

УДК: 327.8:342.9:004.9
DOI: 10.60022/2(2)-29S

Білоусов Олександр Сергійович

доктор політичних наук, професор кафедри
міжнародних відносин та права
Національний університет «Одеська політехніка», Україна

Bilousov Oleksandr

Doctor of Political Sciences, Professor of the
Department of International Relations and Law
National University «Odesa Polytechnic», Ukraine
ORCID: 0009-0009-2533-7287

Кривдіна Інна Борисівна

кандидат історичних наук, доцент кафедри
міжнародних відносин та права
Національний університет «Одеська політехніка», Україна

Kryvdina Inna

Candidate of Historical Sciences, Associate Professor of the Department
of International Relations and Law
National University «Odesa Polytechnic», Ukraine
ORCID: 0000-0002-1472-3037

ПРАВОВІ ТА ПОЛІТОЛОГІЧНІ ВИМІРИ ЦИФРОВОЇ ПУБЛІЧНОЇ ДИПЛОМАТІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Анотація. У статті досліджується трансформація публічної дипломатії в умовах гібридної війни та цифрової епохи з акцентом на її правовий і політологічний виміри. Цифрова публічна дипломатія постає як ключовий інструмент формування міжнародних наративів, протидії дезінформації та посилення «м'якої сили» держави. Повномасштабне вторгнення російської федерації в Україну у 2022 році засвідчило здатність держав до активного використання цифрових платформ для захисту своїх позицій у глобальному інформаційному просторі, мобілізації міжнародної підтримки та спротиву агресивній пропаганді. Проаналізовано практики цифрової дипломатії демократичних держав, зокрема України, у відповідь на гібридні загрози. Розглянуто міжнародно-правові основи цифрової дипломатії, зокрема Декларацію Ради Європи про свободу вираження в цифровому середовищі, Кіберстратегію ЄС, українські нормативні акти щодо інформаційної безпеки та національного спротиву. Обґрунтовано необхідність формування нормативної бази цифрової дипломатії та інтеграції її в систему національної та міжнародної безпеки. У політичному аспекті висвітлено застосування дипломатії, цифрової кризової комунікації та боротьби за наративи. Публічна дипломатія розглядається як інструмент формування сприятливого міжнародного іміджу, опору дезінформації та розбудови довіри до державних інститутів. Досвід України у сфері цифрової дипломатії представлено як приклад стійкості та стратегічної комунікації для демократичних держав. Зроблено висновок про необхідність інтеграції цифрової дипломатії в стратегії національної безпеки в умовах глобального цифрового протистояння. Стаття базується на міждисциплінарному підході, поєднуючи норми міжнародного права, комунікаційні стратегії та політичні практики.

Ключові слова: цифрова дипломатія, гібридна війна, міжнародне право, інформаційна безпека, публічна дипломатія, дезінформація, стратегічна комунікація, кіберзагрози, Україна, війна наративів.

LEGAL AND POLITICAL DIMENSIONS OF DIGITAL PUBLIC DIPLOMACY IN THE CONDITIONS OF HYBRID WAR

Abstract. This article examines the transformation of public diplomacy in the context of hybrid warfare and the digital era, with a focus on the legal and political dimensions of this phenomenon. Digital public diplomacy is becoming a key tool in shaping international narratives, countering disinformation, and enhancing a state's soft power. The Russian full-scale invasion of Ukraine in 2022 has demonstrated how states

can use digital platforms to defend their positions in the global information space, mobilize support, and resist aggressive propaganda. The article analyzes the mechanisms of digital diplomacy implemented by democratic states, including Ukraine, and their responses to hybrid threats. Legal foundations such as the Council of Europe Declaration on Freedom of Expression in the Digital Environment, the EU Cybersecurity Strategy, and Ukrainian legislation on national resistance and information security are examined. The need to form a regulatory framework for digital diplomacy and integrate it into the system of national and international security is substantiated. Politically, the article highlights the strategic use of Twitter diplomacy (Twiplomacy), digital crisis communication, and narrative warfare. Public diplomacy is considered as a tool for forming a favorable international image, resisting disinformation and building trust in state institutions. Ukraine's digital diplomacy experience is considered a valuable model for other states facing similar information challenges. The article concludes that the integration of digital diplomacy into national security strategies is essential for modern democratic governance in the age of global digital confrontation. The article is based on an interdisciplinary approach, combining the norms of international law, communication strategies and political practices.

Keywords: digital diplomacy, hybrid warfare, public diplomacy, strategic communication, disinformation, international law, Ukraine, information resilience, cyber threats, narrative warfare, information security.

Постановка проблеми. У ХХІ столітті публічна дипломатія зазнала сутнісної трансформації, зокрема через динамічний розвиток цифрових технологій та посилення інформаційних загроз, вона переживає глибоку трансформацію під впливом цифрових технологій, соціальних мереж, глобальних комунікаційних платформ. Цифрова публічна дипломатія перестала бути лише інструментом «м'якої сили», перетворившись на один із фронтів сучасної гібридної війни, яка включає у себе інформаційні, кібератаки, дезінформацію та маніпуляцію громадською думкою. Війна в інформаційному просторі, як це яскраво проявилось у контексті російської агресії проти України, набула безпрецедентного масштабу, де уряди та недержавні актори змагаються за увагу, довіру та легітимність у глобальній публічній сфері. В цих умовах цифрова дипломатія виступає інструментом не лише поширення культурної, політичної та ціннісної інформації, а й складовою захисту національної безпеки.

Сучасна міжнародна політика також дедалі більше зосереджується не лише на збройних, а й на інформаційних засобах впливу. У цьому контексті цифрова публічна дипломатія виступає не лише як засіб просування національних інтересів, але й як засіб протидії дезінформації, пропаганді та кіберактивності супротивників. Гібридна війна, яка поєднує військові, інформаційні, економічні й дипломатичні інструменти, актуалізує потребу в переосмисленні ролі держави у цифровому інформаційному просторі. Правові основи діяльності цифрової дипломатії залишаються фрагментарними, а політична практика вимагає системного аналізу ефективності таких стратегій. Постає проблема визначення місця цифрової публічної дипломатії в системі міжнародних правовідносин та в політичній архітектурі безпеки.

Аналіз останніх досліджень і публікацій. Звернемо увагу, що гібридні загрози, зокрема кібератаки, інформаційні операції та кампанії дезінформації, набули масштабного характеру під час збройної агресії російської федерації проти України, що визнано численними міжнародними інституціями, зокрема Європейським Союзом, НАТО, ООН [8; 14].

У сфері цифрової дипломатії, особливо в контексті гібридних конфліктів, працюють провідні західні та українські дослідники. Питання цифрової публічної дипломатії досліджуються у працях таких науковців, як Джозеф Най (Joseph Nye, США) [17] – автор концепції «м'якої сили» та її цифрового продовження; Ніколас Калл (Nicholas J. Cull, США) – фахівець із публічної дипломатії, один із перших описав її цифровий вимір; James Pamment (Швеція) – досліджує цифрову дипломатію та стратегії цифрового впливу урядів; Corneliu Bjola (Оксфорд) [10] – вивчає взаємодію цифрових технологій і дипломатії. Також, проблематику публічної дипломатії та її трансформації в цифрову форму активно розробляють такі дослідники, як Н. Сноу (Nancy Snow), М. Леонард (Mark Leonard), Ян Мельс, а в українському контексті – Олена Герасименко – аналізує цифрову комунікацію України під час війни; Наталія Белкіна – досліджує інформаційну безпеку в умовах гібридних загроз; Лілія Шишкіна – працює над правовим регулюванням цифрового середовища, Л. Нагорна, А. Васютинський, Н. Костюченко, О. Сятковська, В. Резнік, Л. Корнеєва, А. Грабовський [9, 10, 15-17]. Однак, попри наявні дослідження, бракує комплексного аналізу її правових та політологічних вимірів у контексті гібридної війни.

Сучасні дослідження наголошують на зростанні ролі «м'якої сили» (soft power) у міжнародних

відносинах, водночас відзначаючи небезпеку використання цифрових платформ для дезінформації та втручання у внутрішні справи держав. Проте в умовах гібридної війни спостерігається брак комплексних досліджень, що поєднують правову оцінку та політологічний аналіз цифрової публічної дипломатії, зокрема в контексті досвіду України.

Метою статті є визначення правових та політологічних вимірів цифрової публічної дипломатії в умовах гібридної війни, аналіз її потенціалу як інструменту протидії дезінформації та інформаційній агресії, а також формулювання пропозицій щодо вдосконалення нормативного забезпечення та комунікаційних стратегій.

Завдання статті:

- визначити поняття цифрової публічної дипломатії в сучасному міжнародному контексті;
- проаналізувати її роль як інструменту протидії гібридним загрозам;
- розглянути міжнародно-правові норми, що регулюють діяльність держав у цифровому середовищі;
- виявити виклики та перспективи правового врегулювання цифрової дипломатії.

Виклад основного матеріалу дослідження. Публічна дипломатія визначається як комунікаційна діяльність держави з іноземною громадськістю з метою формування позитивного образу, культурного впливу та політичного капіталу [19]. Цифрова публічна дипломатія – це застосування цифрових технологій та соціальних медіа (соціальні мережі, офіційні вебсайти, відео та стрімінгові сервіси) для здійснення дипломатичних завдань, зокрема комунікації з зовнішньою аудиторією з метою формування позитивного іміджу держави.

Якщо провести порівняння класичної та цифрової публічної дипломатії, то це дозволяє виявити суттєві трансформації у способах комунікації держав із зовнішнім світом. Якщо традиційна дипломатія переважно оперує через офіційні канали та міжурядові зустрічі, то цифрова дипломатія створює нові механізми впливу – через соціальні медіа, цифрові платформи, відеозвернення та цифровий сторітелінг. Вона є значно швидшою, мобільнішою та орієнтованою на масову аудиторію. Водночас цифрова дипломатія посилює виклики безпеки, правового регулювання та протидії інформаційним загрозам, особливо в умовах гібридної війни.

Як складова нової дипломатичної парадигми, цифрова публічна дипломатія, стикається з низкою правових викликів, пов'язаних із транснаціональним характером цифрових комунікацій, нечіткістю юрисдикцій, а також правом на інформацію, свободу слова та безпеку. Особливо ці питання загострюються у контексті гібридної війни, коли держави використовують не лише військову силу, а й інформаційні операції, кібератаки, маніпулятивні кампанії та інші форми впливу через цифрові платформи.

У часи гібридної війни цифрова дипломатія, стає критично важливою для формування спротиву дезінформації та пропаганді, комунікації із закордонною громадськістю; мобілізації міжнародної підтримки та просування стратегічного національного наративу, нейтралізації інформаційного впливу супротивника.

Так, під час повномасштабного вторгнення РФ в Україну (з 24 лютого 2022 року) Міністерство закордонних справ України, Центр стратегічних комунікацій, а також волонтерські проєкти (наприклад, United24 або NAFO) активно використовували цифрові платформи (Twitter, TikTok, YouTube та інші) для донесення правди про події в Україні, спростування фейків, закликів до підтримки санкцій і надання допомоги.

Цифрова публічна дипломатія виконує низку ключових функцій, що інтегрують як класичні дипломатичні завдання, так і нові – пов'язані з комунікаційними викликами цифрової доби. Зокрема, можна виокремити такі функції:

- комунікативну (донесення позицій уряду до іноземної аудиторії). Забезпечення відкритої та оперативної взаємодії з міжнародною громадськістю через цифрові канали. Це включає офіційні заяви, звернення, публікації, відеозвернення, а також дипломатичну діяльність у соціальних мережах (Twitter, Facebook, LinkedIn, TikTok тощо). Комунікативна функція дає змогу державам без посередників формувати позитивний міжнародний імідж та поширювати власний наратив;
- інформаційну (полягає в інформуванні іноземної аудиторії про позицію держави щодо внутрішньої або зовнішньої політики, кризових подій, збройного конфлікту, гуманітарних ініціатив, міжнародного партнерства. У період гібридної війни це особливо важливо як засіб контрпропаганди та протидії дезінформації);
- репутаційну (спрямована на формування, підтримання та захист позитивного іміджу країни за кордоном. Це охоплює культурну дипломатію, просування освіти, туризму, науки, цінностей демо-

кратії, свободи та прав людини. У цифрову епоху це також охоплює боротьбу з кампаніями дискредитації та «інформаційне позиціонування» на міжнародній арені);

- захисну (у період інформаційних воєн цифрова дипломатія виконує оборонну функцію – вона покликана оперативно реагувати на ворожі інформаційні вкиди, фейки, кібератаки проти іміджу держави, інституцій, військових чи дипломатичних дій. Цей елемент також називають “дипломатією безпеки» або частиною інформаційної гігієни держави);

- мобілізаційну (активізація підтримки та взаємодії). Цифрова дипломатія сприяє мобілізації підтримки – фінансової, гуманітарної, військової або політичної – з боку міжнародної спільноти. Успішними прикладами є міжнародні кампанії допомоги Україні, започатковані через цифрові платформи та дипломатичні звернення (зокрема кампанія United24, дипломатична присутність в Instagram, Facebook, YouTube);

- антикризову (реагування на фейки, інформаційні атаки);
- культурну (цифрове культурне представництво).

З правової точки зору, цифрова дипломатія вимагає дотримання норм міжнародного гуманітарного права, норм щодо свободи слова, захисту персональних даних та протидії інформаційним загрозам. Водночас міжнародне право не встигає за швидкістю технологічних змін, що створює правову прогалину. Нестабільне правове поле, лише частково регулює прояви цифрової публічної дипломатії. Важливою є наявність правових механізмів:

- забезпечення інформаційної безпеки;
- захисту свободи слова та доступу до інформації;
- протидії кіберзлочинності та інформаційним атакам;
- відповідальності за маніпулятивну або фейкову інформацію.

З політологічного погляду, цифрова публічна дипломатія виступає інструментом «м'якої сили» «soft power», формуючи сприйняття держави за кордоном та «розумної сили» (smart power). Вона здатна впливати на рішення закордонних громад, урядів, міжнародних організацій не через примус, а через інформаційний вплив і культурний імідж. Це прояв «м'якої сили» та засіб нелінійної дипломатичної взаємодії, зокрема через вплив на громадську думку, підтримку міжнародної коаліції та інформаційний супровід воєнних дій.

Вперше термін «soft power» було запропоновано американським політологом Джозефом Наєм у 1990-х роках [17], а згодом розвинено в контексті нових цифрових реалій.

Цифрова публічна дипломатія виступає складовою «м'якої сили» (soft power), яка, за визначенням Дж. Ная, є здатністю досягати цілей через привабливість, а не примус [18].

У цифровому вимірі «м'яка сила» означає здатність впливати на цільову аудиторію, формувати її уявлення, цінності та поведінку без прямого тиску. Інструментами стають: культурні продукти (фільми, музика, символіка); публікації в соцмережах; інформаційні кампанії; цифрові платформи для діалогу. Наприклад, позитивний імідж України як демократичної, стійкої, сміливої держави формувався не лише через ЗМІ, а й завдяки онлайн-зверненням українського лідерства, цифровим ініціативам, мемам, підтримці лідерів думок та інфлюенсерів у цифровому просторі.

Звернемо увагу й на цифрову дипломатію як елемент «розумної сили». Розумна сила (smart power) – це комбінація жорсткої (примус, санкції, сила) і м'якої сили. У гібридній війні цифрова дипломатія використовується разом з інформаційними спецопераціями, санкційною політикою, кіберконтрзаходами. Її функція – переконати світ у правомірності дій держави, обґрунтувати дипломатичні або військові дії та підготувати міжнародне підґрунтя для прийняття рішень. Наприклад, українська дипломатія активно використовувала цифрові платформи для:

- інформування міжнародних партнерів про ракетні удари;
- звернення до міжнародних організацій;
- формування тиску на агресора через мобілізацію світової спільноти.

У цифровій публічній дипломатії також є інструментальне та стратегічне використання меседжів, наративів, образів, даних для досягнення політичних цілей. Платформи, які зазвичай використовуються для розважального або неформального контенту, стають політичними аренами, де боротьба точиться за лояльність, підтримку, довіру та правду.

Це особливо важливо у боротьбі з інформаційною диктатурою авторитарних режимів, які використовують дезінформацію та цензуру. У відповідь, демократичні держави формують позитивну цифрову ідентичність, базовану на прозорості, відкритості, етиці.

Отже, у гібридній війні цифрова дипломатія:

- забезпечує формування альянсів;
- працює на делегітимацію противника (наприклад, висвітлення воєнних злочинів РФ);
- мобілізує підтримку міжнародної спільноти;
- створює нові форми національної ідентичності у віртуальному просторі.

Політологічна ефективність цифрової дипломатії залежить від:

- інформаційної відкритості та прозорості держави;
- креативності та адаптивності цифрових наративів;
- здатності до швидкого реагування на фейки та пропаганду.

Держава має адаптувати комунікаційні стратегії до нових форматів — інфлюенсерів, дипломатичних акаунтів, платформ, таргетованої реклами, верифікованих меседжів, оперативного спростування фейків (fact-checking у реальному часі).

У випадку України успішними прикладами цифрової дипломатії у 2022–2023 рр. стали активність Міністерства закордонних справ, комунікаційні кампанії Офісу Президента, звернення Президента В. Зеленського до парламентів світу та міжнародних форумах через відеозв'язок; кампанія «Be Brave Like Ukraine»; активність посольств України у Twitter та Facebook (Twitter-дипломатія), платформи United24, волонтерські інформаційні ініціативи.

Проте цифрова публічна дипломатія потребує не лише креативних рішень, але й чіткої координації, законодавчої бази та цифрової безпеки. Без правової визначеності існує ризик зловживання, втрати довіри, маніпуляцій. Необхідним є створення міжнародних стандартів і механізмів контролю за інформаційним впливом у міждержавному середовищі.

Таким чином, у контексті гібридної війни цифрова дипломатія виконує також функції: контрдезінформації; цифрової ідентичності держави; зміцнення довіри до інституцій; мобілізації міжнародної підтримки.

На відміну від класичних дипломатичних каналів, цифрова дипломатія не регламентована Віденською конвенцією про дипломатичні зносини 1961 року.

В офіційних документах Європейського Союзу почав активно використовуватися термін «загроза». У розробленому у 2020 р. Плані ЄС щодо просування демократії зазначено, що «інформація перетворюється на зброю» закордонними акторами, «особливо росією та Китаєм» [12], і виникає в результаті «загрози демократії, яка вимагає всеосяжної та колективної відповіді». Раніше, у 2019 р., ЄВСС розглядала Китай як економічного конкурента та системного суперника [13].

Цифрова дипломатія діє в умовах транснаціонального цифрового середовища. Виникає конфлікт юрисдикцій: наприклад, контент, розміщений дипломатичним відомством у Facebook, може бути видалений або обмежений відповідно до політики платформи, яка базується на законодавстві США, а не міжнародному праві. Цифрова дипломатія вразлива до кібератак, підміни особи (spoofing), витоку інформації. Це ставить питання про захист офіційних акаунтів дипломатів, цифрових платформ, веб-ресурсів посольств – у тому числі як об'єктів критичної інформаційної інфраструктури.

Міжнародне право досі не має чітко визначеної відповідальності за інформаційні атаки та дезінформацію, які є ключовими елементами гібридної війни. Попри зусилля ЄС, НАТО, ОБСЄ, Ради Європи, не існує уніфікованої конвенції, яка б окреслювала допустимі та недопустимі форми цифрового інформаційного впливу між державами.

Станом на сьогодні цифрова дипломатія не має окремого комплексного регулювання у міжнародному праві, однак функціонування здійснюється фрагментарно, через такі інституції та ключові міжнародні документи:

Організацію Об'єднаних Націй (ООН):

- діяльність Групи урядових експертів з кібербезпеки (GGE) [20]. Звіти Групи за 2010, 2013, 2015, 2021 роки – закладають принципи відповідальної поведінки держав у кіберпросторі;
- Відкрита робоча група (OEWG), займаються розробкою норм й рекомендацій щодо відповідального поведіння держав у кіберпросторі (2021). Звіти цієї групи озглядають питання безпеки, норм, CBMs і потенційних домовленостей щодо кіберзброї;
- Статут ООН [8] (особливо принципи ненападу, суверенітету та невтручання);
- ITU (Міжнародний союз електрозв'язку) відповідає за технічні стандарти, інфраструктуру та глобальну цифрову політику;
- UNESCO – опікується етичними, правозахисними та інформаційними аспектами в умовах цифровізації.

Європейський Союз (ЄС):

- Європейська служба зовнішніх справ (EEAS) має підрозділ Hybrid Threats and Cybersecurity, який відповідає за кібердипломатію;
- ENISA – Європейське агентство з кібербезпеки, займається питаннями технічної підтримки цифрової дипломатії. Cybersecurity Act (2019) – регламент про сертифікацію та роль ENISA;
- EU Cyber Diplomacy Toolbox (2017) – механізми для узгодженої дипломатичної реакції на кіберінциденти; набір заходів для спільного реагування на зловмисну кібердіяльність;
- Стратегія з кібербезпеки – EU Cybersecurity Strategy (2020) – стратегія цифрової стійкості, захисту критичної інфраструктури та просування глобальних норм;
- Кодекс практики з протидії дезінформації (2022), регламент DSA (Digital Services Act);
- EU Strategic Compass for Security and Defence (2022) – інтегрує цифрову дипломатію до зовнішньополітичної стратегії.

НАТО:

- має Центр передового досвіду з кібероборони у Таллінні (CCDCOE). Tallinn Manual 2.0 (2017) – неофіційний довідник застосування міжнародного права в кіберконфліктах ;
- NATO Cyber Defence Pledge (2016) – зобов'язання держав-членів зміцнювати власну кіберстійкість. Визнало кіберпростір «операційною доменою» (operation domain) та як простір бойових дій (2016), концепція «кіберзахисної дипломатії»;
- NATO Strategic Concept (2022) – вперше включає цифрові загрози як серйозний виклик колективній безпеці;
- співпрацює з партнерами щодо реагування на кібератаки через дипломатичні, економічні та військові механізми.

Організацію з безпеки і співробітництва в Європі (ОБСЄ):

- розробила міри довіри у сфері кібербезпеки (Confidence Building Measures – CBMs), що сприяють відкритості між державами.

Раду Європи:

- ініціатор Будапештської конвенції про кіберзлочинність (2001), яка є юридичною базою боротьби з незаконною діяльністю в кіберпросторі, першим міжнародним документом про боротьбу з кіберзлочинами, включаючи дезінформацію – рекомендації щодо свободи вираження в цифровому середовищі.

Інші інституції:

- Групу G7, G20, ОЕСР – формують глобальні політики у сфері цифрових технологій, ШІ та кібербезпеки;
- ICANN, IETF, W3C – технічні організації, які регулюють інфраструктуру Інтернету;
- Global Forum on Cyber Expertise (GFCE) – платформа співпраці в царині кіберзнань і цифрового розвитку.

А також функціонує в межах норм:

- Міжнародного пакту про громадянські і політичні права [5] – стаття 19 гарантує свободу висловлювання, але дозволяє її обмеження для захисту нацбезпеки;
- Європейської конвенції з прав людини [4] – стаття 10 визначає рамки свободи вираження;
- Резолюції ГА ООН A/RES/73/27 (2018) – про відповідальну поведінку держав у кіберпросторі, включаючи заборону шкідливої інформаційної діяльності;
- Digital Services Act (ЄС, 2022) – нового регламенту ЄС, що встановлює відповідальність онлайн-платформ за поширення дезінформації, hate speech тощо [9];
- Парижського заклику до довіри та безпеки в кіберпросторі (2018) – політичної декларації для формування відповідального кіберпростору.

Що стосується національного законодавства, то цифрова публічна дипломатія спирається на такі Українські нормативні акти:

- Доктрину інформаційної безпеки України (від 25 лютого 2017 року) – стратегічний документ, який визначає цифрову комунікацію як інструмент захисту націнтересів [2];
- Закон України «Про основи національного спротиву» (2021) – інформаційна боротьба як складова спротиву [1];
- Стратегію інформаційної безпеки України (від 28 грудня 2021 року) – акцент на боротьбі з дезінформацією та зміцнення міжнародного іміджу [3].

Проте відсутній міжнародний договір, який би безпосередньо регулював специфіку цифрової дипломатії, її правовий статус, межі відповідальності та захист.

З міжнародно-правової точки зору, держави зобов'язані не використовувати цифрові канали для втручання у внутрішні справи інших держав (ст. 2 Статуту ООН) [8], однак в реальності цифрова дипломатія часто межує з інформаційною війною.

Так, після повномасштабного вторгнення РФ у 2022 році акаунти Міністерства закордонних справ України, а також Посольств України у США, Великій Британії, Франції тощо, стали активними платформами цифрового спротиву. Через офіційні акаунти поширювались звернення до міжнародної спільноти, відео з доказами злочинів РФ, заклики до санкцій, бойкотів, підтримки України.

У 2022-2023 роках Україна зазнала низки кібератак на вебсайти своїх дипломатичних установ, зокрема DDoS-атак на сайти МЗС та консульств. Наприклад, у жовтні 2022 року були атаковані сайти Посольства України в Польщі та Чехії. Це вкотре підкреслило потребу в посиленні кіберзахисту цифрової дипломатичної інфраструктури.

Для правового регулювання цифрової дипломатії в Україні необхідно:

- створення підзаконного акту, який би чітко визначив: статус цифрової дипломатії у системі зовнішньополітичної діяльності; регламент користування офіційними акаунтами дипломатів; вимоги до кіберзахисту цифрових ресурсів дипломатичних установ;
- розробка «Цифрової стратегії публічної дипломатії України», яка передбачала б: пріоритетні цілі в онлайн-присутності держави; сегментування цільових аудиторій у світі; інтеграцію цифрових інструментів у культурну та економічну дипломатію;
- законодавче визнання цифрових комунікацій дипломатів як форм офіційної комунікації;
- посилення кіберзахисту дипломатичних акаунтів і сайтів, створення централізованої системи верифікації акаунтів дипломатичних установ;
- інституційне оформлення цифрової дипломатії, створення окремого департаменту цифрової дипломатії при МЗС, за прикладом Естонії або Франції, з функціями стратегії, SMM, аналітики цифрових загроз.

Взагалі, цифрова публічна дипломатія стає інструментом об'єднання міжнародних коаліцій та створення тиску на агресора через інформаційні кампанії.

Як приклади міжнародної взаємодії можна навести створення платформи EUvsDisinfo у ЄС, яка займається боротьбою з російською дезінформацією; G7 Rapid Response Mechanism (RRM) – координує дії у сфері протидії іноземному впливу; група стратегічних комунікацій НАТО (STRATCOM COE, Рига) – робить аналітику та підготовку рекомендацій щодо цифрової комунікації; глобальні ініціативи: «Freedom Online Coalition», «Paris Call for Trust and Security in Cyberspace» – створюють стандарти цифрової етики.

Водночас існують серйозні виклики:

- правова невизначеність – відсутність міжнародного договору про правила поведінки у сфері цифрової дипломатії;
- нечітке визначення меж «пропаганди» та «публічної дипломатії». Підміна понять – використання терміну «дипломатія» для прикриття інформаційних атак;
- використання цифрових платформ як «інструментів війни»;
- маніпуляція громадською думкою через алгоритмічні системи – держави можуть зловживати платформами, просуваючи фейки або підриваючи демократичний дискурс;
- ризик конфлікту з правами людини – боротьба з дезінформацією може обмежити свободу слова, якщо немає чітких меж.

З огляду на виклики цифрової епохи, необхідно:

- розробити міжнародні стандарти цифрової дипломатії;
- посилити відповідальність платформ за сприяння дезінформації;
- запровадити механізми верифікації офіційної інформації в умовах війни;
- визначити у національному праві роль публічної дипломатії як частини кібербезпеки та національної комунікаційної політики.

У цьому контексті перспективними є ініціативи ЄС у сфері цифрових сервісів (Digital Services Act), а також створення механізмів кібердипломатії в межах міжнародних організацій.

Таким чином, правові аспекти цифрової дипломатії залишаються складною і недостатньо врегульованою сферою. У контексті гібридної війни її значення зростає, а з ним – і потреба у чіткому міжнародно-правовому регулюванні. Необхідним є формування міждержавних механізмів відповідальності за зловживання цифровими інструментами, захисту цифрових представництв та розробки універсальних правил взаємодії у цифровому дипломатичному середовищі. Глобальний цифровий простір вима-

гає нових підходів до регулювання, кооперації та етичних стандартів міжнародної взаємодії.

В сучасних реаліях, цифрова публічна дипломатія – це не просто інструмент комунікації, а стратегічний ресурс держави у сфері безпеки, політики та міжнародного впливу, який в умовах гібридної війни перетворюється на ключовий інструмент державної комунікації, міжнародної мобілізації та протидії ворожим інформаційним впливам. Її ефективність значною мірою залежить від здатності держави:

- оперативно реагувати на фейки й ворожі наративи;
- використовувати цифрові платформи для побудови позитивного міжнародного іміджу;
- діяти в рамках міжнародного права, не порушуючи свободу слова і права людини.

Цей інструмент є частиною сучасного арсеналу політичної боротьби, де слово, зображення та меседж можуть впливати сильніше, ніж зброя, а ефективність у гібридній війні залежить від здатності до адаптації, креативності, швидкого реагування та інформаційної прозорості.

Взагалі, політологічно цифрова дипломатія в умовах гібридної війни зміщується в бік інформаційного фронту, де держави змагаються не лише за територію, а й за довіру, підтримку, інформаційну перевагу. Україна стала прикладом цифрової мобілізації дипломатичних і громадянських ініціатив у відповідь на російську агресію.

Правовий вимір цієї діяльності наразі фрагментарний. Міжнародне право лише починає осмислювати цифрову комунікацію як об'єкт правового регулювання. Тому необхідно:

- розробити міжнародні стандарти цифрової дипломатії;
- чітко визначити межі допустимої цифрової протидії;
- гармонізувати національні законодавства з міжнародними зобов'язаннями щодо інформаційної безпеки, прав людини і боротьби з кіберзагрозами.

Загалом, цифрова публічна дипломатія є простором перетину права, технологій і політики. Її правове осмислення потребує міждисциплінарного підходу та широкої міжнародної співпраці.

Отже, цифрова публічна дипломатія є сучасним викликом і водночас шансом для формування нової етики міжнародного діалогу в умовах інформаційної війни.

Висновки. В статті обґрунтовано, що цифрова публічна дипломатія в умовах гібридної війни постає як важливий елемент національної безпеки та зовнішньої політики. Досліджено вплив різних факторів на її ефективність, яка залежить перш за все від балансу між свободою слова та інформаційною безпекою, політикою, правовою регламентацією та інноваційністю комунікації.

Для України важливим завданням є формування системної політики цифрової дипломатії, розробка нормативно-правових актів, що регулюють її реалізацію, а також активна участь у міжнародних ініціативах із протидії дезінформації. Подальші дослідження повинні зосередитись на уніфікації термінології, створенні етичного кодексу цифрової дипломатії та розбудові міжнародної нормативної платформи.

Література

1. Закон України “Про основи національного спротиву” (2021). URL: <https://zakon.rada.gov.ua/laws/show/1702-20#Text> (дата звернення: 02.05.2025)
2. Доктрина інформаційної безпеки України (від 25 лютого 2017 року). URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 02.05.2025)
3. Стратегія інформаційної безпеки України (від 28 грудня 2021 року). URL: <https://zakon.rada.gov.ua/laws/show/n0080525-21#Text> (дата звернення: 02.05.2025)
4. Європейська конвенція з прав людини. URL: https://www.echr.coe.int/documents/d/echr/convention_ukr (дата звернення: 03.05.2025)
5. Міжнародний пакт про громадянські і політичні права. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 02.05.2025)
6. Пархомчук, О. Цифрова дипломатія України: інструмент гібридного спротиву. Дипломатичні студії, №3, 2022. С. 12–19.
7. Резнік В. Ю. Цифрова дипломатія: виклики та можливості. Гілея. 2021. № 165. С. 67–71.
8. Статут Організації Об'єднаних Націй. URL: <https://www.un.org> (дата звернення: 01.05.2025)
9. Сятковська О. М. Публічна дипломатія України в умовах гібридної війни / Наукові записки ІПіЕНД ім. І. Ф. Кураса НАН України. 2020. № 4. С. 49–61.
10. Bjola, C., & Holmes, M. (Eds.). (2015). Digital Diplomacy: Theory and Practice. Routledge.
11. Digital Services Act (ЕС, 2022) The Digital Services Act package. Directorate-General CONNECT

of the European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (дата звернення: 30.04.2025)

12. European Commission (2020) On the European democracy action plan. March, Brussels. P. 19. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN> (дата звернення: 01.05.2025).

13. European Commission and HR/VP (2019) EU-China – A strategic outlook. March, Strasbourg. P.1. URL: <https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategicoutlook.pdf> (дата звернення: 01.05.2025)

14. EU Strategic Compass for Security and Defence, 2022.

15. Leonard, M. (2002). Public Diplomacy. The Foreign Policy Centre.

16. Melissen, J. (Ed.). (2005). The New Public Diplomacy: Soft Power in International Relations. Palgrave Macmillan.

17. Nye, J. S. (2011). The Future of Power. Public Affairs.

18. Nye, J. S. (2004). Soft Power: The Means to Success in World Politics. PublicAffairs.

19. Snow, N. (2020). Public Diplomacy and Strategic Communication: Origins, Strategies, and Tools. Palgrave Macmillan.

20. UN GGE and OEWG Reports on Cybersecurity. URL: <https://www.un.org/disarmament/ict-security/> (дата звернення: 01.05.2025).

References

1. Zakon Ukrainy “Pro osnovy natsional’noho sprotyvu” (2021). URL: <https://zakon.rada.gov.ua/laws/show/1702-20#Text> (accessed May 02, 2025)

2. Doktryna informatsiynoyi bezpeky Ukrainy (2017). URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (accessed May 02, 2025)

3. Stratehiya informatsiynoyi bezpeky Ukrainy (2021). URL: <https://zakon.rada.gov.ua/laws/show/n0080525-21#Text> (accessed May 02, 2025)

4. Yevropeys’ka konventsia z prav lyudyny. URL: https://www.echr.coe.int/documents/d/echr/convention_ukr (accessed May 03, 2025)

5. Mizhnarodnyy pakt pro hromadyans’ki ta politychni prava. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (accessed May 03, 2025)

6. Parkhomchuk, O. (2022). Tsyfrova dyplomatiya Ukrainy: instrument hibrydnogo sprotyvu. Dyplomatychni studiyi. №3, 12–19.

7. Reznik V. YU. (2021) Tsyfrova dyplomatiya: vyklyky ta mozhlyvosti. Hileya. № 165. S. 67–71.

8. Statut Orhanizatsiyi Ob'yednanykh Natsiy. URL: <https://www.un.org> (accessed May 01, 2025)

9. Syatkovs’ka O. M. (2020) Publichna dyplomatiya Ukrainy v umovakh hibrydnoyi viyny. Naukovi zapysky IPIEND im. I. F. Kurasa NAN Ukrainy. № 4. S. 49–61.

10. Bjola, C., & Holmes, M. (Eds.). (2015). Digital Diplomacy: Theory and Practice. Routledge.

11. Digital Services Act (YES, 2022) The Digital Services Act package. Directorate-General CONNECT of the European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (accessed May 02, 2025)

12. European Commission (2020) On the European democracy action plan. March, Brussels. P. 19. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN> (accessed May 02, 2025).

13. European Commission and HR/VP (2019) EU-China – A strategic outlook. March, Strasbourg. P.1. URL: <https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategicoutlook.pdf> (accessed May 03, 2025)

14. EU Strategic Compass for Security and Defence, 2022.

15. Leonard, M. (2002). Public Diplomacy. The Foreign Policy Centre.

16. Melissen, J. (Ed.). (2005). The New Public Diplomacy: Soft Power in International Relations. Palgrave Macmillan.

17. Nye, J. S. (2011). The Future of Power. Public Affairs.

18. Nye, J. S. (2004). Soft Power: The Means to Success in World Politics. PublicAffairs.

19. Snow, N. (2020). Public Diplomacy and Strategic Communication: Origins, Strategies, Tools. Palgrave Macmillan.

20. UN GGE ta OEWG Reports on Cybersecurity. URL: <https://www.un.org/disarmament/ict-security/> (accessed May 03, 2025).