європейське агентство з кібербезпеки відіграло координуючу роль у мобілізації експертизи та ресурсів держав-членів для підтримки України, сприяючи двосторонній допомозі та забезпечуючи технічне керівництво з кращих практик захисту критичної інфраструктури, процедур реагування на інциденти та відновлення після кібератак. Яковюк аналізує цей безпрецедентний рівень операційного кіберспівробітництва як парадигмальний зсув у європейському підході до кібербезпекової солідарності, де Україна стала тестовим випадком для механізмів колективної кібероборони та швидкого реагування, що може інформувати майбутній розвиток спроможностей ЄС для підтримки партнерів під кіберзагрозами, водночас оголюючи прогалини у координаційних процедурах, механізмах мобілізації ресурсів та правових рамках для транскордонної кібердопомоги, що вимагають вирішення для інституціоналізації уроків, вивчених з українського досвіду [17, с. 278-281].

Стан інтеграції України у цифровий дипломатичний простір ЄС характеризується поступовим, але нерівномірним прогресом у різних вимірах від регуляторного наближення до операційної співпраці, від технічної гармонізації до інституційної інтеграції, що відображає як досягнення у впровадженні європейських стандартів та практик, так і стійкі виклики, пов'язані з обмеженими ресурсами, інституційними слабкостями та disruptions від триваючої війни. Регуляторне наближення демонструє найбільш відчутний прогрес через прийняття ключових законодавчих актів, що транспонують європейські директиви та регламенти у національне законодавство, включаючи закони про електронні комунікації, електронні довірчі послуги, захист персональних даних, кібербезпеку та електронну комерцію, створюючи правову основу для функціонування цифрової економіки відповідно до європейських стандартів, хоча ефективність імплементації та правозастосування цих законів залишається

нерівномірною через недостатні адміністративні спроможності регуляторних органів, обмежені бюджети для enforcement activities та gaps у судовій практиці з нових цифрових питань. Бебик та Головатий підкреслюють, що формальна транспозиція європейського законодавства, хоча необхідна, є недостатньою для genuine інтеграції у європейський цифровий простір без супутніх інвестицій у розбудову інституційних спроможностей, підготовку кваліфікованих кадрів, розвиток судової експертизи та fostering регуляторної культури, що поєднує facilitation інновацій з захистом прав та суспільних інтересів, що вимагає sustained commitment та resources протягом років для досягнення substantial convergence з європейськими практиками [2, с. 289-292].

Інтеграція цифрових систем України з європейською інфраструктурою просувається в окремих секторах, як-от електронна ідентифікація та телекомунікації. Однак через несумісність старих і нових систем, обмежене фінансування та складну координацію між українськими агентствами залишаються значні виклики для повної інтеграції. Пілотні проєкти взаємного визнання електронних підписів між Україною та окремими країнами ЄС доводять технічну можливість інтеграції в європейську інфраструктуру довірчих послуг. Однак для масштабування на весь ЄС необхідні складна сертифікація, укладання двосторонніх угод із усіма членами та постійне підтримання інтероперабельності зі зміною стандартів. Литвин наголошує, що повна інтеграція – це тривалий процес, який потребує не разових рішень, а системної співпраці, спільного розвитку й адаптації технологій через інституційні механізми та безперервний технічний діалог [6, с. 301-304].

Інституційна інтеграція України до європейських цифрових мереж і програм поступово просувається завдяки участі в різних ініціативах, таких як EU4Digital, Digital Europe Programme, European Cybersecurity Competence Network та мережа European Digital Innovation Hubs. Це створює численні точки дотику для взаємодії між українськими та європейськими інституціями, обміну досвідом, реалізації спільних проєктів та поступового засвоєння європейських норм і практик. Водночас така участь часто залишається периферійною у порівнянні з повноправними членами через обмежені фінансові внески України

до програмних бюджетів, що своєю чергою звужує доступ до фінансування, представництва в органах ухвалення рішень та права голосу в управлінні програмами, формуючи асиметричні відносини, де Україна виступає отримувачем підтримки, а не рівноправним партнером у визначенні стратегічних напрямів і пріоритетів європейських цифрових ініціатив. Потенційна перспектива членства України в ЄС може трансформувати цю динаміку шляхом поступового переходу від асоційованого статусу до повноправного членства з усіма відповідними правами й обов'язками, включаючи повноцінну участь у всіх європейських програмах і процесах ухвалення рішень. Однак конкретні терміни та умови цієї трансформації залишаються невизначеними, що створює виклики для довгострокового планування та стратегічного позиціонування української участі у європейських цифрових ініціативах. Мартинов стверджує, що навіть до набуття повноправного членства Україна має орієнтуватися на максимальну змістову інтеграцію шляхом проактивної участі у доступних можливостях співпраці, демонструвати здатність ефективно засвоювати європейську підтримку, формувати успішний досвід впровадження проєктів і розвивати міжособистісні зв'язки між українськими та європейськими цифровими спільнотами, що стане підґрунтям для плавного переходу до повноправного членства, коли політичні умови це дозволятимуть [7, с. 178-181].

Інтеграція України у цифровий дипломатичний простір ЄС стикається зі структурними та поточними викликами: економічна нерівність, обмежені інституційні спроможності й спадок технологій, а також вплив війни, яка відволікає ресурси, створює невизначеність і ускладнює довгострокове планування. Водночас війна прискорила деякі цифрові реформи, особливо в кіберзахисті та наданні онлайн-послуг. Для сталого прогресу необхідний збалансований підхід, креативні рішення щодо технічної підтримки, гнучкість у виконанні програм і більше фінансової підтримки з боку ЄС, щоб інтеграція не зупинилася навіть у складних умовах [9, с. 267-270].

Таким чином, останнє десятиліття позначило перехід від технічного співробітництва між ЄС та Україною до стратегічного партнерства в цифровій сфері, що виникло під впливом російської агресії та гібридних загроз. Ініціативи

EU4Digital, Digital Europe і Кібердіалог створили основу для регуляторної гармонізації та розвитку інфраструктури, хоча суттєві розбіжності залишаються щодо імплементації й сумісності систем. Повномасштабна війна оголила слабкі місця української цифрової інфраструктури, але водночас сприяла міжнародній підтримці та зміцненню кіберзахисту. Подальша інтеграція залежить від прогресу України на шляху до членства в ЄС, що змінює характер взаємодії з асиметричної допомоги на рівне партнерство, а також формує контекст для вдосконалення політики цифрової дипломатії ЄС.

3.3. Пропозиції щодо вдосконалення політики цифрової дипломатії ЄС та інтеграції України

Формулювання конкретних пропозицій щодо вдосконалення політики цифрової дипломатії Європейського Союзу та оптимізації шляхів інтеграції України у європейський цифровий дипломатичний простір вимагає критичного синтезу теоретичних підходів, емпіричного аналізу існуючих практик та прагматичного врахування реальних можливостей і обмежень обох сторін у контексті динамічного геополітичного середовища, що характеризується зростаючою інтенсивністю гібридних загроз, технологічною конкуренцією великих держав та фундаментальною трансформацією природи міжнародних відносин під впливом цифровізації. Ці пропозиції мають базуватися на розумінні, що ефективна цифрова дипломатія не є самоціллю, а інструментом досягнення ширших стратегічних цілей від забезпечення національної безпеки та економічної конкурентоспроможності до захисту демократичних цінностей та прав людини у цифровому просторі, що вимагає інтегрованого підходу, який би органічно поєднував комунікативні, регуляторні, технологічні та інституційні виміри цифрової трансформації зовнішньої політики. Водночас реалістичне формулювання пропозицій має враховувати політичні, фінансові та інституційні обмеження, що лімітують можливості радикальних змін, натомість фокусуючись на поступових покращеннях, які можуть бути втілені у короткостроковій та середньостроковій перспективі з наявними ресурсами та в межах існуючих

інституційних рамок, водночас не виключаючи більш амбітних довгострокових трансформацій, які можуть вимагати змін договорів, суттєвого додаткового фінансування чи фундаментальних інституційних реформ.

Створення спільних платформ цифрової безпеки між ЄС та Україною становить критичний пріоритет для посилення колективної спроможності протистояти кіберзагрозам та інформаційним операціям, що вимагає переходу від епізодичного ситуативного співробітництва до систематизованої інституційної рамки для постійного обміну інформацією про загрози, координації реагування на інциденти, спільного планування превентивних заходів та взаємної підтримки у розбудові спроможностей для кібероборони. Конкретна пропозиція передбачає створення Спільного центру координації кібербезпеки ЄС-Україна як постійної інституційної структури, що об'єднає представників Європейського агентства з кібербезпеки, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, команд реагування на комп'ютерні надзвичайні ситуації держав-членів ЄС та інших релевантних акторів для забезпечення цілодобового моніторингу кіберзагроз, швидкого обміну розвідувальними даними, координації атрибуції кібератак та мобілізації технічної допомоги у критичних ситуаціях. Горбатенко та Шедяков аргументують, що такий центр має функціонувати не як суто міжурядовий орган з консенсусними процедурами прийняття рішень, що уповільнюють час реагування, а як операційна структура з делегованими повноваженнями для автономних дій у визначених параметрах, використовуючи захищені канали комунікації, протоколи обміну секретною інформацією та процедури швидкого реагування для ефективного функціонування у критичних за часом кіберкризових ситуаціях [2, с. 312-315].

Технічна архітектура Спільного центру координації кібербезпеки має включати інтегровану платформу обміну індикаторами компрометації, яка автоматично поширює інформацію про виявлені шкідливі програми, підозрілі мережеві активності, фішингові кампанії та інші кіберзагрози між усіма учасниками мережі у режимі реального часу, дозволяючи превентивне блокування атак до їхнього поширення на інші системи, водночас забезпечуючи

захист конфіденційної інформації через шифрування, контроль доступу та принципи необхідності знати для чутливої розвідувальної інформації. Система спільної обізнаності про ситуацію має агрегувати дані з множинних джерел від сенсорів мережевого трафіку до систем виявлення вторгнень, від потоків інформації про загрози комерційних постачальників до секретних брифінгів національних розвідувальних агенцій, створюючи комплексну картину кіберзагроз у реальному часі та уможлиблюючи обґрунтоване прийняття рішень щодо розподілу ресурсів кібероборони та встановлення пріоритетів захисних заходів. Кобзар підкреслює, що ефективність такої системи критично залежить від готовності всіх учасників ділитися чутливою інформацією, що вимагає високого рівня довіри, надійних правових рамок для захисту секретних даних, чітких протоколів щодо дозволеного використання спільної розвідувальної інформації, та механізмів підзвітності за несанкціоновані розголошення чи неправомірне використання інформації, що може бути викликом у асиметричних відносинах між повноправними членами ЄС та асоційованим партнером як Україна, що потребує ретельного проектування структур управління та угод про обмін інформацією.

Спільні навчання та кіберучення між українськими та європейськими кіберкомандами мають стати регулярною практикою для відпрацювання координації у відповідь на складні кібератаки на критичну інфраструктуру, тестування протоколів комунікації та процедур прийняття рішень в умовах стресу, виявлення прогалин у спроможностях та процесах, та сприяння особистим стосункам між ключовими працівниками, що полегшують неформальну координацію навіть поза формальними інституційними каналами. Ці учення мають моделювати реалістичні сценарії від атак програм-вимагачів на медичні заклади до порушення роботи енергетичних систем, від втручання у вибори через кампанії дезінформації до компрометації фінансових транзакцій, використовуючи реальні тактики, техніки та процедури, спостережувані у справжніх кібератаках для максимального реалізму та практичної цінності навчальних активностей. Матвієнко зазначає, що спільні кіберучення служать не лише навчальним цілям, але також заходам зміцнення довіри, що демонструють

відданість співпраці, тестують сумісність систем та процедур, виявляють кращі практики для поширення серед країн-учасниць, та надсилають стримувальний сигнал потенційним супротивникам про готовність та спроможність колективної відповіді на кіберагресію [8, с. 312-315].

Платформа стратегічних комунікацій ЄС-Україна має інституціоналізувати координацію між Оперативною групою зі стратегічних комунікацій для Східного сусідства та українськими структурами стратегічних комунікацій для узгодження наративів, синхронізації повідомлень, спільного планування комунікаційних кампаній та взаємного посилення контенту для максимізації охоплення та впливу у протидії російській дезінформації та просуванні позитивних наративів про європейську інтеграцію, демократичні цінності та переваги заснованого на правилах міжнародного порядку. Конкретні механізми мають включати регулярні координаційні зустрічі на операційному рівні для планування календарів контенту, узгодження тематичних повідомлень та координації часу основних комунікаційних активностей, спільні інструменти моніторингу медіа для відстеження дезінформаційних наративів та вимірювання ефективності контрзаходів, спільну спроможність швидкого реагування для оперативної відповіді на нові дезінформаційні загрози через координоване спростування та просування альтернативних наративів, та ініціативи спільного створення контенту від спільно виготовлених відео та інфографіки до комунікаційних кампаній у соціальних мережах зі спільним брендуванням та мультимедійних проєктів. Петренко підкреслює важливість збереження української суб'єктності та голосу у цих спільних ініціативах, уникнення патерналістської динаміки де європейська сторона диктує наративи та підходи, натомість сприяючи справжньому партнерству де українські перспективи, культурні інсайти та місцеве знання інформують розробку стратегії, забезпечуючи автентичність та резонанс комунікацій з цільовими аудиторіями, особливо у контекстах де повідомлення з Брюсселя зверху можуть сприйматися як відірвані від місцевих реалій та турбот [10, с. 356-359].

Програма обміну персоналом між Підрозділом стратегічних комунікацій EEAS та українським Міністерством закордонних справ може сприяти передачі

знань, взаємному навчанню, особистим зв'язкам та культурному розумінню, що зміцнюють довгострокову основу співпраці навіть за обмежень формальних інституційних механізмів, через відрядження українських дипломатів до структур у Брюсселі на періоди від кількох місяців до року та розміщення європейських працівників з комунікацій у Києві для отримання безпосереднього розуміння українського контексту, викликів та перспектив. Такі обміни мають бути структурованими програмами з чіткими навчальними цілями, наставницькими домовленостями, практичною проектною роботою, та систематичним підведенням підсумків для фіксації вивчених уроків та поширення інсайтів у ширших організаційних структурах, а не неформальними ситуативними домовленостями з нечіткими очікуваннями та обмеженим інституційним впливом. Сагайдак та Ісаєнко аргументують, що інвестиції у міжлюдські обміни та можливості професійного розвитку для українських практиків комунікацій приносять довгострокові дивіденди через розбудову стійкої спроможності, сприяння професійним мережам, створення спільного розуміння підходів та викликів, та розвиток особистих стосунків, що полегшують неформальну координацію та вирішення проблем навіть коли формальні канали стикаються з бюрократичними перешкодами чи політичною чутливістю [13, с. 389-392].

Рекомендації для Міністерства закордонних справ України щодо адаптації до стандартів цифрової дипломатії ЄС мають фокусуватися на інституційних реформах, що зміцнюють організаційну спроможність для ефективного цифрового залучення, регуляторному наближенні для узгодження з європейськими рамками, розвитку людських ресурсів для розбудови необхідних компетенцій, та модернізації технологічної інфраструктури для підтримки складних операцій цифрової дипломатії відповідно до кращих практик провідних європейських дипломатичних служб. Створення спеціалізованого Департаменту цифрової дипломатії у структурі МЗС України як окремого інституційного підрозділу з чітким мандатом, адекватними ресурсами та керівництвом високого рівня має консолідувати нині фрагментовані відповідальності за цифрові комунікації, кібердипломатію, координацію

технологічної політики та цифрову публічну дипломатію під єдиним стратегічним керівництвом, забезпечуючи координацію між географічними та тематичними департаментами, розвиваючи інституційну експертизу, та слугуючи координаційним центром для співпраці з європейськими колегами. Толстов зазначає, що просте створення організаційної структури недостатнє без паралельних інвестицій у набір та утримання кваліфікованого персоналу з відповідними технічними навичками, дипломатичною проникливістю та культурними компетенціями, що вимагає конкурентних структур оплати праці для залучення талантів з приватного сектору, гнучких процедур найму для залучення спеціалістів з нетрадиційним походженням, постійних можливостей професійного розвитку для оновлення навичок відповідно до еволюціонуючих технологій, та шляхів кар'єрного просування, що визнають цифрову дипломатію як легітимну спеціалізацію а не тимчасове призначення чи кар'єрний обхідний шлях [14, с. 412-415].

Розробка Національної стратегії цифрової дипломатії України має артикулювати чітке бачення, стратегічні цілі, пріоритетні дії та плани розподілу ресурсів для систематичного розвитку національних спроможностей цифрової дипломатії узгоджених з європейськими підходами та стандартами, надаючи когерентну рамку для координації активностей між різними державними агенціями, забезпечуючи безперервність зусиль за межами виборчих циклів та змін керівництва, та встановлюючи вимірювані індикатори для моніторингу прогресу та оцінювання ефективності втручань. Стратегія має визначати три взаємопов'язані опори: зміцнення цифрової присутності та комунікативних спроможностей для ефективного залучення до наративу у глобальному інформаційному просторі, розбудову кібербезпекової стійкості для захисту критичної інфраструктури та протистояння гібридним загрозам, та регуляторне наближення до європейських стандартів цифрового управління для сприяння інтеграції у єдиний цифровий ринок ЄС. Чекаленко та Воловик підкреслюють, що стратегія має бути не лише декларативним документом з амбіційними цілями але обмеженими механізмами реалізації, а практичною дорожньою картою з конкретними термінами, визначеними відповідальними, розподіленими

ресурсами, рамками моніторингу та механізмами підзвітності для забезпечення справжнього прогресу замість бюрократичних паперових вправ [16, с. 445-448].

Модернізація цифрової інфраструктури МЗС України має охоплювати оновлення застарілих комп'ютерних систем та мережевого обладнання, впровадження сучасних систем управління контентом для вебсайтів посольств та консульств, інтеграцію інструментів управління соціальними мережами для координованої присутності на множинних платформах, розгортання систем аналітики даних для моніторингу ефективності цифрових кампаній та вимірювання впливу комунікаційних активностей, та забезпечення надійного кібербезпекового захисту для запобігання несанкціонованому доступу, витокам даних та скомпрометуванню дипломатичних комунікацій через багаторівневий підхід до безпеки від брандмауерів та систем виявлення вторгнень до протоколів шифрування та безпечних каналів зв'язку. Особливу увагу слід приділити забезпеченню кібербезпеки дипломатичних місій за кордоном, що часто є вразливими до цільових атак через застарілі технології, недостатню обізнаність із безпекою персоналу та обмежені місцеві можливості ІТ-підтримки, що вимагає централізованого забезпечення безпечної ІТ-інфраструктури, обов'язкового навчання з безпеки для всього персоналу, регулярних перевірок безпеки та тестування на проникнення для виявлення вразливостей, та протоколів реагування на інциденти для швидкого локалізування та усунення наслідків у випадку порушень безпеки. Як вбачає аналіз, що технологічна модернізація вимагає не лише одноразових капіталовкладень у апаратне та програмне забезпечення, але й сталого зобов'язання до постійного технічного обслуговування, регулярних оновлень, безперервного навчання персоналу та адаптації до еволюційного технологічного середовища та нових загроз безпеці, що передбачає перехід від проектного підходу до фінансування до систематичних бюджетних асигнувань для цифрової інфраструктури як ключової дипломатичної спроможності.

Програми навчання цифровим навичкам для дипломатичного персоналу МЗС України мають охоплювати базову цифрову грамотність для всіх працівників незалежно від рангу чи спеціалізації, поглиблені навички цифрової

комунікації для працівників, несанкціонований доступ, витіки даних та скомпрометування дипломатичних комунікацій через багаторівневий підхід до безпеки від міжмережових екранів та систем виявлення вторгнень до протоколів шифрування та захищених каналів комунікації. Особливу увагу слід приділити забезпеченню кібербезпеки дипломатичних місій за кордоном, що часто є вразливими до цілеспрямованих атак через застарілі технології, недостатню обізнаність персоналу про безпеку та обмежені місцеві можливості підтримки інформаційних технологій, що вимагає централізованого забезпечення захищеної інфраструктури інформаційних технологій, обов'язкового навчання безпеки для всього персоналу, регулярних аудитів безпеки та тестування на проникнення для виявлення вразливостей, та протоколів реагування на інциденти для швидкого стримування та усунення наслідків у випадку порушень. Як вивчає, що технологічна модернізація вимагає не *merely* одноразових капітальних інвестицій у апаратне та програмне забезпечення, але стійкого зобов'язання до поточного обслуговування, регулярних оновлень, безперервного навчання персоналу та адаптації до еволюціонуючого технологічного ландшафту та нових загроз безпеці, що потребує переходу від проєктного підходу до фінансування до систематичних бюджетних асигнувань для цифрової інфраструктури як основної дипломатичної спроможності [17, с. 478-481].

Програми навчання цифровим навичкам для дипломатичного персоналу МЗС України мають охоплювати базову цифрову грамотність для всіх працівників незалежно від рангу чи спеціалізації, просунуті навички цифрової комунікації для працівників, відповідальних за публічну дипломатію та взаємодію з медіа, спеціалізоване навчання з кібербезпеки для персоналу інформаційних технологій та працівників, що обробляють чутливу інформацію, та стратегічне розуміння геополітичних вимірів цифровізації для керівництва вищого рівня та політичних радників, що формують стратегічні підходи до цифрових питань зовнішньої політики. Навчальні програми мають поєднувати теоретичні модулі про концепції та рамки цифрової дипломатії з практичними практикумами про використання конкретних інструментів та платформ,

випадки-дослідження успішних та невдалих цифрових дипломатичних кампаній для виокремлення уроків, симуляційні вправи для відпрацювання реагування на кризові ситуації в цифровому просторі, та обмінні програми з європейськими дипломатичними службами для ознайомлення з кращими практиками та різноманітними підходами. Бебик та Головатий підкреслюють, що ефективне нарощування потенціалу вимагає не лише одноразових навчальних заходів, але системного професійного розвитку протягом кар'єри, з регулярними курсами оновлення знань, можливостями взаємного навчання для обміну досвідом між практиками, програмами наставництва для передачі неявних знань від досвідчених до молодших працівників, та системами стимулювання, що заохочують безперервне навчання та інноваційність у цифрових дипломатичних практиках [2, с. 501–504].

Розвиток аналітичних спроможностей для політики, заснованої на доказах у цифровій дипломатії має включати створення аналітичного підрозділу у Департаменті цифрової дипломатії, що систематично збирає дані про ефективність цифрових комунікаційних кампаній, моніторинг ставлення аудиторій щодо України у різних країнах та регіонах, відстеження дезінформаційних наративів та їхньої еволюції, аналіз показників залучення на різних цифрових платформах та проведення регулярних оцінок впливу цифрових дипломатичних активностей на досягнення зовнішньополітичних цілей. Використання удосконалених інструментів аналізу даних – від платформ моніторингу соціальних медіа до алгоритмів аналізу тональності – має доповнюватися якісними методами дослідження, включаючи фокус-групи, глибинні інтерв'ю та етнографічні дослідження для глибшого розуміння того, як різні аудиторії сприймають та інтерпретують українські дипломатичні повідомлення, які культурні та політичні контексти формують їхні реакції, та які комунікаційні стратегії найбільш ефективні у різних обставинах. Литвин аргументує, що перехід до підходу, заснованого на даних, у цифровій дипломатії вимагає культурної зміни у дипломатичних організаціях – від традиційної залежності від інтуїції та досвіду до систематичного збирання та аналізу доказів, від показників, орієнтованих на обсяг, як кількість дописів у соціальних медіа,

до індикаторів, орієнтованих на результати, як зміни у громадській думці чи висвітленні у медіа, від епізодичної оцінки окремих кампаній до систематичного моніторингу постійної цифрової присутності та її впливу [6, с. 523–526].

Узагальнюючи пропозиції щодо вдосконалення політики цифрової дипломатії ЄС та інтеграції України, доцільно констатувати, що ефективна реалізація цих рекомендацій вимагає скоординованих зусиль обох сторін, де ЄС має продемонструвати щире відданість у ставленні до України як стратегічного партнера у цифровій сфері через надання належних ресурсів, гнучких процедур та змістовних можливостей участі у європейських цифрових ініціативах, водночас Україна має взяти на себе відповідальність за проведення необхідних інституційних реформ, інвестиції у розбудову потенціалу та узгодження з європейськими стандартами навіть тоді, коли це вимагає складних політичних рішень чи значних фінансових витрат. Створення спільних платформ цифрової безпеки та стратегічних комунікацій може слугувати як конкретний прояв поглибленого партнерства, демонструючи практичну співпрацю поза межами декларативних заяв, забезпечуючи механізми випробування колективної стійкості проти гібридних загроз та надаючи зразок для майбутніх форматів співпраці з іншими партнерськими країнами, що зіштовхуються з подібними викликами. Рекомендації для МЗС України представляють дорожню карту для інституційної трансформації, що узгоджує українську дипломатичну службу з європейськими стандартами та практиками, водночас визнаючи, що справжня інтеграція є процесом, а не подією, який вимагає сталого зобов'язання протягом років та готовності постійно адаптуватися до еволюціонуючого технологічного та геополітичного середовища, підтримуючи динаміку навіть тоді, коли негайні результати не є очевидними чи політична підтримка слабшає в умовах конкуруючих пріоритетів та кризових ситуацій, що характеризують сучасну українську реальність.

Висновки до розділу 3

Проведене дослідження перспектив цифрової дипломатії ЄС та співпраці з

Україною засвідчує, що цифровий вимір європейської інтеграції перетворився з технічного питання на стратегічний пріоритет. Це відображає зміну геополітичної логіки, у якій технологічний розвиток, кіберстійкість та інформаційна безпека формують підґрунтя державного суверенітету. Каталізатором такої трансформації стала російська агресія проти України, що оголила критичну важливість цифрового компонента сучасної гібридної війни та обмеженість попередніх моделей співпраці, орієнтованих на поступові реформи та довгострокові розвиткові програми.

Аналіз цифрової дипломатії як інструменту політики розширення ЄС виявляє суперечність між амбітною риторикою стратегічних документів та обмеженими ресурсами, спрямованими на імплементацію цифрових програм. Це породжує розрив між очікуваннями та реальними можливостями їх виконання і в окремих випадках знижує довіру партнерів до європейських зобов'язань, створюючи простір для конкурентів, які пропонують альтернативні моделі цифрового розвитку. Водночас політика Східного партнерства демонструє еволюцію від технократичного підходу до визнання взаємозалежності між цифровою трансформацією, демократичним врядуванням та геополітичною орієнтацією, хоча її ефективність стримують фрагментація програм, недостатня координація з національними пріоритетами та інституційні слабкості окремих партнерів.

Повномасштабне вторгнення Росії стало переломним моментом, що змусив ЄС перейти до більш інтегрованої моделі цифрової дипломатії, яка охоплює комунікаційні, регуляторні, технологічні та операційні інструменти. Розгортання кіберкоманд для підтримки України, захист критичної інфраструктури, посилення обміну інформацією та публічне викриття інформаційних операцій продемонстрували здатність європейських інституцій до швидкої адаптації, але також виявили структурні обмеження чинних процедур і слабку узгодженість між інструментами допомоги.

Досвід інтеграції України в цифровий простір ЄС засвідчив значний прогрес у регуляторному наближенні, насамперед через ухвалення ключових законів, однак імплементація залишається проблемною через брак

адміністративних ресурсів та інституційну неспроможність забезпечити повноцінне правозастосування. Хоча програми співпраці створили інституційну рамку взаємодії, їхній вплив обмежений через недостатнє фінансування та складність координації. Технічна інтеграція цифрових систем також рухається нерівномірно і потребує довгострокових інвестицій та інституційної стійкості.

Перспективи подальшої цифрової співпраці пов'язані з переходом від моделі «донор—реципієнт» до рівноправного стратегічного партнерства, де Україна виступає не лише отримувачем підтримки, а активним учасником формування колективної безпеки в цифровому просторі. Для цього необхідні спільні платформи цифрової безпеки, оперативної взаємодії та стратегічних комунікацій. Рекомендації для України охоплюють інституційне укріплення, розвиток людського капіталу, модернізацію технологічних систем та посилення аналітичних спроможностей – що є довгостроковим завданням, яке потребує стійкої політичної волі та інвестицій.

Узагальнюючи, цифрова дипломатія стала ключовим напрямом європейської інтеграції України та важливим елементом формування спільної стійкості до гібридних загроз. Досвід співпраці створює прецедент для майбутньої політики ЄС щодо партнерів під зовнішнім тиском і підкреслює потребу в інституціоналізації здобутих уроків для зміцнення європейського цифрового простору в умовах зростаючої глобальної конкуренції.

ВИСНОВКИ

У результаті проведеного дослідження досягнуто мету роботи, що полягала у визначенні концептуальних засад, інституційних особливостей та практичних механізмів політики Європейського Союзу у сфері цифрової дипломатії як складової його зовнішньополітичної діяльності, а також в обґрунтуванні напрямів її удосконалення й оптимізації шляхів інтеграції України у європейський цифровий дипломатичний простір. Послідовний аналіз теоретичних підходів, інституційної архітектури та практичних результатів цифрової дипломатії ЄС дозволив сформувати цілісне уявлення про неї як про багатовимірну систему практик, інструментів та стратегій, що трансформують традиційну дипломатію під впливом цифровізації міжнародних відносин і відкриває нові можливості для реалізації зовнішньополітичних інтересів Європейського Союзу у глобальному інформаційному просторі.

1. Теоретичне осмислення поняття та сутності цифрової дипломатії дало змогу показати, що йдеться не про просте перенесення класичних дипломатичних практик у цифрове середовище, а про якісно новий тип діяльності, що характеризується інтерактивністю, високим рівнем публічності, швидкістю реагування та безпосереднім впливом на масові аудиторії. Це змінює логіку функціонування дипломатичних служб і саму природу міжнародної комунікації. Концептуалізація цифрової дипломатії потребує чіткого розмежування з електронною дипломатією, твіпломатією та публічною дипломатією, аби уникнути термінологічної невизначеності та виокремити предмет дослідження як використання цифрових технологій для досягнення дипломатичних цілей у комунікативному, регуляторному, технологічному та інституційному вимірах зовнішньої політики.

2. Аналіз теоретико-методологічних підходів засвідчив необхідність міждисциплінарного та плюралістичного підходу до вивчення цифрової дипломатії. Реалістичний підхід дозволяє розглядати її як інструмент міждержавної конкуренції за вплив у кіберпросторі; ліберальний інституціоналізм акцентує увагу на ролі міжнародних організацій та норм; конструктивізм – на формуванні наративів та ідентичностей через цифрову

комунікацію; концепція мережевого суспільства – на переході від ієрархічних до горизонтальних форм організації дипломатичної діяльності. Емпіричний аналіз цифрової дипломатії потребує поєднання кількісних методів (аналіз великих даних, метрик охоплення та залучення) з якісними (дискурс-аналіз, кейс-стаді) для оцінки як масштабів комунікації, так і глибинних змін у сприйнятті та поведінці аудиторій.

3. Аналіз інституційної архітектури цифрової дипломатії ЄС виявив складну багаторівневу систему управління, у межах якої повноваження поділяються між Європейською службою зовнішніх дій, Європейською Комісією, Радою ЄС, Європейським парламентом і державами-членами. З одного боку, це забезпечує залучення різноманітної експертизи, з іншого – породжує координаційні виклики й ризики фрагментації. Підрозділ цифрової дипломатії в структурі Європейської служби зовнішніх дій виконує насамперед координаційну та мережеву функції, сприяючи горизонтальній взаємодії між інституціями та делегаціями. Ефективність цієї системи визначається не стільки формальною ієрархією, скільки якістю горизонтальної координації, інтенсивністю неформальних мереж і здатністю гнучко комбінувати інструменти залежно від контексту.

4. Дослідження інструментарію цифрової дипломатії ЄС показало, що він включає широкий спектр засобів: цифрові комунікації в соціальних мережах, програми протидії дезінформації, підтримку цифрової трансформації партнерських країн, інвестиції в цифрову інфраструктуру, кібердипломатичні формати та санкційні механізми. Специфіка європейського підходу полягає в опорі на нормативну та регуляторну силу, а також на довгострокові програми розбудови спроможностей, що дозволяють впливати на інституційні системи та регуляторні середовища третіх країн без використання класичних інструментів «жорсткої сили».

Аналіз цифрової дипломатії у контексті політики розширення ЄС показав, що цифровий вимір поступово став одним із ключових критеріїв інтеграційної готовності країн-кандидатів. Політика Східного партнерства пройшла еволюцію від технічного співробітництва до комплексної стратегії, яка враховує зв'язок

між цифровою трансформацією, якістю врядування та геополітичною орієнтацією. Повномасштабне російське вторгнення в Україну спричинило перехід від переважно нормативного та розвиткового підходу до більш інтегрованої та кризовоорієнтованої моделі цифрової дипломатії, що включає кібердопомогу, захист інфраструктури, підтримку стратегічних комунікацій і протидію інформаційним операціям.

Досвід українсько-європейської цифрової співпраці засвідчив значний прогрес у регуляторному наближенні (ухвалення ключових законів у сфері електронних комунікацій, довірчих послуг, захисту даних), у створенні інституційних рамок для взаємодії (програми EU4Digital, цифрові ініціативи, кібердіалоги), а також у практичній підтримці України в умовах війни (допомога у сфері кібербезпеки, протидія дезінформації, посилення цифрової стійкості). Водночас виявлено проблеми з імплементацією європейських норм, обмеженість фінансових і кадрових ресурсів, складність адаптації універсальних програм до умов країни, що перебуває під тривалою військовою агресією.

5. Сформульовані пропозиції щодо вдосконалення політики цифрової дипломатії ЄС і поглиблення інтеграції України ґрунтуються на необхідності переходу від моделі «донор – реципієнт» до повноцінного стратегічного партнерства. Запропоновано інституціоналізувати співпрацю у сфері кібербезпеки та стратегічних комунікацій через створення спільних структур і постійних платформ взаємодії, розширити участь України в європейських програмах, посилити координацію між інституціями та забезпечити стабільне фінансування цифрових пріоритетів. Для українського зовнішньополітичного відомства рекомендовано розробити національну стратегію цифрової дипломатії, створити спеціалізовані підрозділи, модернізувати технологічну інфраструктуру, інвестувати в підготовку кадрів і розвиток аналітичних спроможностей.

Підсумовуючи результати проведеного дослідження, можна стверджувати, що цифрова дипломатія Європейського Союзу сформувалася як складний, динамічний та стратегічно важливий вимір зовнішньої політики, а її інституційна логіка, інструменти та практики становлять значну цінність для України, яка

перебуває у стані оборони від гібридної та інформаційної агресії. Отримані результати підтверджують, що успішна інтеграція України до європейського цифрового дипломатичного простору потребує не лише регуляторного наближення, а й глибокого переосмислення власних підходів до стратегічних комунікацій, кіберстійкості та зовнішньополітичного позиціювання. Представлене дослідження демонструє, що українсько-європейська співпраця у цифровій сфері має значний потенціал перетворитися на взаємовигідне стратегічне партнерство, здатне зміцнити як національну, так і регіональну безпеку, сприяючи формуванню більш стійкої, відкритої та демократичної цифрової екосистеми Європи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бебик В. М., Головатий М. Ф. Соціальні медіа в дипломатичній практиці: український та європейський контексти. *Українське суспільство: моніторинг соціальних змін*. 2023. Вип. 10. № 1. С. 201–218.
2. Горбатенко В. П., Шедяков В. Є. Цифрова дипломатія в системі міжнародних відносин: теорія та практика. Київ: Інститут держави і права ім. В. М. Корецького НАН України, 2023. 278 с.
3. Камінський Є. Є. Стратегічна автономія ЄС у цифровій сфері: виклики та перспективи. *Стратегічні пріоритети*. 2023. № 2. С. 78–91.
4. Кобзар С. А. Цифрова трансформація публічної дипломатії: виклики та можливості для України. *Актуальні проблеми міжнародних відносин*. 2023. Вип. 154. С. 67–82.
5. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки: схвалено розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Урядовий кур'єр. 2018. № 16.
6. Литвин Л. О. Цифрова дипломатія України в контексті європейської інтеграції: інституційний аспект. *Вісник Київського національного університету імені Тараса Шевченка. Міжнародні відносини*. 2023. Вип. 58. С. 34–41.
7. Мартинов А. Ю. Протидія дезінформації як компонент цифрової дипломатії ЄС. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін*. 2023. Вип. 33. С. 67–75.
8. Матвієнко А. І. Стратегічні комунікації Європейського Союзу в умовах гібридних загроз. *Evropský politický a právní diskurz*. 2023. Т. 10. Вип. 2. С. 45–53.
9. Пашковська І. М. Цифрова трансформація дипломатичних служб: компаративний аналіз. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2023. № 1. С. 145–159.
10. Петренко О. М. Нормативно-правові засади цифровізації зовнішньої політики ЄС. *Науковий вісник Дипломатичної академії України*. 2023. Вип. 30. С. 112–126.

11. Про електронні довірчі послуги: Закон України від 05 жовтня 2017 р. № 2155-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 400.
12. Романюк О. І. Теоретико-методологічні підходи до дослідження цифрової дипломатії в науці про міжнародні відносини. *Politicus*. 2023. Вип. 4. С. 102–109.
13. Сагайдак О. П., Ісаєнко Ю. В. Цифрова дипломатія як інструмент зовнішньої політики сучасних держав. *Гілея: науковий вісник*. 2023. Вип. 178. С. 234–241.
14. Толстов С. В. Кібердипломатія в системі міжнародної безпеки: досвід Європейського Союзу. *Міжнародні відносини: теоретико-практичні аспекти*. 2023. Вип. 11. С. 156–170.
15. Троян С. С., Гончарук А. Д. Європейський Союз як нормативна сила в глобальному цифровому просторі. *Evropský filozofický a historický diskurz*. 2023. Т. 9. Вип. 1. С. 56–64.
16. Чекаленко Л. Д., Воловик М. П. Цифрова дипломатія та публічна дипломатія: концептуальні відмінності та практична синергія. *Зовнішні справи*. 2023. № 5. С. 18–24.
17. Яковюк І. В. Правове регулювання цифрового простору в Європейському Союзі: імплікації для зовнішньої політики. *Право України*. 2023. № 8. С. 89–105.
18. Adler-Nissen R. Digital sovereignty in Europe. *International Affairs*. 2023. Vol. 99, No. 5. P. 1120–1139.
19. Anderson P., Williams S. Strategic Communications in Hybrid Warfare: Lessons from Ukraine. *Defence Studies*. 2023. Vol. 23. No. 4. P. 512–534.
20. Barcevičius E. Digital policies in Eastern Europe. *Journal of Baltic Studies*. 2022. Vol. 53, No. 4. P. 412–430.
21. Bjola C., Holmes M. *Digital Diplomacy: Theory and Practice*. London: Routledge, 2023. 456 p.
22. Borg S. EU digital power projection. *Journal of European Public Policy*. 2023. Vol. 30, No. 6. P. 945–965.

23. Buriak O. EU communication strategy toward Ukraine. *Ukrainian Journal of International Studies*. 2023. No. 4. P. 57–66.
24. Carmen M., Zavattaro S. M. Institutional Adaptation in Digital Diplomacy: The Case of EEAS Organizational Transformation. *Public Administration Review*. 2023. Vol. 83. № 1. P. 110–125.
25. Cooper A., Brown F. Countering Digital Authoritarianism: Lessons for Democratic Resilience. *Journal of Democracy*. 2023. Vol. 34. №. 3. P. 89–104.
26. Council of the European Union. EU Strategic Compass for Security and Defence. Brussels: Council of the EU, 2022. 47 p. URL: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence_en (дата звернення: 25.09.2024).
27. De Luca M., Rossi F. EU Digital Sovereignty and Enlargement Policy. *Journal of European Integration*. 2024. Vol. 46. No. 2. P. 234–256.
28. Eastern Partnership. 20 Deliverables for 2020: Focusing on Key Priorities and Tangible Results. Brussels: European Commission, 2017. URL: <https://www.euneighbours.eu/en/east/stay-informed/publications/20-deliverables-2020> (дата звернення: 28.09.2024).
29. ENISA. Cyber diplomacy practices in the EU. Athens, 2022.
30. ENISA. European cybersecurity threat landscape 2023. Athens, 2023.
31. Eriksen E. EU regulation of platforms and the DSA. *European Law Journal*. 2023. Vol. 29, No. 4. P. 511–529.
32. EU External Action Service. EU-Ukraine Digital Partnership: Progress Report 2023. Brussels: EEAS, 2023. 156 p. URL: https://www.eeas.europa.eu/eeas/eu-ukraine-digital-partnership_en (дата звернення: 15.09.2024).
33. EUISS. Digital geopolitics and European foreign policy. Paris, 2023.
34. EUISS. Hybrid threats and strategic communications. Paris, 2022.
35. European Commission. Digital Europe Programme: Ukraine's Participation Framework. Brussels: European Commission, 2023. 89 p. URL: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme> (дата звернення: 20.09.2024).
36. European Commission. EU Cyber Solidarity Act. Brussels, 2023.

37. European Commission. EU Digital Identity Framework (eIDAS2). Brussels, 2023.
38. European Parliament. Report on EU strategic autonomy in digital policy. Brussels, 2024.
39. Freedom House. Nations in Transit 2024: digital sphere report. Washington, 2024.
40. Handler E., Yehimovich G. Measuring Digital Diplomacy: Metrics, Analytics, and Assessment Frameworks. *Journal of International Communication*. 2024. Vol. 30. №. 1. P. 43–98.
41. Helwig N. EU cyber diplomacy strategy after 2022. *European Security*. 2024. Vol. 33, No. 1. P. 1–19.
42. Hoffman M. EU Cyber Diplomacy Toolbox in practice. *Hague Journal of Diplomacy*. 2024. Vol. 19, No. 1. P. 45–67.
43. Hrechko T. Digital diplomacy tools of the MFA of Ukraine. *Diplomatic Bulletin*. 2024. No. 2. P. 50–61.
44. Hromadska A. Ukraine's participation in European digital market. *Kyiv-Mohyla Law & Politics Journal*. 2023. No. 9. P. 33–47.
45. Jensen L., Kristensen N. Cybersecurity Capacity Building in EU Neighbourhood Policy. *European Security*. 2023. Vol. 32. No. 3. P. 378–399.
46. Karvonen A. Digital infrastructure security. *Global Policy*. 2023. Vol. 14, No. 3. P. 302–320.
47. Keukeleire S. Geopolitics of EU digital partnerships. *Geopolitics*. 2024.
48. Kontinen T. Digital diplomacy innovations in the Baltic States. *Baltic Journal of Political Science*. 2023. No. 12. P. 21–39.
49. Kovalov O. Cybersecurity challenges in Ukraine–EU cooperation. *Journal of Cyber Policy*. 2024. Vol. 9, No. 1. P. 100–118.
50. Kröger T., Olsson K. EU digital regulations and foreign policy. *Journal of Common Market Studies*. 2023. Vol. 61, No. 7. P. 1821–1839.
51. Lanoszka A. Hybrid warfare and digital influence. *Journal of Strategic Studies*. 2022. Vol. 45, No. 9. P. 1215–1234.

52. Manor I. *The Digitalization of Public Diplomacy*. Cham: Palgrave Macmillan, 2023. 489 p.
53. Manor I. *The Digitalization of Public Diplomacy*. Cham: Palgrave Macmillan, 2023. 489 p.
54. Mohan C. Digital resilience and democracy. *Journal of Democracy*. 2024. Vol. 35, No. 2. P. 98–114.
55. NATO CCDCOE. *Cyber defence strategy trends 2024*. Tallinn, 2024.
56. NATO. *NATO's approach to cyber diplomacy*. Brussels, 2023.
57. OECD. *Artificial Intelligence Governance Report 2024*. Paris, 2024.
58. OECD. *Digital Government Index: 2023 Results*. Paris, 2023.
59. Pamment J. Digital Diplomacy as Transmedia Engagement: Aligning Theories of Participatory Culture with International Advocacy Campaigns. *New Media & Society*. 2022. Vol. 24. №. 3. P. 534–551.
60. Panke D. EU normative influence in digital affairs. *European Politics and Society*. 2024. Vol. 25, No. 2. P. 210–229.
61. Paul C. *Strategic Communication: Origins, Concepts, and Current Debates*. Santa Barbara: Praeger, 2022. 312 p.
62. Rathon S. Digital Diplomacy and the Securitisation of Foreign Policy. *The Hague Journal of Diplomacy*. 2023. Vol. 18. №. 2. P. 187–215.
63. Romanenko O., Gaidai M. EU Digital Diplomacy in the Eastern Partnership: Achievements and Challenges. *European Foreign Affairs Review*. 2023. Vol. 28. No. 2. P. 187–210.
64. Ruohonen J. Cybersecurity governance in the EU. *Computer Law & Security Review*. 2024. Vol. 50. P. 105–121.
65. Schneider J., Mueller T. Cyber Resilience and Digital Cooperation: The EU-Ukraine Case. *Journal of Cybersecurity*. 2024. Vol. 10. No. 1. P. 45–67.
66. Schulmann I. Russia's digital influence in Europe after 2022. *Post-Soviet Affairs*. 2023. Vol. 39, No. 6. P. 507–524.
67. Seib M., Taylor K. Digital Diplomacy and International Influence in the Age of Social Media. *International Affairs Review*. 2023. Vol. 31. №. 2. P. 105–178.

68. Sidorov O. EU strategic communication during hybrid threats. *European Security Review*. 2023. No. 18. P. 33–46.
69. Tallinn University. *Digital Diplomacy Review*. Issue 4. Tallinn, 2023.
70. UN DESA. *E-Government Development Index 2022: Europe chapter*. New York, 2023.
71. UNESCO. *Guidelines for digital platforms governance*. Paris, 2023.
72. Vuori J. Digital influence and security threats. *Security Dialogue*. 2023. Vol. 54, No. 2. P. 143–160.
73. Watanabe K., Ishida Y. Digital Infrastructure Partnerships in EU External Relations. *Asia Europe Journal*. 2023. Vol. 21. No. 3. P. 289–308.
74. Watanabe K., Ishida Y. Digital infrastructure partnerships in EU external relations. *Asia Europe Journal*. 2023. Vol. 21, No. 3. P. 289–308.
75. Wigell M. Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy. *International Affairs*. 2023. Vol. 99. №. 1. P. 255–272.
76. Yaremchuk M. European integration and digital transformation of Ukraine. *European Studies Review*. 2024. No. 3. P. 77–91.
77. Zavidniuk O. EU response to digital threats during Russia's war against Ukraine. *European Security Review*. 2023. No. 22. P. 14–28.

АНОТАЦІЯ

Зайко І. Д. Політика ЄС у сфері цифрової дипломатії (магістерська робота). Харків: Харківський національний університет імені В. Н. Каразіна, 2025. 107 с. (рукопис).

Метою магістерської роботи є визначення концептуальних засад, інституційних особливостей та практичних механізмів політики Європейського Союзу у сфері цифрової дипломатії як складової його зовнішньополітичної діяльності.

Об'єктом дослідження є політика Європейського Союзу у сфері міжнародних комунікацій та зовнішньополітичних відносин у цифрову епоху.

Предмет дослідження – зміст, принципи, інституційні механізми та практичні інструменти реалізації політики ЄС у сфері цифрової дипломатії.

У першому розділі розглянуто теоретичні засади дослідження цифрової дипломатії в Європейському Союзі. Проаналізовано поняття та сутність цифрової дипломатії в системі сучасних міжнародних відносин, окреслено основні теоретико-методологічні підходи до її вивчення, а також досліджено нормативно-правові та концептуальні основи цифрової дипломатії ЄС, що формують рамкові умови її реалізації.

У другому розділі проаналізовано інституційно-аналітичний вимір політики ЄС у сфері цифрової дипломатії. Визначено коло суб'єктів формування та реалізації цифрової дипломатії Європейського Союзу, розглянуто інструменти й програми цифрової комунікації, механізми стратегічних комунікацій та протидії дезінформації, а також особливості функціонування цифрової дипломатії ЄС у глобальному та регіональному вимірах.

У третьому розділі досліджено перспективи розвитку цифрової дипломатії ЄС та її співпраці з Україною. Окреслено роль цифрової дипломатії як складової політики розширення Європейського Союзу, проаналізовано ключові напрями цифрової взаємодії між ЄС та Україною в контексті європейської інтеграції, а також запропоновано пропозиції щодо вдосконалення політики цифрової дипломатії ЄС та оптимізації шляхів інтеграції України до європейського цифрового простору.

Ключові слова: інституційні механізми, інформаційна безпека, кібербезпека, міжнародні комунікації, стратегічні комунікації, цифрова дипломатія, цифрова стійкість, цифрове врядування, цифровий простір.

ANNOTATION

Zaiko I. D. EU Policy in the Field of Digital Diplomacy (Master's thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 107 p. (manuscript).

The aim of the master's thesis is to determine the conceptual foundations, institutional specifics and practical mechanisms of the European Union's policy in the field of digital diplomacy as a component of its foreign policy activities.

The object of the research is the policy of the European Union in the field of international communications and foreign policy relations in the digital era. The subject of the research is the content, principles, institutional mechanisms and practical instruments of the EU policy in the sphere of digital diplomacy.

The first section examines the theoretical foundations of studying digital diplomacy in the European Union. It analyses the concept and essence of digital diplomacy in the system of contemporary international relations, outlines the main theoretical and methodological approaches to its research, and studies the normative and conceptual basis of EU digital diplomacy that shapes the framework conditions for its implementation.

The second section analyses the institutional and analytical dimension of the EU policy in the field of digital diplomacy. It identifies the actors involved in shaping and implementing EU digital diplomacy, considers digital communication tools, programmes of strategic communications and countering disinformation, and examines the functioning of EU digital diplomacy at both global and regional levels.

The third section explores prospects for the development of EU digital diplomacy and its cooperation with Ukraine. It outlines the role of digital diplomacy within the EU enlargement policy, analyses key directions of digital interaction between the EU and Ukraine in the context of European integration, and proposes recommendations for improving the EU policy on digital diplomacy and optimising the pathways for Ukraine's integration into the European digital space.

Keywords: cyber security, digital diplomacy, digital governance, digital resilience, digital space, information security, institutional mechanisms, international communications, strategic communications.

ВІДГУК

на кваліфікаційну роботу магістра
студента 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

Зайка Ігоря Дмитровича

на тему: «Політика ЄС у сфері цифрової дипломатії»

Магістерська кваліфікаційна робота Зайка Ігоря Дмитровича присвячена актуальній і суспільно значущій проблематиці цифрової трансформації зовнішньополітичної діяльності Європейського Союзу. Тема дослідження є важливою в контексті посилення ролі цифрових комунікацій у міжнародних відносинах, протидії інформаційним загрозам та формування нових механізмів стратегічної взаємодії між країнами. Автор аргументовано обґрунтовує необхідність дослідження цифрової дипломатії як специфічного інструменту впливу ЄС у глобальному інформаційному просторі.

Робота відзначається логічною структурою та методичною послідовністю. У першому розділі систематизовано наукові підходи до визначення концепту цифрової дипломатії, розкрито її ключові характеристики та взаємозв'язок з поняттями публічної дипломатії, стратегічних комунікацій та кібердипломатії. Другий розділ присвячено аналізу інституційних та регуляторних механізмів реалізації цифрової дипломатії Європейського Союзу, зокрема діяльності Європейської служби зовнішніх дій, платформ протидії дезінформації та впровадженню нормативних актів щодо цифрових послуг. У третьому розділі автор сформулював практичні рекомендації щодо оптимізації взаємодії між Україною та ЄС у цифровій сфері, окреслив перспективні напрями розвитку та

визначив можливості використання інструментів цифрової дипломатії для посилення міжнародної підтримки України.

Оцінка отриманих результатів свідчить про відповідність висновків визначеним меті та завданням дослідження. У роботі показано, що цифрова дипломатія ЄС є комплексною системою заходів, що поєднують регулювання цифрового середовища, інституційні механізми стратегічних комунікацій та інформаційно-аналітичну підтримку партнерських країн. Запропоновані рекомендації мають прикладний характер, узгоджуються з метою роботи і демонструють практичну спрямованість отриманих результатів.

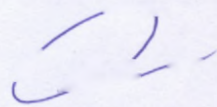
Водночас доцільно було б детальніше висвітлити критерії оцінки ефективності цифрових дипломатичних стратегій та порівняти політику ЄС з аналогічними моделями інших міжнародних акторів. Такі уточнення могли б посилити аргументаційну складову дослідження, але ці зауваження мають рекомендаційний характер і не знижують загальної якості роботи.

Магістерська кваліфікаційна робота Зайка Ігоря Дмитровича відповідає встановленим вимогам до робіт другого (магістерського) рівня вищої освіти, відзначається актуальністю, цілісністю структури та логічністю висновків. Роботу можна рекомендувати до захисту перед екзаменаційною комісією.

Науковий керівник:

д. держ. упр., професор,

професор кафедри міжнародних відносин



Солових В. П.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 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
Зайка Ігоря Дмитровича
на тему: «Політика Європейського Союзу у сфері цифрової дипломатії»

1. Актуальність теми

Тема цифрової дипломатії Європейського Союзу є надзвичайно значущою в умовах цифрової трансформації міжнародних комунікацій та посилення інформаційних загроз у глобальному середовищі. ЄС системно формує власну політику цифрової участі у міжнародних процесах, поєднуючи нормативні інструменти, механізми стратегічної комунікації та інституційну взаємодію для протидії дезінформаційним кампаніям і захисту демократичних процесів.

Обрана тема є актуальною не лише з академічного погляду, але й з практичної точки зору.

2. Характеристика якості виконання розділів роботи

Кваліфікаційна робота має чітку структуру та витримані вимоги до наукового дослідження.

Перший розділ присвячено теоретичним підходам до аналізу цифрової дипломатії.

Другий розділ містить аналіз інституційної системи Європейського Союзу, що забезпечує реалізацію політики цифрової дипломатії.

Третій розділ має прикладний характер і спрямований на оцінку поточних результатів та інструментів реалізації цифрової дипломатії ЄС.

3. Ступінь обґрунтованості висновків

Висновки роботи відповідають поставленим завданням та коректно відображають результати проведеного дослідження. Автор робить узагальнення, що ґрунтуються на нормативних документах ЄС та наукових джерелах.

4. Позитивні сторони роботи

Серед сильних сторін роботи варто відзначити її всебічність, послідовність викладу та добір релевантних джерел. Позитивною є увага до програм та інституцій, що формують цифрову стійкість Європейського Союзу.

5. Недоліки роботи

До недоліків можна віднести недостатній рівень критичної оцінки ефективності окремих інструментів цифрової дипломатії ЄС та брак розширеного порівняльного матеріалу.

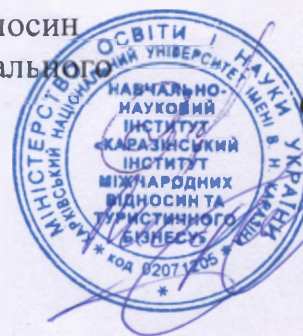
6. Загальна оцінка кваліфікаційної роботи

Кваліфікаційна робота Зайка Ігоря Дмитровича виконана відповідно до вимог, встановлених до магістерських досліджень спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Робота є змістовною, методологічно коректною та практично значущою, заслуговує на високу оцінку і може бути рекомендована до захисту.

Рецензент:

доктор історичних наук, професор,
професор кафедри світової політики,
дипломатії та туристичного бізнесу

ННІ «Каразінський інститут міжнародних відносин
та туристичного бізнесу» Харківського національного
університету імені В.Н. Каразіна



С.І. Лиман