

Львівський національний університет імені Івана Франка
Факультет міжнародних відносин
Кафедра міжнародних комунікацій та цифрової дипломатії
Лабораторія цифрової дипломатії
Центр міжнародної безпеки та партнерства
Ягеллонський університет в Кракові
Інститут політичних наук і міжнародних відносин

**ЦИФРОВА ДИПЛОМАТІЯ УКРАЇНИ:
СТРАТЕГІЧНІ КОМУНІКАЦІЇ,
АНАЛІЗ ДАНИХ, КРИЗОВЕ УПРАВЛІННЯ**

**Матеріали міжнародної
наукової конференції**

14 листопада 2025 р.
Львів

УДК [327.82:004.738.5:316.77]:005.334](06)

Ц 72

Цифрова дипломатія України: стратегічні комунікації, аналіз даних, кризове управління. Матеріали міжнародної наукової конференції. Львів, 14 листопада 2025 р. / Упорядники: М. Мальський, Р. Вовк, О. Кучик. – Львів: Львівський національний університет імені Івана Франка, 2025. – 120 с.

У збірнику опубліковані тези виступів учасників конференції, присвячені актуальним проблемам цифровізації, аналізу та прогнозування у сфері політичних, економічних, правничих, соціологічних та історичних наук.

Матеріали подано в авторській редакції. За зміст, оприлюднені факти та поданий цифровий і статистичний матеріал відповідальність несуть автори.

© Центр міжнародної безпеки та партнерства, 2025

© Львівський національний університет імені Івана Франка, 2025

Ivan Franko National University of Lviv
Faculty of International Relations
Department of International Communications and Digital Diplomacy
Data Diplomacy Lab
International Security and Partnership Centre
Jagiellonian University in Kraków
Institute of Political Sciences and International Relations

UKRAINE'S DIGITAL DIPLOMACY: SYNERGY OF REALITY AND VIRTUALITY

**Proceedings of the international
scientific conference**

November 14, 2025
Lviv

Ukraine's Digital Diplomacy: Strategic Communications, Data Analysis, Crisis Management. Proceedings of the international scientific conference. (Lviv, November 14, 2025) / Edited by: Malskyy M., Vovk R., Kuchyk O. – Lviv: Ivan Franko National University of Lviv. – 2025. – 120 p.

The proceedings contain abstracts of the participants of International scientific conference, discovering a wide range of issues of theory and practice of digitalization, analysis and forecasting in the field of political, economic, legal, sociological and historical sciences.

The authors are responsible for the content, facts and submitted digital and statistical material. Abstracts are published in the author's edition.

ЗМІСТ

Юрій Боднар Штучний інтелект як дипломат: майбутнє переговорів і репутацій у цифрову епоху	8
Vasylyna-Mukhailyna Burek Rezyliencja w Ukrainińskiej dyplomacji publicznej: projekcja 'miękkiej siły' podczas pełnoskalowej agresji Rosji.....	11
Діана Васишлишин Міжнародна співпраця та багатосторонні ініціативи у сфері кіберпростору	15
Роман Вовк, Маркіян Мальський Використання штучного інтелекту для виявлення дезінформації у зовнішній політиці	19
Орест Гогоша, Юрій Марченко Кіберпростір як поле геополітичного протистояння США, КНР та РФ	25
Віталій Гутник Використання цифрових технологій міжнародним кримінальним судом: шлях чи перешкода для міжнародного правосуддя?	30
Ігор Доцяк, Богдан Гнатів Е-демократія в умовах війни за незалежність України: ризики та перспективи.....	34
Іванна Земан X-дипломатія як інструмент сучасної міжнародної комунікації	38
Ігор Земан Нові виклики та переваги цифрової дипломатії для міжнародного права	40

Ігор Іжнін, Любомир Харченко	
Інструменти цифрової дипломатії в умовах трансформації міжнародних відносин	43
Ганна Іпполітова	
Розвиток цифрового простору України як складова гармонізації з політиками Європейського Союзу	48
Оксана Когут-Ференс	
Стратегічні комунікації України в умовах війни.....	52
Олександр Кучик, Наталія Стручок	
Міжнародний імідж держави як об'єкт кризового менеджменту у цифровому комунікаційному середовищі	54
Аліна Лега	
Досвід НАТО у сфері боротьби з інформаційними загрозами в Україні	57
Włażej Matuła	
United24 as a Tool of Ukrainian Public Diplomacy	64
Solomiia Melnyk	
Dziedziczenie aktywów cyfrowych w prawie prywatnym międzynarodowym: obecne wyzwania i perspektywy harmonizacji	69
Марія Павлюх	
Інформаційна безпека у польському медіапросторі: наративи російської пропаганди (на прикладі блогера мережі «Х» Мартіна Демірова)	75
Іван Панкевич, Маркіян Панкевич	
Діджиталізація виборів: європейський досвід.....	80
Костянтин Поліщук	
Поняття та інструменти аналізу й вимірювання ефективності цифрового дипломатичного впливу.....	84

Світлана Прийма Управління ризиками підприємства в умовах цифрової трансформації.....	89
Agnieszka Sawicz Zarządzanie strachem i zarządzanie pamięcią jako narzędzia wojny hybrydowej	93
Михайло Сінаюк Система цифрової пропаганди Російської Федерації та стратегія проактивної протидії.....	98
Віталій Ткачук Етичні рамки цифрової активності суб'єктів політичних процесів	101
Надія Харченко Новий інформаційний порядок цифрової доби	105
Дарина Чижова Цифрові нарративи стратегічного залякування: кейс російської «зброї судного дня».....	109
Roman Chuprin Sport as a Digital Battlefield: Data, Diplomacy, and Failed Neutrality in the Russian–Ukrainian War.....	113
Роман Шипка Кібербезпека та цифрова дипломатія.....	116

*Юрій Боднар
студент
Львівський національний університет
імені Івана Франка*

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ДИПЛОМАТ: МАЙБУТНЄ ПЕРЕГОВОРІВ І РЕПУТАЦІЙ У ЦИФРОВУ ЕПОХУ

Цифровізація дипломатії стала одним із найпомітніших трендів XXI століття. Технологічна революція, штучний інтелект (ШІ) та аналітика великих даних не лише змінили інструменти політичної комунікації, а й створили передумови для появи нового типу актора – «алгоритмічного дипломата». Якщо традиційна дипломатія спиралася на інтуїцію, досвід і особисту харизму переговорників, то сучасна – дедалі частіше на точність прогнозів, аналітичну об'єктивність і швидкість обробки інформації. У цьому контексті ШІ перестає бути лише технічним інструментом: він стає **посередником**, який формує рішення, визначає рамки дискурсу та навіть впливає на міжнародну репутацію держав.

1. Штучний інтелект як аналітичний дипломат

ШІ здатний опрацьовувати колосальні обсяги інформації, виявляти закономірності в поведінці держав, політиків та громадської думки. Алгоритми машинного навчання аналізують політичні заяви, медійні патерни, економічні тенденції й навіть тональність висловлювань, формуючи точні прогнози щодо можливих сценаріїв переговорів.

У структурі ЄС, НАТО та ООН уже тестуються системи, які визначають, коли доцільно ініціювати дипломатичний контакт, а коли – утриматися. Таким чином, ШІ стає інструментом превентивної дипломатії, що дозволяє передбачити конфлікт і пом'якшити його ще до публічного загострення.

Для України подібні технології мають особливе значення – у контексті війни та протидії дезінформації. Алгоритмічний аналіз інформаційного простору дає змогу виявляти кампанії впливу,

розрізняти автентичні настрої та скоординовані фейки, будуючи ефективну комунікаційну стратегію з партнерами.

2. Етичні та правові виклики алгоритмічної дипломатії

Якщо рішення формуються за участі ШІ, виникає фундаментальне питання: хто несе відповідальність за наслідки алгоритмічного вибору?

ШІ може не лише обробляти дані, а й відтворювати людські упередження, зафіксовані у навчальних вибірках. Це створює ризик появи цифрової упередженості у міжнародних рішеннях — коли штучна система несвідомо повторює політичні або культурні патерни певних країн. Саме тому дипломатія майбутнього має включати етичний контроль штучного інтелекту. Йдеться про розробку міжнародного «Кодексу алгоритмічної поведінки», який регулюватиме використання ШІ в аналітичних процесах зовнішньої політики.

Такий кодекс повинен гарантувати:

- прозорість джерел даних;
- пояснюваність алгоритмів;
- неможливість використання ШІ для маніпуляцій або дискримінації.

У цьому аспекті ШІ виступає не стільки заміною дипломата, скільки його етичним дзеркалом – змушуючи людство усвідомити власну відповідальність за рішення, делеговані машинам.

3. Репутаційна дипломатія в епоху алгоритмів

Дипломатія сьогодні відбувається не лише в залах переговорів, а й у Twitter, Telegram чи TikTok. Алгоритми визначають, які теми стають вірусними, як формується ставлення до держав, хто виглядає агресором, а хто – жертвою.

У цьому середовищі ШІ стає архітектором міжнародного іміджу: він фіксує реакції користувачів, моделює тональність дискусій і пропонує урядам комунікаційні стратегії в реальному часі.

В умовах постправди, коли факти часто поступаються емоціям, саме аналітичні системи здатні утримувати стратегічну стабільність. Країни, які вміють грамотно використовувати ШІ для моніторингу нарративів, мають інформаційну перевагу. Дипломатія більше не є

лише мистецтвом слова — вона стає мистецтвом цифрового контексту.

4. Український вимір алгоритмічної дипломатії

Україна сьогодні є прикладом того, як цифрові технології стають частиною національної стратегії. З початку повномасштабного вторгнення Україна використовує інструменти відкритих даних, платформ цифрових комунікацій і аналітичних систем для протидії російській дезінформації та підтримки довіри міжнародної спільноти. Інтеграція ШІ у зовнішньополітичну діяльність — це наступний крок. Українська модель цифрової дипломатії поєднує технологічну ефективність із ціннісною автентичністю: правду, відкритість і людяність.

Саме ці принципи мають стати основою для формування нового типу дипломатії — алгоритмічно-гуманістичної, де штучний інтелект підсилює людські моральні орієнтири, а не підміняє їх.

Висновки

Штучний інтелект перестає бути інструментом — він стає співучасником дипломатичного процесу. Його головна перевага — аналітична точність, головний ризик — відсутність моралі. Майбутнє дипломатії полягає не у протиставленні людини й машини, а у створенні симбіозу, де людина надає алгоритму сенс, а алгоритм — людині аналітичну силу. Україна, як держава, що водночас веде війну й цифрову трансформацію, має шанс стати одним із центрів формування нової епохи — епохи етичного штучного інтелекту у глобальній політиці.

Vasylyna-Mykhailyna Burek
magister

Lwowska Obwodowa Administracja Państwowa,
Alumna of Uniwersytet Jagielloński

REZYLIENCJA W UKRAIŃSKIEJ DYPLOMACJI PUBLICZNEJ: PROJEKCJA 'MIĘKKIEJ SIŁY' PODCZAS PEŁNOSKALOWEJ AGRESJI ROSJI

Współczesna faza wojny rosyjsko-ukraińskiej doprowadziła do zasadniczej redefinicji pozycji dyplomacji publicznej w systemie polityki zagranicznej Ukrainy: instrument, który do 2022 r. pełnił głównie funkcje uzupełniające wobec dyplomacji tradycyjnej (kształtowanie pozytywnego wizerunku państwa, podtrzymywanie wymiany kulturalnej, wprowadzanie ukraińskiej narracji do obiegu instytucji międzynarodowych), został przekształcony w jeden z podstawowych kanałów realizacji podmiotowości międzynarodowej państwa. Wskazuje to na jakościową zmianę statusu tego wymiaru aktywności - komunikacja skierowana do audytoriów zagranicznych zaczęła stanowić warunek utrzymania poparcia politycznego, konsensusu sankcyjnego oraz legitymizacji stanowiska Ukrainy w globalnym dyskursie bezpieczeństwa.

Zmianę tę należy wiązać z przeobrażeniami środowiska międzynarodowego. Pod wpływem procesów globalizacji, przyspieszonej cyfryzacji oraz mediatyzacji polityki ukształtowała się wielopoziomowa, transnarodowa i wysoce konkurencyjna przestrzeń interakcji dyplomatycznych, w której równolegle funkcjonują podmioty państwowe, organizacje międzynarodowe, struktury subnarodowe, sieci akademickie i eksperckie, wspólnoty diasporyczne, inicjatywy obywatelskie oraz prywatne platformy cyfrowe, uzyskujące de facto status nowych pośredników wpływu. Stwierdza się, że tak rozumiana wieloaktorowość i platformowość zwiększają fragmentaryczność oraz podatność pola komunikacyjnego na operacje dezinformacyjne, jednocześnie jednak poszerza możliwości selektywnej projekcji narracji narodowej i kapitału symbolicznego w przypadku państwa dysponującego odpowiednią zdolnością komunikacyjną.

W tym kontekście przypadek ukraiński może być traktowany jako materiał empiryczny szczególnie przydatny do weryfikacji i dalszego rozwijania klasycznych koncepcji *dplomacji publicznej* i *soft power* - od wczesnych prac E. Gulliona, który konceptualizował public diplomacy jako skierowaną na zewnątrz komunikację państwa, która nie sprowadza się do negocjacji międzyrządowych, po model normatywny J. Naya, który udowodnił, że międzynarodowy wpływ może opierać się nie tylko na przymusie lub materialnej nagrodzie, ale także na atrakcyjności kultury, praktyk politycznych i zgodności wartości, w tych podejściach można dostrzec wspólną intencję: państwo, które jest w stanie wywołać i utrzymać pozytywny wizerunek siebie w oczach innych, rozszerza swoje zasoby polityki zagranicznej. Ukraina była zmuszona zastosować te teoretyczne założenia w najbardziej niekorzystnych warunkach - w sytuacji egzystencjalnego zagrożenia bezpieczeństwa, kiedy konieczne było jednocześnie (a) zapewnienie ciągłego i jednoznacznego międzynarodowego nagłaśniania przyczyn i prawnego charakteru rosyjskiej agresji, (b) utrzymanie woli politycznej partnerów do sankcji, wsparcia wojskowo-technicznego i finansowego, (c) współpracować z zagranicznymi społeczeństwami, od nastrojów których bezpośrednio zależą decyzje ich rządów. Właśnie dlatego dyplomacja publiczna w przypadku Ukrainy przestała być peryferyjnym dodatkiem do tradycyjnej dyplomacji i została zintegrowana z rdzeniem polityki zagranicznej, a jej głównym środowiskiem realizacji stało się cyfrowe, sieciowe, wysoce dynamiczne pole komunikacyjne.

W obowiązujących modelach oceny „miękkiej siły” wskazuje się, że na pozycję państwa składają się m.in. rozpoznawalność marki narodowej, reputacja międzynarodowa, rzeczywisty wpływ na postawy innych społeczeństw oraz zestaw filarów atrakcyjności (kultura, edukacja i nauka, polityka zagraniczna, media i komunikacja, potencjał gospodarczo-innowacyjny, jakość rządzenia, profil wartościowo-humanitarny). W przypadku Ukrainy od 24 lutego 2022 r. zaobserwowano synchroniczne uruchomienie wymienionych komponentów: odnotowano gwałtowny wzrost widoczności międzynarodowej państwa, wizerunek został nasycony wymiarem moralnym (państwo-ofiara niesprowokowanej agresji, ale zarazem podmiot zdolny do

oporu), a działania kulturalne, edukacyjne i obywatelskie zostały włączone w szerszą ramę dyplomacji publicznej. W ten sposób aktywności, które w warunkach pokojowych klasyfikowano by jako politykę kulturalną, w realiach wojny zaczęły pełnić funkcje stricte zewnątrzpolityczne.

Zastosowanie znalazła również kategoria rezyliencji, rozumianej w badaniach nad bezpieczeństwem nie tylko jako zdolność do odtworzenia stanu równowagi po szoku, lecz przede wszystkim jako możliwość długotrwałego funkcjonowania w warunkach presji przy zachowaniu kluczowych parametrów sprawności systemu. Przeniesienie tej kategorii na grunt dyplomacji publicznej pozwoliło na sformułowanie wniosku, iż działania komunikacyjne państwa powinny być projektowane w taki sposób, aby nie ulegały dezintegracji pod wpływem operacji informacyjno-psychologicznych, lecz adaptacyjnie na nie odpowiadały, zachowując rdzeń przekazu normatywnego i politycznego. W praktyce wykazano, że możliwe jest utrzymywanie uwagi głównych mediów i elit politycznych państw Zachodu również po wygaśnięciu pierwszej „fali zainteresowania” konfliktem, jak też możliwe jest reaktywowanie poparcia w okresach zmęczenia odbiorców oraz objaśnianie kolejnych faz działań wojennych w ramach już ugruntowanych schematów komunikacyjnych.

Za istotny nośnik projekcji „miękkiej siły” uznano praktyki kulturowo-komunikacyjne: koncerty charytatywne, pokazy kina ukraińskiego, prezentacje literatury, projekty wystawiennicze oraz otwarte wykłady o wojnie i odbudowie. Wykazano, że działania te tworzą emocjonalny kanał solidarności z państwem-ofiarą, co ułatwia rządów państw partnerskich uzasadnianie utrzymywania sankcji, pomocy wojskowej i udziału w programach rekonstrukcyjnych. Zauważono ponadto, że aktywizacja diaspory i środowisk uchodźczych w państwach przyjmujących umożliwiła poziome, oddolne replikowanie narracji ukraińskiej, co w istotny sposób zawęziło przestrzeń dla alternatywnych, prorosyjskich ujęć konfliktu.

Za integralny składnik dyplomacji publicznej uznano także działania w sferze bezpieczeństwa cybernetycznego i informacyjnego. W warunkach skoordynowanych cyberataków, kampanii dezinforma-

cyjnych i masowego użycia zautomatyzowanych sieci dystrybucji treści ochrona przestrzeni informacyjnej przestała być traktowana wyłącznie jako zadanie techniczne i została włączona do katalogu praktyk komunikacyjnych państwa na zewnątrz. Wskazano, że identyfikacja i atrybucja operacji informacyjnych, weryfikacja danych, współpraca z globalnymi platformami cyfrowymi oraz publiczne komunikowanie tych działań wzmacniają odporność krajowego pola informacyjnego i jednocześnie podnoszą poziom zaufania międzynarodowego do Ukrainy jako podmiotu zdolnego do profesjonalnej reakcji na zagrożenia hybrydowe.

Podsumowując, że ukraińska dyplomacja publiczna w warunkach pełnoskalowej agresji państwa rosyjskiego realizuje równolegle kilka sprzężonych zadań: zapewnia ciągłą obecność wojny i jej przyczyn w agendzie międzynarodowej; podtrzymuje obraz Ukrainy jako państwa nowoczesnego, europejskiego i aksjologicznie kompatybilnego ze światem demokratycznym; mobilizuje zagraniczne audytoria do wsparcia o charakterze praktycznym; ogranicza skuteczność operacji dezinformacyjnych. Przewiduje się, że w okresie powojennym aktywność ta zostanie przeprofilowana na przyciąganie zasobów odbudowy, inwestycji, technologii i kapitału ludzkiego, przy czym jej rdzeń- rozumiany jako projekcja ukraińskiej „miękkiej siły”- pozostanie zachowany. Tym samym wskazuje się, że w epoce informacyjnej dyplomacja publiczna nie powinna być ujmowana jako peryferyjny dodatek do dyplomacji tradycyjnej, lecz jako jej pełnoprawny, sieciowy i wielopodmiotowy wymiar, w którym obok państwa aktywnie uczestniczą także miasta, uczelnie, instytucje kultury i zorganizowane społeczeństwo obywatelskie.

Bibliografia:

1. Joseph, N. (2004). *Soft Power—the means to success in world politics*, Public Affairs. New York.
2. Melissen, J. (2005). *The new public diplomacy*. Palgrave.
3. Public diplomacy strategy of the Ministry of Foreign Affairs of Ukraine for 2021–2025, [w:] <https://mfa.gov.ua/storage/app/sites/1/Crпaтepiї/public-diplomacy-strategy.pdf>

4. Кравчук, Н., Луцишин, О., Андрощук, Д. (2025). Публічна дипломатія як стратегічний імператив зміцнення конкурентоспроможності держави в умовах трансформації світового порядку.
5. Миронова, М., Полякова, Ю., Шайда, О. (2024). *Публічна дипломатія у системі міжнародних економічних відносин*. Herald of Lviv University of Trade and Economics Economic sciences.
6. Трофименко М. (2023). *Трансформація публічної дипломатії в умовах глобалізації та діджиталізації: Методологічні засади й практичні аспекти (український кейс)*, Вісник Маріупольського Державного Університету.
7. Хоменська, І., Іващук О. (2023). *Базові концепти публічної дипломатії*. Інноваційна економіка, 4.

*Діана Василюшин
студентка
Львівський національний університет
імені Івана Франка*

МІЖНАРОДНА СПІВПРАЦЯ ТА БАГАТОСТОРОННІ ІНІЦІАТИВИ У СФЕРІ КІБЕРПРОСТОРУ

Міжнародна співпраця у сфері кібербезпеки сьогодні є дуже важливою х огляду на те, що технології розвиваються дуже стрімко. Цифровий світ приносить не лише нові можливості, а й серйозні ризики: кібератаки, шпигунство, гібридні загрози, які можуть завдати шкоди економіці чи навіть зупинити ключові системи країни. Тому держави, організації та компанії повинні працювати спільно, щоб протистояти цим небезпекам і зробити кіберпростір більш захищеним.

Міжнародні організації відіграють особливу роль. Скажімо, ООН¹ уже давно намагається встановити правила для цифрового

¹ ООН.URL: <https://www.unhcr.org/ua/united-nations-ukraine>

середовища. Ще у 2004 році вони зібрали експертів, які визначили, що країни не повинні, наприклад, атакувати важливі об'єкти одна одної чи порушувати їхні цифрові кордони — ці ідеї з'явилися у звітах за 2013, 2015 і 2021 роки¹. А щоб більше держав долучалися до розмови, є ще спеціальні групи, яка працює відкрито й залучає всіх охочих. Це Група урядових експертів ООН (UN GGE)² та Відкрита робоча група ООН (OEWG)³. До того ж ООН намагається допомогти країнам із меншими ресурсами краще захищатися, пов'язуючи це зі своїми планами розвитку.

В той час як НАТО розглядає кіберпростір як ще одну зону бойових дій — таку ж, як земля чи небо. Це було вирішено це у 2016 році, відколи Альянс визнав кіберпростір п'ятою операційною сферою,⁴ й відтоді активно вдосконалюються: захищають свої системи, підтримують партнерів і враховують кіберзагрози у військових планах. Був створений центр у Таллінні,⁵ який не лише проводить масштабні тренування типу Locked Shields⁶, а й стає платформою для створення законодавчих аспектів та документів для успішного перебування у кіберпросторі.

Європейський Союз має на меті забезпечити кіберпростір як безпечне середовище. У 2016 році було запроваджено Директиви про мережеву та інформаційну безпеку,⁷ які змушують дбати про захист даних критичної інфраструктури. Була створена спеціальна команда — ENISA⁸, яка все це контролює й перевіряє та при потребі

¹ Звіти. URL:<https://peacekeeping.un.org/en/reports>

² Група урядових експертів. URL: <https://disarmament.unoda.org/group-of-governmental-experts/>

³ Робоча група відкритого складу. URL:<https://disarmament.unoda.org/open-ended-working-group/>

⁴ Багатодоменні операції. URL:<https://www.act.nato.int/activities/multi-domain-operations/>

⁵ Кооперативний центр передового кіберзахисту НАТО. URL:<https://ccdcoe.org>

⁶ Замкнені щити. URL: <https://ccdcoe.org/locked-shields/>

⁷ Директива Європейського парламенту і Ради. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

⁸ ENISA. URL: <https://www.enisa.europa.eu>

покращує захист даних. А з 2020 року в ЄС з'явився план, як боротися з фейковими новинами, забезпечити нові мережі 5G і вкладати гроші у круті розробки через проєкт Horizon Europe.¹

ОБСЄ більше зосереджується на тому, як зробити так, щоб країни довіряли одна одній у цифрових питаннях. У контексті кіберпростору ОБСЄ розробляє заходи зміцнення довіри², які спрямовані на зниження ризиків конфліктів, спричинених кібератаками, та підвищення прозорості між країнами. У 2013 і 2016 роках вони домовилися ділитися новинами про загрози й мати спеціалістів, до кого можна звернутися в разі потреби чи небезпеки.³ Це дієво, коли країни не підтримують дружні відносини, але, водночас, хочуть уникнути проблем у кіберпросторі.

Крім того, країни часто домовляються напряму — вдвох чи групами. Наприклад, США й Британія обмінюються секретною інформацією через свою угоду Five Eyes⁴, а з Ізраїлем у 2018⁵ році запустили спільну боротьбу з атаками на банки. Такі договори зазвичай включають створення команд для швидкого реагування й діляться технологіями.

Коли ж потрібно об'єднати більше країн, створюються масштабніші угоди. Європейська конвенція 2001 року⁶ допомагає боротися з кіберзлочинцями й координувати суди — її підписали вже десятки держав по всьому світу. У 2018 році з'явився Паризький

¹ Горизонт Європа. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

² Заходи щодо побудови довіри і безпеки. URL: <https://www.osce.org/secretariat/107484>

³ Резолюція закликає приєднатись до Конвенції про кіберзлочинність. URL: <https://www.osce.org/pa/111213>

⁴ Форбс. URL: <https://www.forbes.com/advisor/business/what-is-five-eyes/>

⁵ Офіційний веб-сайт уряду Сполучених Штатів. URL: <https://www.state.gov/u-s-security-cooperation-with-israel/>

⁶ Європейська конвенція про захист аудіовізуальної спадщини (Страсбург, 2001). URL:

<https://www.coe.int/en/web/culture-and-heritage/audiovisual-heritage>

заклик¹, де країни й компанії сказали, що разом захищатимуть кіберпростір. Паризький заклик до дій у кібербезпеці був оголошений у 2018 році в рамках Першої міжнародної конференції з кібербезпеки, організованої в Парижі. Цей документ став важливим кроком на шляху формування глобальних стандартів кібербезпеки та співпраці держав і приватного сектору для захисту кіберпростору від загроз. Основною метою Паризького заклику було створення глобальної платформи для співпраці в сфері кібербезпеки. Заклик передбачав розвиток міжнародного консенсусу, який би дозволив країнам і компаніям спільно працювати над захистом цифрових інфраструктур і забезпеченням стабільності кіберпростору.

Щоб усе це діяло, потрібні способи швидко ділитися інформацією й працювати разом. У кожній країні є свої команди — CERT², які стежать за кібербезпекою. Через міжнародну мережу FIRST³ вони обмінюються новинами про атаки — так було, наприклад, коли у 2017 році вірус WannaCry ⁴налякав усіх, і це справді допомогло. Є ще платформи, які показують, хто як готовий до загроз, чи системи НАТО, які перевіряють, чи можуть їхні технології працювати разом. Однією з важливих ініціатив є використання NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE),⁵ що створене для зміцнення кіберзахисту в Альянсі та його партнерських країнах. Центр займається розробкою стандартів для оцінки рівня кіберзахисту, а також пропонує тренування та симуляції для перевірки здатності різних держав до спільного реагування на кіберзагрози.

¹ Паризький заклик. URL: Paris Call

² Комп'ютерна аварійна служба України. URL: <https://cert.gov.ua>

³ Форум груп реагування на інциденти та безпеки. URL: <https://www.first.org>

⁴ Вірус WannaCry пошкодив комп'ютери у 99 країнах світу. URL: <https://www.bbc.com/ukrainian/features-39907984>

⁵ Кооперативний центр передового досвіду кіберзахисту НАТО. URL: <https://ccdcOE.org>

Ще однією важливою платформою є NATO Communications and Information Agency (NCIA)¹, яка розробляє новітні технології для забезпечення кібербезпеки в межах Альянсу. Ця платформа дозволяє країнам-членам НАТО перевіряти, чи можуть їхні кіберсистеми працювати в єдиному просторі під час спільних операцій. Це важливо для забезпечення швидкої реакції на можливі загрози, адже під час кіберконфліктів необхідно, щоб різні національні системи безпеки та технології могли ефективно взаємодіяти між собою.

Отже, співпраця у кібербезпеці — це ціла система, де є великі гравці, як ООН чи НАТО, прямі договори між країнами й практичні інструменти, як команди CERT чи тренування. Але не все ідеально: країни сперечаються, у когось бракує техніки, а довіри часто немає. Щоб стало краще, треба чіткіші правила, більше залучати бізнес і підтримувати слабші держави — тоді кіберпростір справді стане безпечнішим.

*Роман Вовк
кандидат фіз.-мат. наук, доцент,
Маркіян Мальський
доктор екон. наук, професор
Львівський національний університет
імені Івана Франка*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ У ЗОВНІШНІЙ ПОЛІТИЦІ

Сучасні міжнародні відносини переживають глибоку трансформацію, спричинену стрімким розвитком цифрових технологій. Інформація стала стратегічним ресурсом, а кіберпростір перетворився у масштабне поле протистояння між країнами. За таких обставин дезінформація, як навмисне поширення неправдивої або маніпулятивної інформації з метою введення в оману та досягнення

¹ Агенція зв'язку та інформації НАТО. URL: <https://www.ncia.nato.int>

політичних цілей, все частіше застосовується для реалізації руйнівних гібридних загроз для демократії та глобальної стабільності.

Дезінформаційні кампанії здатні підірвати довіру до державних інститутів, посилити соціальну поляризацію та безпосередньо вплинути на зовнішньополітичні рішення, виборчі процеси та міжнародні конфлікти. Для ефективного реагування на ці виклики цифрова дипломатія повинна активніше використовувати технології штучного інтелекту (ШІ) та застосовувати аналіз великих даних. У цьому напрямку ШІ здатний запропонувати широкий спектр інструментів для швидкого, масштабного та точного виявлення дезінформаційних потоків та своєчасного реагування на них.

Цифрова дипломатія в сучасних умовах є комплексом дипломатичних практик, що використовують інтернет, соціальні медіа, аналіз даних та інші цифрові інструменти для реалізації зовнішньополітичної діяльності, просування національних інтересів та взаємодії з громадськістю.

У дипломатичній діяльності ШІ може використовуватися в комп'ютерних системах, здатних виконувати завдання, що зазвичай вимагають людського інтелекту (наприклад, розпізнавання мовних патернів чи класифікація даних), для підтримки зовнішньополітичного аналізу та комунікацій.

Дезінформація як інструмент зовнішньої політики використовувалася впродовж багатьох століть, однак цифрова ера, насамперед з появою глобальних соціальних мереж (Twitter/X, Facebook, Instagram, Telegram, TikTok та ін.), створила зручне середовище для її гіпершвидкого, масованого та мікротаргетованого поширення. У наш час дезінформація більше не обмежується простором досяжності традиційних медіа, а поширюється в режимі реального часу на всю планету і доноситься мільярдам користувачів.

Водночас дезінформація все частіше спрямована не лише на зміну переконань чи спотворення дійсності, але й на формування емоційної реакції людей, таких як тривога, страх чи гнів, що сприяє швидшому поширенню контенту через алгоритми соціальних мереж.

Основні труднощі у виявленні та протидії дезінформації зумовлені широким застосуванням анонімних серверів, ботів і фейкових акаунтів, що робить складним достовірне визначення джерела атаки, конкретного державного чи недержавного актора.

Часто головним середовищем протистояння цифрової дипломатії та дезінформації стають соціальні мережі. Алгоритми платформ, розроблені для максимізації залученості, часто ненавмисно сприяють поширенню емоційного та поляризуючого контенту – саме того типу, який характерний для фейкових новин. Це спричиняє створення так званої “ехокамери” – середовища, де люди бачать лише ту інформацію, що підтверджує їхні існуючі погляди. А це, в свою чергу, ускладнює діалог та просування об’єктивних фактів.

Зовнішньополітичні відомства можуть використовувати аналогічні платформи для просування своїх наративів, проте їм доводиться конкурувати не лише з іноземними державними структурами, а й з “фабриками тролів”, які генерують величезні обсяги ворожого контенту.

Новітні інформаційні технології та інструменти ШІ дають змогу перейти від простого використання соціальних мереж для публічної дипломатії до багатогранного аналізу інформаційних потоків, виявлення загроз та вивчення настроїв суспільства. Дипломатичні інституції можуть використовувати ШІ як ключовий елемент для створення стратегічної стійкості, що передбачає не лише реактивне спростування, а й проактивну ідентифікацію викликів, аналіз схем фінансування та логіки поширення дезінформації для її превентивного блокування.

Методологія ШІ для виявлення дезінформації набуває популярності насамперед через необхідність опрацьовувати гігантські обсяги даних у режимі, недосяжному традиційними інструментами. Найпопулярнішими інструментами ШІ у цій сфері є технологія обробки природної мови (NLP) та алгоритми “машинного навчання” (Machine Learning) і “глибокого навчання” (Deep Learning).

Основне призначення NLP дати машинам можливість “розуміти” людську мову, що є необхідною умовою для виявлення дезінформації, яка часто має лінгвістичний характер. При цьому використовують такі підходи, як аналіз тональності, коли алгоритми ШІ класифікують емоційне забарвлення тексту (позитивне, негативне, нейтральне). Відслідковуються також різкі, несподівані або скоординовані зміни тональності щодо певної теми, країни чи державного діяча, що можуть свідчити про початок дезінформаційної кампанії. Ефективне використання цієї методології дасть змогу здійснювати моніторинг іноземної публічної думки і прогнозувати можливі загострення чи непорозуміння у міждержавних відносинах.

Ще один напрям обробки природної мови використовує стилістичний аналіз та ідентифікацію аномалій. Тут NLP може виявляти нетипові лінгвістичні патерни, характерні для ботів або “фабрик тролів”, такі як використання специфічних, повторюваних фраз, граматичних помилок, які невластиві носіям мови, або скоординовану публікацію однакового контенту.

Підґрунтя для створення систем автоматизованого фактчекінгу та ідентифікації акторів дають алгоритми машинного навчання та глибокого навчання. Серед інших варто відзначити класифікацію текстових повідомлень. При цьому побудовані моделі ML навчаються на дуже великих датасетах, що містять як правдиві, так і заздалегідь позначені фейкові новини. Вони вивчають ознаки брехні, такі як невідповідність заголовка тексту, використання сенсаційних слів, відсутність достовірних джерел тощо. Глибоке навчання (наприклад, нейронні мережі) здатне виявляти складні, приховані зв'язки, що робить його ефективним проти витончених форм дезінформації.

Важливе значення у протидії дезінформації має ідентифікація бот-мереж. У цьому випадку системи ML аналізують поведінкові метрики користувачів, а не лише сам контент. Йдеться насамперед про аномально високу швидкість публікацій, ідентичні часові проміжки активності, відсутність оригінального контенту (лише репости), підозрілі патерни взаємодії з іншими акаунтами.

Дезінформація часто включає не лише текст, а й маніпульовані зображення чи відео (Deepfakes). ШІ здатний використовувати “комп’ютерний зір” для виявлення ознак маніпуляцій у візуальному контенті, порівнюючи метадані та виявляючи невідповідності у зображенні.

На даний час існує чимало добре відомих міжнародних та регіональних організацій, які активно використовують цифрові інструменти для моніторингу та аналізу дезінформації, в тому числі промосковської. Не завжди можна з впевненістю стверджувати, що ці організації у своїй діяльності використовують технології ШІ, однак без сумніву їхні бази даних та аналітичні дослідження слугують основою для побудови ШІ-моделей. Серед інших слід відзначити Європейську обсерваторію цифрових медіа¹ (EDMO), що об’єднує фахівців з перевірки фактів, експертів з медіаграмотності та академічних дослідників і взаємодіє з мережею із 15 національних або багатонаціональних центрів. Значний внесок у протидію дезінформації здійснює незалежна некомерційна організація EU Disinfo Lab², яка поєднує розслідувальну діяльність із дослідженням поширення дезінформації в Європі та її впливу на політичні процеси і настрої громадянського суспільства в різних країнах. На дослідженні соціальних мереж та виявленні дезінформаційних кампаній, що там активно поширюються, сконцентрована діяльність відомої американської компанії Graphika³. Проблеми забезпечення інформаційної безпеки і стабільності в Євроатлантичному просторі є в полі зору Центру передового досвіду стратегічних комунікацій НАТО⁴ (NATO StratCom COE). Серед українських організацій варто відзначити проект StopFake⁵ громадської організації “Центр Медіареформи”, діяльність якої

¹ European Digital Media Observatory URL: <https://edmo.eu>

² EU Disinfo Lab. URL: <https://www.disinfo.eu>

³ Graphika URL: <https://www.graphika.com>

⁴ NATO Strategic Communications Centre of Excellence URL: <https://stratcomcoe.org>

⁵ StopFake URL: <https://www.stopfake.org>

спрямована на перевірку інформації та підвищення медіаграмотності громадськості. Великий обсяг роботи з протидії поширення російської пропаганди та дезінформації здійснює відома громадська організація “Детектор медіа”¹. При Раді національної безпеки та оборони України діє Центр протидії дезінформації², який забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері.

Одним із перспективних напрямів використання ШІ у зовнішньополітичній діяльності можна назвати створення систем раннього попередження інформаційних загроз, які найчастіше проявляються перед важливими міжнародними подіями, переговорами чи напередодні, та проведення аналізу соціальної напруги і підозрілих інфопотоків у регіонах, які можуть стати “гарячими точками” дезінформації. Алгоритми ШІ можна успішно використовувати для моделювання, як той чи інший фейк буде поширюватися і на які аудиторії він вплине найбільше, дозволяючи дипломатам завчасно підготувати “вакцину правди” – набір фактів та повідомлень, які знівелюють або пом’якшують ефект від дезінформаційних операцій.

Загальновідомо, що фейкові новини поширюються значно швидше, ніж їх спростування, тому для протидії їм доцільно застосовувати алгоритми автоматизації фактчекінгу, автоматизований пошук першоджерел з використанням ШІ. Так можна за лічені секунди порівняти зміст підозрілого повідомлення з масивами достовірних, верифікованих даних, щоб визначити його правдивість.

Важливими є також механізми створення контрнарративів та їх таргетування. Замість публікації загального спростування, яке може не дійти до цільової аудиторії, аналіз даних дає змогу точно ідентифікувати демографічні та психографічні групи, які найбільше піддалися впливу конкретного фейку.

¹ Детектор медіа URL: <https://detector.media>

² Центр протидії дезінформації URL: <https://cpd.gov.ua>

Попри високий потенціал, використання ШІ у сфері міжнародних відносин несе серйозні етичні, правові та технологічні виклики. Насамперед слід взяти до уваги упередженість алгоритмів, адже моделі ШІ навчаються на існуючих даних, які інколи відображають певні політичні, культурні чи мовні упередження. За таких обставин ШІ може помилково класифікувати законний контент як “дезінформацію” або, навпаки, не помітити ворожу дезінформацію, спрямовану проти певних груп. Це ставить під сумнів ефективність застосовуваних контрзаходів.

Водночас надмірна автоматизація виявлення та блокування контенту може призвести до неправомірного обмеження свободи слова, тому державні структури, які покликані захищати демократичні цінності, повинні забезпечити прозорість та можливість оскарження рішень, прийнятих з використанням алгоритмів ШІ. Також слід взяти до уваги, що моніторинг соціальних мереж як на національному, так і міжнародному рівні для виявлення дезінформації неминуче передбачає збір та аналіз великих масивів персональних даних, що потребує чітких міжнародних стандартів та законодавчих рамок.

Загалом можна підсумувати, що цифрова дипломатія сьогодні зіткнулася з екзистенційними викликами у вигляді масованої дезінформації, і штучний інтелект повинен виконувати функції не просто допоміжного інструменту, а стати критично важливою технологічною перевагою в інформаційній війні.

Орест Гогоша
0000-0002-6664-4736

Юрій Марченко
студент

Львівський національний університет
імені Івана Франка

КІБЕРПРОСТІР ЯК ПОЛЕ ГЕОПОЛІТИЧНОГО ПРОТИСТОЯННЯ США, КНР ТА РФ

Традиційно геополітика зосереджувала свою увагу насамперед на просторі та всьому, що з ним пов'язане. З'явилася навіть класифікація держав за типом їхньої просторової домінанти –

телурократія (сухопутна держава) та таласократія (морська держава). З розвитком людства геополітична наука (або правильніше називати як підхід до міжнародних відносин, політичних процесів) продовжувала еволюціонувати, що зумовило появу нових класифікацій і критеріїв оцінки державного потенціалу та управління. Зокрема, почали враховувати такі поняття, як аерократія, ефірократія, а також в XXI ст. кіберпростір і кібербезпеку.

У XXI ст. держави опинилися в умовах, коли раціональне використання ресурсів стало критично необхідним. Попри глобалізацію та відкритість світу, шлях до зміцнення впливу чи встановлення гегемонії значно ускладнився. Провідні держави активно застосовують усі доступні інструменти для збереження або розширення своїх позицій на міжнародній арені.

Кібербезпека сьогодні є одним із ключових інструментів забезпечення національних інтересів у кіберпросторі. Водночас поки що неможливо говорити про існування єдиного, цілісного та стабільного світового кіберпростору. Різні держави, залежно від рівня розвитку, прагнуть створити власний або, навпаки, відкритий і глобальний кіберпростір, тоді як інші намагаються впливати чи навіть підірвати ці системи відповідно до власних стратегічних інтересів.

У XXI ст. Сполучені Штати Америки та Китайська Народна Республіка постали головними суперниками, які прагнуть формувати власні «правила гри» на міжнародній арені та забезпечити, щоб інші держави їх дотримувалися. США представляють Західний світ із моделлю «представницької демократії», наголошуючи на поділі держав на «демократичні» та «недемократичні» режими. Натомість Китай просуває концепцію «Китайської меритократії», яка базується на відмінних принципах державного управління порівняно з представницькою демократією. Таким чином, обидві держави фактично формують власні «табори» впливу: Західний табір, орієнтований на представницьку демократію, та Китайський табір, що спирається на ідею китайського меритократичного управління. Щоб розширювати

коло союзників, кожна зі сторін використовує широкий спектр інструментів: фінансових, військових, культурних, політичних та ідеологічних. У цьому контексті кіберпростір і кібербезпека стають одними з ключових засобів просування національних інтересів і цінностей на глобальній арені.

Стратегії держав, які активно використовують кіберпростір для реалізації власних цілей, істотно різняться. США дотримуються так званої «*Multistakeholder model*», що передбачає демократичне управління інтернетом, свободу обміну інформацією, відкритість і децентралізацію. Ця модель ґрунтується на принципі багатосторонньої участі різних суб'єктів урядів, бізнесу, громадських організацій і технічних спільнот та активно просувається США на глобальному рівні. Натомість КНР реалізує концепцію «*Cyber sovereignty*», яка, навпаки, передбачає захист державного контролю над інформаційним простором і протидію зовнішньому втручання у внутрішню політику, зокрема у сфері цензури та регулювання. При цьому Китай пропонує запровадити подібний підхід і на регіональному рівні, фактично поділяючи світ на окремі «кіберпростори», що перебувають під контролем конкретних держав або об'єднань [1].

Російська Федерація, у свою чергу, також сповідує принцип «*Cyber sovereignty*» у внутрішній політиці, але водночас активно застосовує кіберпростір у межах гібридних стратегій для дестабілізації противників через кібератаки, дезінформацію, втручання у виборчі процеси та інші форми інформаційного впливу [2].

Варто зазначити, що США та КНР є двома потужними економіками світу та глобальними лідерами у сфері кібербезпеки. РФ поки що не досягла рівня кіберможливостей США чи Китаю. Незважаючи на значний прогрес КНР у розвитку цифрових технологій та кіберпотенціалу, розрив із США залишається великим через високий рівень розвитку цифрової економіки в США. У червні 2021 р. британський аналітичний центр Міжнародного інституту стратегічних досліджень оцінив кіберздатності 15 найбільших світових гравців у сфері хакерства та цифрового захисту.

Центр визначив США як найбільш кіберспроможну державу, а КНР та РФ – як другий рівень кіберпотенціалу. США довгий час залишатимуться лідером у кіберпросторі завдяки високо розвиненому військовому потенціалу, системному державному підходу до кібербезпеки та управління ризиками, великій кількості висококваліфікованого персоналу технологічних компаній, а також розвиненій інфраструктурі для забезпечення як наступальних, так і оборонних кібероперацій. Попри домінування США, Китай продовжує активно розвивати цифровий сектор і прагне наблизитися до рівня кіберпотенціалу США [3].

Для активної конкуренції своїх світоглядів держави прагнуть встановлювати правила та стандарти. У сфері кібербезпеки ті, чий стандарти дотримуються більшою кількістю учасників, отримують стратегічну перевагу над противниками. Так, у 2021 р. США разом із G7 ухвалили «Декларацію міністрів з питань цифрових технологій», яка просуває «*Multistakeholder model*». Усвідомлюючи ці дії Західного блоку, Китай також пропонує власні ініціативи, зокрема концепцію «*new IP*», що передбачає обов'язкову реєстрацію користувачів і полегшує державний нагляд за онлайн-діяльністю.

Крім того, ініціатива Сі Цзіньпіна 2014 р. «*Cyber power*» демонструє перехід КНР від споживача міжнародних стандартів до держави, яка сама встановлює і формує стандарти у цифровій сфері. Прикладом цього є ситуація, коли Китай бойкотував Систему доменних імен (ICANN), керовану США, та наполягав на проведенні міжнародної реформи управління інтернет-ресурсами. Крім того, КНР створив Китайський центр інформаційної мережі (CNNIC), який контролює китайські доменні імена, включаючи «.cn».

Загальна конкуренція у таких сферах, як впровадження 5G, розвиток штучного інтелекту та створення «розумних міст», також впливає на військово-економічну динаміку між США та КНР [1].

Конкуренція у кіберпросторі між США, Китаєм і Росією охоплює технологічні, військові, економічні та геополітичні аспекти. США залишаються беззаперечним лідером завдяки розвитку цифрової економіки, інфраструктури та системному підходу до кібербезпеки, тоді як Китай активно скорочує відставання та

формує власні стандарти. Росія, сповідує принцип «*Cyber sovereignty*», поступається обом державам і використовує кіберінструменти переважно в гібридних стратегіях.

Стратегічне суперництво проявляється не лише у технологіях, а й у встановленні правил і стандартів кіберпростору. США просувають багатосторонню модель управління інтернетом, а саме «*Multistakeholder model*», тоді як Китай впроваджує концепцію «*Cyber sovereignty*» та активно формує власні внутрішні стандарти, наприклад через ініціативи «*new IP*» та «*Cyber power*». Конкуренція у сферах 5G, штучного інтелекту та «розумних міст» підсилює взаємний вплив і визначає розподіл глобального цифрового впливу.

Отже, кіберпростір стає ключовим полем геополітичного протистояння, де технологічна перевага та контроль над інформаційними потоками впливають на міжнародну безпеку. Для зменшення напруженості необхідно впроваджувати спільні стандарти, залучати міжнародну спільноту та розробляти правила поведінки держав у кіберпросторі.

Список використаних джерел:

1. Navigating the nexus: geopolitical, international relations and technical dimensions of US-China cyber strategic competition. URL: <https://doi.org/10.1080/23311886.2025.2499171>;
2. Федонюк С. Магдисюк Г. Протистояння між США й Китаєм у сфері кібербезпеки. URL: <https://doi.org/10.31861/mhpi2022.45.113-127>;
3. Cyber posture trends in China, Russia, the United States and the European Union. URL: https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf.

*Віталій Гутник
доктор юридичних наук, професор
Львівський національний університет
імені Івана Франка*

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ МІЖНАРОДНИМ КРИМІНАЛЬНИМ СУДОМ: ШЛЯХ ЧИ ПЕРЕШКОДА ДЛЯ МІЖНАРОДНОГО ПРАВОСУДДЯ?

В останні роки застосування цифрових технологій та штучного інтелекту досягло досі небаченого масштабу в усіх сферах суспільних відносин. Тенденція подальшого розвитку цифрових технологій та штучного інтелекту очевидно буде продовжуватися й надалі.

Яким же чином Міжнародний кримінальний суд (далі – МКС), який є єдиним постійно діючим органом міжнародного кримінального правосуддя, використовує диджиталізацію та чи використовує штучний інтелект у процесі своєї діяльності?

На перший погляд, Римський статут МКС, який був прийнятий 1998 року, містить усталені норми кримінального правосуддя, які формувалися протягом століть й не згадує можливості використання цифрових засобів для збирання доказів та їх використання, не кажучи вже про можливість використання штучного інтелекту.

Однак, цифровізація суспільства, характер та масштаби міжнародних злочинів щодо яких МКС володіє предметною юрисдикцією, стали локомотивом зміщення акценту на невідомі ще декілька десятиліть форми збору доказів, зокрема тих, які містяться в кіберпросторі. Викликом виявилось те, що вивчення співробітниками Офісу Прокурора МКС усієї інформації, доступної в Інтернеті у відкритих джерелах та яка стосується конкретних збройних конфліктів (і ймовірно вчинених злочинів) займе роки, якщо не десятиліття. Унікальне середовище збору доказів вимагало нового підходу, і технології стали ключем до цього підходу. У наш час, розслідування міжнародних злочинів уже не може проводитися виключно на основі аналогових засобів (коли людина «вручну» перевіряє кожен ймовірний доказ) у світі, який так швидко став

цифровим. МКС бере активну участь у цифровій революції у своїх розслідуваннях міжнародних злочинів [1, с.3].

З 1 січня 2025 року Україна стала державою-учасницею МКС, однак до моменту набуття членства у МКС двічі визнавала юрисдикцію МКС в порядку, передбаченому у ст.12 (3) Статуту. Вперше, Україна прийняла юрисдикцію у 2014 року щодо вчинених злочинів протягом мирних протестів в Україні з 21 листопада 2013 до 22 лютого 2014 року; вдруге – у 2015 році – щодо злочинів, вчинених на території України з 20 лютого 2014 року. У переданих ситуаціях щодо вчинених міжнародних злочинів, виникла проблема з величезною кількістю доказів, які були подані, та відсутністю необхідного персоналу для їх опрацювання. Тому, до повномасштабного вторгнення у 2022 році навіть не було прийнято рішення про початок розслідування.

Враховуючи обмежені фінансові та людські ресурси, а також реалії цифровізації світу, МКС почав активно шукати шляхи вирішення цієї проблеми й серед іншого – використовувати для збору та опрацювання доказів інтернет платформу OTP link (*Office of the Prosecutor's link*), яка була представлена у 2023 році та через яку, будь-яка особа, включаючи тих, хто стали свідками або жертвами вчинення злочинів, мають змогу подати докази.

Ця платформа спрощує традиційний процес перевірки вручну, дозволяючи Офісу прокурора МКС обробляти більші обсяги інформації за допомогою штучного інтелекту і машинного навчання (*Machine Learning*), щоб запропонувати краще розуміння отриманої інформації, значно скорочуючи час, необхідний для її перегляду та вжиття заходів. Платформа підтримує міжнародні стандарти обробки доказів, використовуючи при цьому цифровий ланцюжок зберігання, який збирає та зберігає інформацію. Це зберігає цілісність доказів і створює надійний і захищений від підробки запис процесу збору та обробки [2].

Як підкреслив Прокурор МКС, анонсовуючи у 2023 році старт роботи цієї платформи, її запуск «знаменує собою віху в ширшій технологічній модернізації Офісу Прокурора МКС... Щоб

ефективніше відстоювати справедливість, ми повинні використовувати потужність передових технологій» [2].

Задля активного впровадження передових технологій у березні 2022 році було утворено Цільовий фонд Офісу Прокурора МКС з передових технологій та спеціалізованого потенціалу, створений у березні 2022 року, який окрім власне пришвидшення дослідження фактів та обставин вчинення міжнародних злочинів, дозволив Офісу ефективно вирішувати фундаментальні проблеми щодо посилення здатності Офісу ефективно боротися зі злочинами за гендерною ознакою та злочинами проти дітей, дотримуючись підходу, що враховує травматичний досвід [3, п.222]. Цікаво, що головним донором цього Фонду виступає Європейський Союз. У 2024 році внесок ЄС у Фонд склав 7,2 з 33,7 мільйона євро загального бюджету [4, с.39]. Додатково, кожна з держав-учасниць сплачувала окремі внески.

Оскільки процес розслідування справ займає щонайменше декілька років, результат застосування штучного інтелекту буде помітним у найближчі роки. Натомість уже сьогодні спостерігається тенденція збирання доказів з відкритих даних з мережі Інтернет, а також соціальних мереж. Досить знаковим у цьому руслі є рішення Судової палати V МКС від 24 липня 2025 року, яким Альфреда Єкатама та Патріса-Едуара Нгайссона визнано винними у вчиненні низки воєнних злочинів та злочинів проти людяності в Центральньоафриканській Республіці у період з 2012 до 2014 роками та яким засуджено А.Єкатама до 15 років, а П.-Е. Нгайссона – до 12 років позбавлення волі.

У цьому рішенні цифрові докази зайняли дуже помітне місце. Так, для прикладу, Палата визнала офіційно поданими приблизно 943 документи, пов'язані з доказами у Facebook («Матеріали Facebook»). Такі матеріали Facebook включали, серед іншого, приватні повідомлення, зокрема вкладення, надіслані між користувачами; скріншоти публікацій, видимих у профілях користувачів Facebook, фотографії та списки друзів у Facebook; а також ділові записи Facebook з інформацією та метаданими про профілі користувачів, такими як імена та адреси електронної

пошти, що використовуються для реєстрації, та журнали [5, п.144]. Обвинувачення отримало свої матеріали Facebook після серії запитів на допомогу («RFA») від Facebook Ireland Limited (Meta INC) [5, п.145].

Підводячи підсумки використання цифрових технологій МКС, слід підкреслити активну участь МКС в освоєнні нових форм збирання доказів, зокрема тих, які містяться у кіберпросторі та застосування штучного інтелекту для їх систематизації та верифікації. Фактично МКС опинився перед вибором: або застосовувати старі правила, пов'язані зі звичними фізичними доказами, або значно розширити джерела збирання доказів, шляхом використання інтернет ресурсів. Очевидно, що цифрові докази сьогодні не так складно сфабрикувати, особливо шляхом використання штучного інтелекту. Для попередження таких випадків, залучення штучного інтелекту самим МКС сприяє виключення цих фактів; штучний інтелект значно економить людські та фінансові ресурси у пошуку, систематизації та верифікації доказів чим сприяє досягненню основної функції МКС – боротьбі з безкарністю за вчинені міжнародні злочини.

Список використаних джерел

1. Kuczyńska H.. The ICC enters into the future: the digital evidence revolution or evolution?. *Revista Brasileira De Direito Processual Penal*. 2024. Vol. 10(3). P.1=40. URL: <https://doi.org/10.22197/rbdpp.v10i3.1073>
2. ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTPLink. Statement: 24 May 2023. URL: <https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink>
3. Proposed Programme Budget for 2025 of the International Criminal Court. ICC-ASP/23/10. URL: https://asp.icc-cpi.int/sites/default/files/asp_docs/ICC-ASP-23-10-ENG.pdf
4. Report of the Committee on Budget and Finance on the work of its forty-fifth session. ICC-ASP/23/25, 22 November 2024. URL.

https://asp.icc-cpi.int/sites/default/files/asp_docs/ICC-ASP-23-25-ENG.pdf

5. Situation: Situation in the Central African Republic II . Prosecutor v. Alfred Yekatom and Patrice-Edouard Ngaïssona. ICC-01/14-01/18. Judgment, 24 July 2025. URL: <https://www.icc-cpi.int/sites/default/files/CourtRecords/0902ebd180c2c849.pdf>

Ігор Доцяк
кандидат політичних наук, доцент,
Богдан Гнатів
аспірант
Карпатський національний університет
імені Василя Стефаника

Е-ДЕМОКРАТІЯ В УМОВАХ ВІЙНИ ЗА НЕЗАЛЕЖНІСТЬ УКРАЇНИ: РИЗИКИ ТА ПЕРСПЕКТИВИ

Сучасний світовий досвід свідчить, що цифровізація демократичних процесів відповідає реаліям інформаційного суспільства та є одним із ключових чинників зміцнення взаємодії між громадянами та владою. Е-демократія дає можливість поєднувати технологічний прогрес із соціально-політичною участю, формуючи нові підходи до ухвалення політичних рішень, контролю та комунікації. У науковому дискурсі е-демократію визначають як сукупність інституцій, практик і технологій, що забезпечують участь громадян у публічному управлінні через цифрові канали. Згідно концепції розвитку е - демократії в Україні, вона визначена як форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоврядування шляхом широкого застосування інформаційно-комунікаційних технологій в демократичних процесах, що дає змогу: посилити участь, ініціативність та залучення громадян на загальнодержавному, регіональному та місцевому рівні до публічного життя; поліпшити прозорість

процесу прийняття рішень, а також підзвітність демократичних інститутів; поліпшити зворотну реакцію суб'єктів владних повноважень на звернення громадян; сприяти публічним дискусіям та привертати увагу громадян до процесу прийняття рішень [1]. В той же час, е-демократія не замінює традиційні форми демократії, а лише розширює можливості для реалізації громадянських прав та свобод. Саме вона дає можливість прискорювати євроінтеграційні процеси в Україні. Єврокомісія оцінила цифрову трансформацію України у Звіті про розширення 2025. На думку Єврокомісії, Україна досягла значного прогресу в наданні послуг та цифровізації [2]. Адже це не просто про зручні сервіси, а масштабні зміни й реформи цілих галузей. Реалії військового стану сформували нові виклики для функціонування та розвитку е-демократії в Україні. Війна за Незалежність України стала не лише випробуванням для держави, а й каталізатором глибоких суспільно-політичних змін. В умовах воєнного стану е-демократія набула нового значення, стаючи інструментом не лише участі громадян у прийнятті рішень, а й способом консолідації нації. З розвитком цифрових технологій в Україні сформовано унікальну екосистему електронного врядування, яка включає сервіси «Дія», електронні петиції, онлайн-бюджети, платформи участі та консультацій. Після початку повномасштабного вторгнення роль цих інструментів значно посилилась. Кількість користувачів «Дії» з початку повномасштабного вторгнення зросла на 20%. У віці понад 60 років в «Дії» понад 4,5 млн користувачів, і ця цифра стрімко зростає [3]. Серед головних ризиків функціонування е-демократії у період війни можна виділити: кіберзагрози, інформаційні маніпуляції, обмеження громадянських прав у зв'язку з воєнним станом та нерівний доступ до інтернету на прифронтових територіях. Серед найбільш знакових кібератак варто відзначити атаку ворога 19 грудня 2024 року, коли понад 60 держреєстрів, а також близько 20 сервісів «Дія» не працювали [4]. Попри наявні виклики, розвиток е-демократії під час війни має позитивні тенденції. Українці демонструють високий рівень цифрової грамотності та готовності використовувати онлайн-інструменти для захисту власних прав. У

контексті децентралізації влади е-демократія виконує функцію інтегратора між центральною та місцевою владою. Саме на рівні громад формується нова культура участі, де електронні інструменти допомагають поєднати ініціативу громадян із можливостями державної політики. Післявоєнне відновлення України відкриє нові можливості для розбудови цифрової демократії. Очікується залучення міжнародних донорів для створення інноваційних платформ участі, розбудови кібербезпеки та модернізації IT-інфраструктури. Е-демократія в умовах війни постає як індикатор зрілості українського суспільства. Вона доводить, що навіть у надзвичайних умовах громадяни готові брати участь у прийнятті рішень і не відмовляються від демократичних цінностей. У цьому контексті особливого значення набуває розвиток цифрової довіри між державою та громадянами. Адже будь-яка система е-участі потребує високого рівня захисту персональних даних, прозорості алгоритмів прийняття рішень та підзвітності органів влади. Важливим напрямом є підвищення цифрової інклюзії, тобто забезпечення рівного доступу до цифрових інструментів для всіх категорій населення, зокрема для внутрішньо переміщених осіб, людей похилого віку та осіб з інвалідністю. Крім того, слід врахувати досвід інших держав, які перебували у стані конфлікту або відновлення. Наприклад, досвід Естонії та Литви свідчить, що навіть у періоди загроз національній безпеці можна забезпечити безперервність електронного урядування шляхом децентралізованих дата-центрів, багаторівневої автентифікації користувачів та посилення громадського контролю за цифровими процесами. Для України перспективним є створення єдиної платформи громадської участі, що об'єднає електронні петиції, консультації, бюджет участі та цифрові обговорення в межах однієї екосистеми. Це дозволить не лише спростити доступ громадян до механізмів е-участі, а й підвищити ефективність ухвалення управлінських рішень. Також доцільно розширювати освітні програми з цифрової грамотності на базі закладів освіти та центрів надання адміністративних послуг. Підсумовуючи, можна стверджувати, що розвиток е-демократії в умовах війни став не лише

засобом адаптації, а й проявом стійкості української демократії. Вона перетворилася на дієвий інструмент зміцнення довіри, взаємодії та солідарності. Подальші дослідження мають бути спрямовані на аналіз ефективності цифрових інструментів участі, вдосконалення нормативно-правової бази та вироблення стратегічного бачення цифрової демократії як складової національної безпеки та післявоєнного відновлення держави.

Список використаних джерел та літератури:

1. Концепція розвитку електронної демократії в Україні : розпорядження Кабінету Міністрів України від 8 листопада 2017 р. № 797-р. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/797-2017-p> (дата звернення: 27.10.2025)
2. Єврокомісія оцінила цифрову трансформацію України <https://thedigital.gov.ua/news/progress/nablyzayemo-ukrayinu-do-yes-yevrokomisiia-vidznachyla-uspikhy-tsyfrovizatsiyi>
3. Брифінг керівника з розвитку електронних послуг у Міністерстві цифрової трансформації Мстислава Баніка, від 25.01.2023. — URL: <https://www.ukrinform.ua/amp/rubric-technology/3659267-kilkist-koristuvaciv-u-dii-zrosla-na-20-z-pocatkuvijni-mincifri.html>
4. Аналіз кібератаки на українські державні реєстри від «Forbes», від 20.12.2024. — URL: <https://forbes.ua/innovations/za-atakoyu-stoyat-rosiyski-spetssluzhbiponad-60-derzhreestriv-ne-pratsyuyut-cherezataku-rosiyan-na-minyust-yaki-naslidki-y-chimzagrozhue-ukraintsyam-vitik-danikh-20122024-25742>

*Іванна Земан
кандидат педагогічних наук, доцент
Львівський національний університет
імені Івана Франка*

X-ДИПЛОМАТІЯ ЯК ІНСТРУМЕНТ СУЧАСНОЇ МІЖНАРОДНОЇ КОМУНІКАЦІЇ

Соціальні мережі у сучасному світі є важливим засобом комунікацій для політиків та дипломатів у міжнародних відносинах. Найпопулярнішими соціальними мережами в Україні залишаються Telegram, YouTube, Facebook, TikTok, Instagram та X (Twitter).

Соціальні мережі стали важливим каналом цифрової дипломатії та слугують для покращення взаємодії між політиками та громадськістю. Політичні лідери активно комунікують як з внутрішньою, так і з міжнародною аудиторією, через пости про актуальні події та висловлювання власних поглядів щодо певних політичних питань.

Соціальні мережі стали ефективним засобом для покращення міжнародного іміджу країни завдяки можливості постійної взаємодії та безперервній комунікації. Зокрема, X (Twitter) є особливою платформою комунікації, яка відображає активність топ-політиків світу. Існує навіть доктринальне визначення X-дипломатії (Twitter-дипломатія) або Twiplomacy як поєднання традиційної цифрової дипломатії та Twitter [3].

X-дипломатія (Twitter-дипломатія, Twiplomacy) – це форма цифрової дипломатії, яку використовують вищі посадові особи країн як інструмент зовнішньої політики для ведення публічної дипломатії [2, p.113].

Попри те, що мережа X є не досить популярною в Україні, ця платформа містить *найпопулярніший контент* стосовно оперативних новин, військових зведень та аналітики [1].

Початок міжнародного збройного конфлікту в Україні (2014 р.), пандемія COVID-19 та повномасштабне вторгнення потребують

оперативного висвітлення і дописів, які дозволяє здійснювати X-дипломатія (Twiplomacy).

Значна частина українських посольств мають облікові записи у мережі X (Twitter), що сприяє посиленню міжнародного іміджу України.

Згідно з останніми дослідженням понад 60 % іноземних посольств в Україні мають облікові записи в X (Twitter).

Таблиця 1.

**Топ-3 найактивніших користувачів X (Twitter)
серед українських посольств та дипломатів.**

№	Країна	Посольство Посли	Рік приєд- нання	Кіль- кість підпис- ників	Кіль- кість публі- кацій
1	Йорданія	Посольство України в Йорданії (@UKRinJOR)	2014	2 816	41 500
		Керівник: Мирослава Щербатюк (@ShcherbatiukM)	2017	447	4 276
2	Туреччина	Посольство України в Туреччині (@UKRinTR)	2014	108 900	23700
		Керівник: Нариман Джелялов (@narimandzhelyai)	2024	977	94
3	США	Посольство України в США (@UKRintheUSA)	2012	1 337	20400
		Керівник: Оксана Маркарова (@OMarkarova)	2018	36 300	1 854

Таблиця демонструє, що посольства твітять набагато активніше, ніж їхні керівники-посли. Що стосується тематики публікацій то вони в основному про війну в Україні. Тому використання X-дипломатії (Twiplomacy) для дипломатії є дуже доцільним у період кризи.

Таким чином, у сучасному світі X (Twitter) стає потужним інструментом комунікації, що дозволяє світовим лідерам та відомим особам транслювати важливі повідомлення мільйонам людей по всьому світу. X (Twitter) все більше трансформує традиційну дипломатичну практику для досягнення диплома-

тичних цілей, щодо зовнішньополітичних ініціатив своєї країни. Ведення дипломатії в сучасному світі показує, що X-дипломатія суттєво впливає на міжнародні відносини, змінює традиційні правила комунікацій і має значний потенціал.

Список використаної літератури:

1. Galerea news. Топ соціальних мереж в Україні. URL: <https://galera.news/top-sotsialnykh-merezh-v-ukraini-11128/>
2. Osondu-Oti, A., Agesin, J. O., & Olominu, O. (2024). The Impacts of Twitter (X) Diplomacy on Contemporary International Relations. *Journal of Contemporary International Relations and Diplomacy (JCIRD)* Vol. 5, No. 1, 2024, pages 110-127. URL: [file:///C:/Users/Admin/Downloads/ARTICLE---007+\(1\)%20\(3\).pdf](file:///C:/Users/Admin/Downloads/ARTICLE---007+(1)%20(3).pdf)
3. Radhika Chhabra (2020). Twitter Diplomacy: A Brief Analysis. ORF Issue Brief No. 335, Observer Research Foundation, URL: <https://www.orfonline.org/research/twitter-diplomacy-abrief-analysis-60462>.

Ігор Земан
кандидат юридичних наук, доцент
Львівський національний університет
імені Івана Франка

НОВІ ВИКЛИКИ ТА ПЕРЕВАГИ ЦИФРОВОЇ ДИПЛОМАТІЇ ДЛЯ МІЖНАРОДНОГО ПРАВА

Дипломатія є однією з найдавніших форм міждержавних відносин. Впродовж століть методи дипломатії розвивались разом з поступом людської цивілізації. В епоху інтернету та електронних гаджетів невідворотним є вплив і на традиційні засоби ведення міжнародних відносин.

Цифрова дипломатія стає важливим фактором міжнародної комунікації та відкриває нові можливості для посилення діалогу між різними країнами. Цифрова дипломатія не може застосовувати класичні протокольні формати та створює нові сфери для

координації та переговорів. Особливою рисою цифрової комунікації є можливість для офіційної влади та громадськості обмінюватись інформацією в реальному часі. Проте цифрова дипломатія створює не лише можливості, але і виклики. Крім очевидних переваг щодо оперативного та актуального висвітлення інформації чи позиції такі технології містять і небезпеку. По-перше йдеться про відсутність «права на помилку» у висловлювання офіційних представників держави, а по-друге є ризик викиду дезінформації шляхом хакерських атак на офіційні соціальні сторінки вищих посадових осіб держави [4, с. 31].

Сучасні міжнародно-правові акти у сфері дипломатії сьогодні не охоплюють усі тонкощі використання цифрової дипломатії. Зокрема положення Віденської конвенції про дипломатичні зносини 1961 р. та Віденської конвенції про консульські зносини 1963 р. не містять жодних згадок про цифрові канали комунікації. Аналогічні прогалини містяться щодо відсутності критеріїв цифрової дипломатичної установи. Класичні привілеї та імунітети дипломатичних представництв та дипломатичних агентів потребують поширення на цифровий контент і специфічне обладнання (сервери), які забезпечують його роботу.

Водночас «позитивному» кодифікованому праву у таких ситуаціях завжди на допомогу приходять міжнародний звичай. Можна припустити, що вже формуються звичаєві норми, які відносять цифрові платформи комунікації до різновидів сучасних методів ведення дипломатичних переговорів.

Останнім часом набирає популярності формат віртуального дипломатичного представництва. Формат цифрових посольств активно застосовують деякі країни (США, Ізраїль, Сінгапур). Віртуальні посольства створюються переважно у особливих випадках коли відкриття посольства на території приймаючої сторони ризиковане або коли посольство закладає плацдарм для поглиблення відносин чи навіть у випадку відсутності встановлених офіційних дипломатичних відносин між країнами [1, с. 19].

Українське законодавство частково врегульовує можливість створення цифрового посольства. Згідно ст. 5 закону «Про

дипломатичну службу» передбачено можливість створення Посольства України з резиденцією Надзвичайного і Повноважного Посла України в Києві [2]. Таку опцію було конкретизовано у 2021 р. у «Положенні про закордонні дипломатичні установи України». Там йдеться що «Надзвичайний і Повноважний Посол України з резиденцією в Києві є вищим офіційним представником України у державі акредитації, в якій не утворено закордонну дипломатичну установу України, здійснює загальне керівництво та координацію діяльності посадових та інших осіб, членів делегацій України, які перебувають у цій державі з метою виконання посадових або службових обов'язків» [3].

Таким чином, нині існує потреба перегляду міжнародно-правових документів у сфері класичної дипломатії. Потребують розробки правові норми присвячені регулюванню ефективної та безпечної цифрової дипломатії. Сьогодні фактично наявне лише фрагментоване правове регулювання цифрової дипломатії. Існують прогалини щодо уніфікованих правових норм, технологічного захисту офіційних онлайн платформ та відповідальності за дезінформацію в цифровій дипломатії. Україні варто переходити до стадії впровадження віртуальних дипломатичних представництв на практиці.

Список літератури

1. Маркарян М. Віртуальне дипломатичне представництво: адміністративно-правовий аналіз. Київський часопис права. 2021. № 2. С. 18-22. URL: <http://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/17/16>
2. Про дипломатичну службу. URL: <https://zakon.rada.gov.ua/laws/show/2449-19#Text>
3. Про Положення про закордонні дипломатичні установи України. URL: <https://zakon.rada.gov.ua/laws/show/99/2021#Text>
4. Britchenko I. Digital diplomacy as a tool of international legal communication: Challenges and prospects. *Journal of International Legal Communication*. 2025. Vol. 16(1). P. 30–39. URL: <https://doi.org/10.32612/uw.27201643.2025.16.1.pp.30-39>

Ігор Іжнін
кандидат політ. наук, доцент,
Любомир Харченко
Львівський національний університет
імені Івана Франка

ІНСТРУМЕНТИ ЦИФРОВОЇ ДИПЛОМАТІЇ В УМОВАХ ТРАНСФОРМАЦІЇ МІЖНАРОДНИХ ВІДНОСИН

Під терміном «цифрова дипломатія» (англ. *digital diplomacy*) зазвичай розуміють застосування інформаційно-комунікаційних технологій (ІКТ), соціальних медіа, даних, алгоритмів і новітніх комунікаційних каналів у дипломатичній практиці¹.

При цьому слід окремо відмітити, що цифрова дипломатія не замінює традиційну дипломатію, але доповнює її: реалізуючи нові методи комунікації і залучаючи нові (ширші) аудиторії. Через активне використання ІКТ і цифрових платформ обміну повідомленнями особливого значення набувають швидкість реагування на події і на реакції аудиторій, значно зростає увага до публічного компоненту діяльності дипломатів, виникає потреба більш ретельно вивчати інформаційні (і комунікативні) характеристики «зовнішніх аудиторій» (тобто аудиторій, які безпосередньо не залучені у професійну дипломатичну діяльність, але, тим не менше, можуть виступати агентами просування інтересів в державі перебування чи на міжнародній арені: неурядові організації, молодіжні організації, професійні спілки, бізнес-асоціації, культурні, спортивні та інші спілки і об'єднання тощо).

Сучасний етап трансформації міжнародних відносин характеризується тим, що держави (себто органи державної влади, державні організації та інституції, державні діячі і політики) все ширше застосовують цифрові та інформаційно-комунікаційні технології для організації та здійснення своєї діяльності, а частина

¹ Digital diplomacy: Where tech meets international relations. URL: <https://www.ie.edu/uncover-ie/digital-diplomacy-where-tech-meets-international-relations/>

діяльності переноситься в цифровий простір. Не є виключенням і дипломатія. Поширення цифрових технологій та платформ трансформують канали дипломатичної та, ширше, зовнішньополітичної комунікації. Конкуренція за цифровий простір, кібербезпека, керування даними стають важливими елементами міжнародних відносин. Дипломатія в наш час відбувається не лише за зачиненими дверима, а в онлайн-середовищі, де громадська думка, наративи й медіа мають значний вплив на рішення, які приймаються. Втім, відзначається зростаюча невизначеність і багатомірність викликів – від кіберзагроз до дезінформації та інформаційного впливу на системи прийняття рішень, від цифрового розриву до етичних проблем, пов'язаних із використанням алгоритмів. Тим не менше, можна стверджувати, що цифрова дипломатія є неминучою відповіддю на те, що міжнародні відносини стають більш мережевими, оперативними та інформаційно насиченими.

При цьому слід відзначити, що Стратегія публічної дипломатії МЗС України розглядає цифрову дипломатію як один з напрямів публічної дипломатії, а саме як напрям, де «професійне та систематичне використання можливостей соціальних мереж і цифрових платформ дозволяє налагодити пряму комунікацію з громадянами іноземних країн з метою формування у них позитивного сприйняття України»¹.

В той же час інструменти цифрової дипломатії можна визначити як сукупність технологій, платформ та алгоритмів, які дозволяють: здійснювати ефективну міжнародну комунікацію в цифровому середовищі; формувати зовнішній імідж держави через відкритість і прозорість; протидіяти інформаційним загрозам і кризам; підвищувати аналітичну спроможність дипломатичних інституцій;

¹ Стратегія публічної дипломатії МЗС України. URL: <https://mfa.gov.ua/storage/app/sites/1/Стратегія/public-diplomacy-strategy.pdf>

створювати інтелектуальну, технологічно стійку систему зовнішньополітичного управління¹.

Основні інструменти цифрової дипломатії:

1. Комунікаційні платформи та соціальні медіа (найпоширеніша трактовка цифрової дипломатії): акаунти міністерств закордонних справ, посольств, дипломатів у соцмережах (Twitter/X, Facebook, Instagram, YouTube) – відомі як «твіт-дипломатія» (Twiplomacy). Метою є прямиий контакт із зовнішньою аудиторією (громадськість, діаспора, міжнародні спільноти), швидка реакція, формування іміджу, підвищення прозорості. Перевагами є: низька вартість, велике охоплення, можливість мультимедійного формату. В той же час є ризик дезінформації, «звинувачення» у неофіційній дипломатії, відсутність контролю над реакціями.

2. Аналітика даних, Big Data, ШІ-інструменти: використання аналітики соцмереж, моніторингу настроїв, великої об'ємів даних (big data) та генеративного ШІ для передбачення ризиків, формування стратегій комунікації, оцінки суспільної думки. Наприклад, аналіз настроїв щодо дипломатичних подій, зміна наративів на основі моделювання. Використовується, як правило, як частина систем підтримки прийняття рішень, своєчасного реагування, підвищення якості комунікації. Втім, в цьому випадку викликами є етичні питання, алгоритмічна упередженість, залежність від використовуваних наборів даних.

3. Платформи громадської участі: залучення громадян, діаспори, неурядових організацій через цифрові канали – народна (громадська) дипломатія. Прикладом є онлайн-хакатони, онлайн-конференції, які передбачають залучення різнопланових і розпорошених географічно аудиторій з метою вирішення міжнародно значущих задач/проблем. Перевагами тут є розширення спектру дипломатичної участі у суспільно і міжнародно значущих подях, підвищення авторитетності (як події,

¹ Digital Diplomacy: Transforming International Relations in the 21st Century. Tech Diplomacy Institute. URL: <https://tech-diplomacy.com/digital-diplomacy-transforming-international-relations-in-the-21st-century/>

так і залучених дипломатів), створення нових каналів впливу. Але, при цьому, проблемними моментами з точки зору дипломатії є: забезпечення достовірності (при подальшому поширенні інформації), контроль над (стратегічним) нарративом, цифровий розрив між аудиторіями.

4. Кризові та іміджеві інструменти, які використовуються для швидкого реагування, підтримки/підвищення довіри з боку громадськості та захисту іміджу держави¹. До них можна віднести: системи кризової комунікації (GPS-сповіщення – інформування під час надзвичайних ситуацій), публічна дипломатія онлайн (#DigitalUkraine, United24 Media – формування міжнародного іміджу через комунікаційні кампанії в цифровому просторі), фактчекінг і просування контрнарративів (StopFake, EUvsDisinfo – протидія дезінформації). Викликами є складність фільтрації повідомлень, обмежений контроль над комунікаційними каналами, залежність від алгоритмів соцмереж, швидкість поширення фейків, відсутність уніфікованих стандартів перевірки.

5. Інноваційні інструменти, котрі формують цифрову дипломатію майбутнього на основі ШІ, VR та блокчейну. Прикладом є VR/AR-переговори та віртуальні саміти (ООН, UNESCO), блокчейн-інструменти для верифікації угод і документів (Smart Contracts), Quantum та ШІ-аналітика для прогнозування ризиків і сценаріїв (DeepMind Diplomacy). Втім, викликами є відсутність правових норм, етичні питання конфіденційності, технічна складність, алгоритмічна упередженість, технологічна нерівність між країнами.

Європейська служба зовнішніх справ (EEAS) зазначає, що запуск ініціативи «Digital Diplomacy for an inclusive and sustainable digital future» свідчить про активне включення цифрової дипломатії в

¹ Digital Diplomacy and Its Tools. DiploFoundation. Geneva: DiploEdu. URL: <https://www.diplomacy.edu/topics/digital-diplomacy/>

стратегію ЄС¹. У свою чергу Україна має високий рівень цифрового розвитку, але ще не достатньо використовує цифрову політику як частину зовнішньополітичних пріоритетів².

Отже, в сучасних умовах трансформації міжнародних відносин цифрова дипломатія стала важливим інструментом зовнішньополітичної діяльності держав. Вона поєднує технології, комунікаційні платформи та аналітичні алгоритми для забезпечення ефективної міжнародної взаємодії, формування позитивного іміджу, оперативного реагування на кризи та протидії дезінформації. Інструменти цифрової дипломатії – від соціальних медіа та Big Data-аналітики до блокчейну й ШІ – формують новий формат глобальної комунікації, де швидкість, відкритість і технологічна стійкість визначають успіх дипломатичної політики. Для України розвиток цифрової дипломатії є важливим інструментом посилення міжнародної суб'єктності, інформаційної безпеки та інтеграції у світовий цифровий простір. Однак при цьому цифровізація (дипломатії) також створює нові виклики та загрози, які потребують оперативного реагування та адаптації існуючих (класичних) форм дипломатичної діяльності.

¹ Digital Diplomacy for an inclusive and sustainable digital future. The Diplomatic Service of the European Union. URL: https://www.eeas.europa.eu/eeas/digital-diplomacy_en

² Omelianenko V. EU's and Ukraine's approaches to digital diplomacy in the geopolitics of technologies. URL: <https://prismua.org/en/english-eus-and-ukraines-approaches-to-digital-diplomacy-in-the-geopolitics-of-technologie>

*Ганна Іпполітова
студентка
Львівський національний університет
імені Івана Франка¹*

РОЗВИТОК ЦИФРОВОГО ПРОСТОРУ УКРАЇНИ ЯК СКЛАДОВА ГАРМОНІЗАЦІЇ З ПОЛІТИКАМИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Цифрова трансформація стала одним із найважливіших напрямків європейської інтеграції України, набуваючи особливого значення в контексті прагнення країни до повноправного членства в Європейському Союзі. Згідно з даними аналітичного звіту "Reform Radar", станом на кінець 2024 року Україна виконала 71% вимог Угоди про асоціацію з ЄС у сферах науки, технологій, інновацій, космосу та цифрової інтеграції [1]. Це свідчить про значний прогрес, але також вказує на необхідність подальшої роботи для досягнення повної сумісності з європейськими стандартами. Актуальність теми посилюється декількома факторами. По-перше, цифрова трансформація України відбувається в умовах повномасштабної війни, коли ефективне електронне урядування стало критично важливим для забезпечення стабільності держави та її зв'язку з громадянами [2]. По-друге, Європейський Союз надає Україні безпрецедентну підтримку в цифровій сфері – з 2016 року обсяг фінансування перевищив €51 мільйон [3]. По-третє, успішна гармонізація з цифровими політиками ЄС відкриває для України доступ до Єдиного цифрового ринку, що створює нові можливості для економічного зростання, залучення інвестицій та розвитку інноваційного сектору [4].

Україна демонструє один із найдинамічніших процесів цифрової трансформації у світі, піднявшись з 30-го місця у 2022 році на 16-е

¹ Науковий керівник: Сичов Віктор Вікторович, кандидат політичних наук, доцент кафедри міжнародних відносин і дипломатичної служби Львівського національного університету імені Івана Франка

місце в Індексі розвитку електронного урядування у 2024 році [2]. Цей стрибок відбувся всього за два роки в умовах війни, що робить український досвід унікальним та гідним детального аналізу.

Мета цієї роботи – провести комплексний аналіз розвитку цифрового простору України в контексті гармонізації з політиками Європейського Союзу.

Процес системної цифрової трансформації України розпочався у 2019 році зі створенням Міністерства цифрової трансформації [2]. Це рішення дозволило реалізувати масштабні зміни у сфері електронного урядування. Правовою основою співпраці між Україною та ЄС у цифровій сфері є положення Угоди про асоціацію, а також домовленості, досягнуті на саміті Україна-ЄС та в рамках двосторонніх органів Асоціації [4]. Також Україна імплементувала законодавство ЄС про електронні комунікації, яке набрало чинності у січні 2022 року, що відображає пріоритет України щодо подальшої інтеграції до Єдиного цифрового ринку ЄС [4].

В свою чергу, Європейський Союз реалізує в Україні низку масштабних проєктів, спрямованих на підтримку цифрової трансформації та гармонізацію законодавства. Розглянемо детально кожен з цих проєктів.

1. Програма EU4Digital охоплює широкий спектр напрямків: зниження тарифів на роумінг, розвиток високошвидкісного ширококутного зв'язку, покращення кібербезпеки, гармонізацію цифрових рамок у суспільстві від логістики до охорони здоров'я, розвиток цифрових навичок та створення робочих місць у цифровій індустрії [4].

2. Проєкт EGOV4UKRAINE (2016-2021), завдяки ньому було розроблено і впроваджено дві нові системи електронних послуг, що забезпечують кращий обмін даними між органами влади [4]. Його продовженням став проєкт EU4DigitalUA (2020-2024) з бюджетом €20,5 мільйона, який зосередився на п'яти ключових цілях: сумісність та інфраструктура цифрового уряду, інституційне зміцнення, електронні послуги, кібербезпека та захист даних [3].

3. З листопада 2022 року реалізується проєкт DT4UA ("Цифрова трансформація для України") з бюджетом €17,4 мільйона, який продовжує підтримку цифрової трансформації України [5]. Проєкт зосереджений на чотьох пріоритетних напрямках: розвиток цифрових послуг та середовища надання послуг "Дія", покращення обміну даними між реєстрами та постачальниками послуг, розвиток інфраструктури електронної ідентифікації відповідно до регламенту eIDAS, та розробка системи електронного управління справами [5].

Завдяки проєкту DT4UA Україна стала першою країною поза ЄС, чий цифровий підпис "Дія.Підпис" відповідає вимогам eIDAS і визнається в Європейському Союзі [6]. Це дозволяє громадянам України підписувати документи в цифровому форматі, які визнаються в усіх країнах ЄС, відкриваючи доступ до транскордонних цифрових послуг без необхідності фізичної присутності.

4. У вересні 2022 року Україна підписала угоду про приєднання до програми ЄС "Digital Europe" з бюджетом €7,5 мільярда [7]. Ця угода дозволяє українським організаціям подавати заявки на фінансування та підтримку проєктів у сферах суперкомп'ютингу, штучного інтелекту, розширених цифрових навичок та інших цифрових напрямків [7].

Попри значні досягнення, Україна стикається з низкою викликів на шляху повної гармонізації з цифровими політиками ЄС:

1) кібербезпека – у 2024 році кількість кіберінцидентів зросла на 49,2% порівняно з 2022 роком [1];

2) захист персональних даних та регулювання ШІ – необхідна подальша адаптація українського законодавства до стандартів ЄС, особливо в сферах захисту даних та регулювання штучного інтелекту;

3) реформа місцевої цифрової інфраструктури – необхідна подальша робота для забезпечення ефективної цифрової трансформації на регіональному рівні.

4) розширення широкосмугового доступу – 2024 по 2026 роки планується розширення широкосмугового інтернету в селах, розвиток 5G-інфраструктури та підвищення цифрової грамотності.

Таким чином, розвиток цифрового простору України як складової гармонізації з політиками Європейського Союзу демонструє значний прогрес та системний підхід, особливо вражаючий в умовах повномасштабної війни. Україна змогла перетворити цифрову трансформацію з технологічного виклику на стратегічну перевагу, що забезпечує стійкість держави та її просування до європейської інтеграції.

Список літератури

1. Vox Ukraine. (2024). State Digital Transformation in Ukraine: 2019–2024 Review. URL: <https://voxukraine.org/en/state-digital-transformation-in-ukraine-2019-2024-review> (дата звернення: 01.11.2025).
2. E-Governance Academy. (2025). Ukraine is digital by design: Resilience and trust, embedded in governance. URL: <https://ega.ee/ukraine-digital-by-design/> (дата звернення: 01.11.2025).
3. European External Action Service. (2024). The European Union supports Ukraine's digital transformation: results of EU4DigitalUA's work. URL: https://www.eeas.europa.eu/delegations/ukraine/european-union-supports-ukraines-digital-transformation-results-eu4digitaluas-work_en?s=232 (дата звернення: 01.11.2025).
4. Mission of Ukraine to the European Union. (2024). Digital transformation. URL: <https://ukraine-eu.mfa.gov.ua/en/2633-relations/galuzeve-spivrobitnictvo/yedinij-cifrovij-rinok-yes> (дата звернення: 01.11.2025).
5. E-Governance Academy. (2025). Digital Transformation for Ukraine (DT4UA). URL: <https://ega.ee/project/dt4ua/> (дата звернення: 01.11.2025).
6. EU4Ukraine. (2025). European Union Supports Ukraine's Digital Path to the EU: DT4UA Project Results. URL:

<https://eu4ukraine.eu/en/whats-happening-en/news-en/igital-path-to-the-eu-dt4ua-project-results.html> (дата звернення: 01.11.2025).

7. Science | Business. (2022). Ukraine joins Digital Europe programme. URL: <https://sciencebusiness.net/news/ukraine-joins-digital-europe-programme> (дата звернення: 01.11.2025).

Оксана Когут-Ференс
кандидат економічних наук, доцент
Львівський національний університет
імені Івана Франка
ORCID ID: 0000-0001-6015-5205

СТРАТЕГІЧНІ КОМУНІКАЦІЇ УКРАЇНИ В УМОВАХ ВІЙНИ

Стратегічні комунікації це один з ключових елементів забезпечення національних інтересів держави, а в умовах війни, - це паралельний процес з військовими діями для збереження незалежності, територіальної цілісності та суверенітету держави. Основними традиційними інструментами стратегічним комунікації є публічна дипломатія, військові комунікації та інформаційні і психологічні операції [1, 2]. Проте в умовах війни зовнішні комунікації країни дещо змінюють кут погляду, акцентуючи увагу на національній самоідентифікації, безпекових національних інтересах та пошуку не лише економічних, а військово-політичних партнерів, тому сучасними інструментами СтатКому України є:

- публічна дипломатія та налагодження стратегічного партнерства;
- військові та оборонно-стратегічні комунікації;
- інформаційні операції спрямовані на підкреслення національної ідентифікації українців;
- активна боротьба з інформаційною пропагандою;
- забезпечення стійкої інформаційної безпеки.

Відповідно реалізація стратегічних комунікацій України здійснюється на основі ряду законодавчих документів, в яких чітко

зазначено пріоритетність ведення діалогу та досягнення спільних стратегічних рішень з міжнародними партнерами, зокрема це Стратегія воєнної безпеки України [3], Указ Президента України про Стратегію забезпечення державної безпеки [4], Комунікаційна стратегія Міністерства закордонних справ України [5] та інші.

Поєднання військової та дипломатичної сили України лежить в основі забезпечення миру, тому реалізація довгострокової стратегії національної безпеки є неможливим без ефективних стратегічних комунікацій (див. рис.1).



Рис.1. Вплив ефективних стратегічних комунікацій на національну безпеку України в умовах війни

Джерело: розробка автора

Тому реалізація ефективних стратегічних комунікацій є основою збереження цілісності країни та ефективному протистоянні агресору, а дієвий комунікативний апарат країни є інструментом

пришвидщення європейської інтеграції України та економічної і інфраструктурної відбудови після завершення воєнних дій.

Список використаної літератури та джерел

1. Меленко, О.С. Стратегічні комунікації як правова категорія. *Правничий часопис* (2023): 85.
2. Новицький, В.Я. "Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах." *Інформація і право* 1 (40) (2022): 111-118.
3. Стратегія воєнної безпеки України : Указ Президента України No 121/2021 від 25 березня 2021 року „Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року „Про Стратегію воєнної безпеки України””.
4. Про Стратегію забезпечення державної безпеки: Указ Президента України від 16 лютого 2022 року No 56/2022.
5. Комунікаційна стратегія МЗС України розроблена за підтримки експертів Групи кризового управління Програми розвитку ООН в Україні при МЗС України <https://mfa.gov.ua/storage/app/sites/1/Стратегія/communication-strategy.pdf>

Олександр Кучик
кандидат історичних наук, доцент,
Наталія Стручок
кандидат економічних наук, доцент
Львівський національний університет
імені Івана Франка

МІЖНАРОДНИЙ ІМІДЖ ДЕРЖАВИ ЯК ОБ'ЄКТ КРИЗОВОГО МЕНЕДЖМЕНТУ У ЦИФРОВОМУ КОМУНІКАЦІЙНОМУ СЕРЕДОВИЩІ

Тенденції поглиблення міжнародної інтеграції України в контексті становлення нового світового порядку, завдання формування позитивного іміджу держави на міжнародній арені із

збереженням культурної унікальності та ідентичності, а також пошук консолідуючої національної ідеї залишаються ключовими чинниками її сучасного прогресивного розвитку.

Сучасні процеси формування іміджу держави на міжнародній сцені та роль інформаційно-комунікаційних технологій у цьому контексті є об'єктом дослідження представників різних наукових шкіл і підходів у світі. Зокрема, ці питання активно розглядаються у межах політології, теорії соціальних технологій, політичної культури та теорії комунікації, які визначають ключові чинники як внутрішньої, так і зовнішньої політики держав.

Імідж держави являє собою сукупність взаємопов'язаних об'єктивних характеристик її системи (економічних, географічних, національних, демографічних та інших), що сформувалися впродовж історичного розвитку державності як складної багатокомпонентної підсистеми світового порядку. Рівень узгодженості та ефективності функціонування цих елементів впливає на динаміку соціально-економічних, суспільно-політичних, національно-конфесійних та інших процесів. Імідж держави — це база, що визначає, яку репутацію має країна у свідомості своїх громадян і світової спільноти в результаті дії або без дієвості тих або інших її суб'єктів, що взаємодіють із зовнішнім світом [1].

На формування іміджу України впливають три групи факторів:

1) природно - ресурсний потенціал; національна та культурна спадщина; постійні геополітичні фактори — географічне положення, площа території, довжина кордонів держави, вихід до морів; історичні події, що вплинули на розвиток української державності (завоювання, великі наукові й географічні відкриття), а також внесок видатних українців, діяльність яких нерозривно пов'язана з історією розвитку країни; базова форма державного устрою та структура управління;

2) соціально - психологічні настрої в українському суспільстві; форми суспільно - політичної інтеграції українців, структура, характер і принципи діяльності суспільно - політичних об'єднань України; моральні аспекти розвитку українського суспільства;

3) стабільність української економіки, яка оцінюється рівнем доходів на душу населення, обсягом залучених інвестицій, фінансовою забезпеченістю бюджетів усіх рівнів, гарантією прав і свобод господарюючих на українському ринку суб'єктів реального сектора економіки; правовий простір України та відповідність українських правових норм міжнародним вимогам; функції, повноваження й механізми державного регулювання різних галузей і сфер діяльності в українській державі (ефективність владної конструкції) [2].

В умовах сучасних міжнародних відносин формування позитивного образу держави виступає важливою складовою дипломатичної діяльності, оскільки ефективність роботи дипломатичних інституцій визначається здатністю посилювати позиції країни у світовій політичній системі та узгоджувати її національні інтереси з інтересами інших держав.

Професійні дипломати, виступаючи від імені держави на міжнародній арені, відіграють ключову роль у зміцненні її авторитету та формуванні позитивного світового іміджу, забезпечуючи захист національних інтересів на глобальному рівні. Водночас серед різних інструментів впливу особливого значення в сучасних умовах набувають цифрові технології, що стають важливим засобом підтримки та просування міжнародного іміджу держави.

В рамках реалізації іміджевої кампанії було запущено міжнародну комунікаційну кампанію WhatWeAreFightingFor, мета якої формування іміджу України, як держави у міжнародному комунікаційному середовищі.

Це унікальний спецпроект на платформі UKRAINE.UA, який представляє особливість кожного регіону України у боротьбі за державну цілісність, демократію, свою історичну спадщину та культуру, мову та можливість самостійно обирати своє майбутнє.

UKRAINE.UA – це екосистема офіційних цифрових платформ України для комунікації та взаємодії з міжнародною аудиторією, що реалізується в рамках публічної дипломатії Міністерством закордонних справ України [3].

Одним із ключових ресурсів реалізації зовнішньої політики є створення позитивного образу держави у міжнародному інформаційному середовищі. Формування іміджу країни є тривалим процесом і залежить від низки чинників: рівня економічного розвитку, життєвого добробуту населення, активності інвестиційної діяльності, туристичної привабливості, впровадження сучасних технологій та інших складових.

Список використаних джерел та літератури:

1. Вербицька Г. Міжнародний імідж України: проблеми та шляхи формування. URL: http://ijimv.knukim.edu.ua/zbirnyk/1_1/knukim_zbirka170x265mmCMYK_part2_print.pdf
2. Boulding, Kenneth. National Image and International System. URL: <https://www.semanticscholar.org/paper/National-images-and-international-systems-Boulding/60d52900ee54811aad78f1fd4e07af580e7d4e7c>.
3. Офіційна комунікаційна платформа про Україну Міністерства закордонних справ України. URL: <https://ukraine.ua/>
4. Нагорняк, Т., Польовий, М., Бондаренко, С., & Осмоловська, А. (2022). Комунікативний вимір формування і просування публічного іміджу держави. *Copernicus Political and Legal Studies*, (1).

*Аліна Лега
студентка
Львівський національний університет
імені Івана Франка*

ДОСВІД НАТО У СФЕРІ БОРотьБИ З ІНФОРМАЦІЙНИМИ ЗАГРОЗАМИ В УКРАЇНІ

У сучасному глобалізованому світі, де інформація та технології відіграють ключову роль у створенні передумов демократичного суспільства кібербезпека стала одним із найбільших викликів для національної та міжнародної безпеки не тільки для України, але й

для всього світу. Необхідно зазначити, що Україна частково перейняла модель інтегрального підходу до протидії гібридним загрозам НАТО, створивши два окремі органи – Центр протидії дезінформації при РНБО, діяльність якого є більш закритою, та Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики, який виконує функції СтратКому.

Побудову міцної співпраці з НАТО у сфері інформаційної безпеки за допомогою цих двох органів. Необхідною умовою для цього є їх політична незалежність, відсутність тиску та спроб використання у внутрішньополітичній боротьбі, й інституційна стійкість, адже Альянс не зацікавлений у співпраці з нестабільним партнером, принципи діяльності якого не є прозорими та зрозумілими.

При цьому для України така співпраця може мати практичну безпекову цінність, стати стратегічним кроком до євроатлантичної інтеграції, а також дати позитивний іміджевий результат. Той факт, що найбільш інтенсивні гібридні, зокрема й інформаційні, атаки Російська Федерація веде саме проти України є визнаним – так само, як і системні спроби використовувати Україну в якості тестового майданчика для нових зразків гібридного впливу. Це надає українській державі перевагу передового досвіду, в отриманні якого Альянс глибоко зацікавлений. Можливість ділитись таким досвідом у рамках системної співпраці сприятиме принаймні точковій реалізації євроатлантичної інтеграції на практиці. Враховуючи, що як в роботі СтратКому НАТО, так і в стратегії протидії гібридним загрозам Альянсу велику роль відіграє моделювання криз та практичні навчання, з безпекової точки зору, для України участь у подібних ініціативах дала б цінний досвід. Побіжно вона стала б сигналом державі-агресору про реальне зближення з партнерами по НАТО, яке є необхідним для стримування та знешкодження.

Таким чином, для України є бажаною участь у діяльності СтратКому НАТО – зважаючи на те, що він надає допомогу в «поліпшенні спроможностей стратегічних комунікацій всередині Альянсу та союзникам». Київ має можливість використати

задекларовану підсумками брюссельського саміту 2021 підтримку «рішення, ухваленого у 2008 році на Бухарестському саміті НАТО, про те, що Україна стане членом Альянсу і при цьому План дій щодо членства (ПДЧ) буде невід'ємною частиною цього процесу». З наданням ПДЧ можливість для спільних дій зросте, однак вона існує вже зараз і полягає, зокрема, в ініціюванні спільних зі СтратКомом навчань, інформаційних кампаній та досліджень, у рамках яких Україна може запропонувати власну широку експертизу. Такий же підхід справедливий і для інших органів, які у рамках інтегрального підходу НАТО функціонують на протидію гібридним загрозам.

Окрім того, для України залишається актуальним підхід із залученням широкого кола фахівців із недержавного сектору для протидії дезінформації та іншим гібридним загрозам. Саме таким шляхом пішов Альянс, формуючи відповідні органи, аби забезпечити комплексне та стратегічне бачення їх роботи. Створення центру при Міністерстві культури та інформаційної політики відбувалось за таким же принципом, який важливо підтримувати у подальшій роботі інституції та поширити, там, де це можливо, на роботу фахового центру при РНБО.

Доречною є кооперація із державами Балтії та Польщею, які мають найближче до України розуміння гібридних загроз, є її постійними адвокатами на міжнародному рівні – а також активними учасниками роботи СтратКому та інших спеціалізованих органів НАТО. Три головних напрямки цифровізації України: застосування штучного інтелекту; системи захищеного зв'язку; системи управління інформаційними джерелами. Державна служба спеціального зв'язку та захисту інформації України забезпечує виконання завдань у рамках реалізації РНП (Річна національна програма співробітництва України), зокрема за такими напрямками: інформаційна безпека у сфері криптографічного і технічного захисту інформації, що передбачає проведення планових заходів контролю за станом технічного захисту інформації НАТО з обмеженим доступом у державних органах України; кібернетична безпека, що передбачає взаємодію з відповідними органами іноземних держав і

міжнародними організаціями в режимі реального часу через Центр реагування на комп'ютерні інциденти CERT-UA, який створений і функціонує у складі Держспецзв'язку; забезпечення провадження інспекційної діяльності, в тому числі проведення спостережних польотів, відповідно до Договору про звичайні збройні сили в Європі, Віденського документа 2011 року про заходи зміцнення довіри і безпеки та Договору з відкритого неба.

Особливе партнерство з НАТО є невід'ємною складовою євроінтеграційного курсу України, а РНП розглядається як ефективний інструмент для здійснення євроінтеграційних реформ. Відповідно до Стратегічної мети 2.12. «Державна служба спеціального зв'язку та захисту інформації України забезпечує функціонування та розвиток державної системи урядового зв'язку» в рамках наступної цілі створення інфраструктури безпеки інформації, яка відповідає політиці НАТО: захист у кіберпросторі державних інформаційних ресурсів та інформації, кіберзахист об'єктів критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах; створення необхідної правової бази у сфері безпеки інформації; наявність достатнього ресурсного та експертного забезпечення для акредитації комунікаційно-інформаційних систем.

Приклад підходу НАТО в захисті персональних даних: аналітики звертають увагу, що транснаціональні компанії (Google, Apple, Facebook, Amazon, Microsoft) збирають величезні обсяги персональних даних для просування реклами, які до того ж можна використати з метою формування політичних уподобань, просування потрібних ідей.

У 2016 році був введений в дію Загальний регламент захисту персональних даних (General Data Protection Regulation – GDPR), на підставі якого зокрема, користувачі Інтернету мають право знати, які дані збираються під час відвідування певного веб-сайту. Регламент також вимагає, щоб дані цих користувачів не виходили за межі будь-якому вигляді. Наразі у держав-членів відсутнє «колективне» усвідомлення кіберзагроз, що пов'язано з тим, що національні органи влади систематично не обмінюються

інформацією (на відміну від приватного сектора), яка може допомогти оцінити стан кібербезпеки в НАТО та ЄС. Держави-члени повідомляють лише про частину інцидентів, а обмін інформацією не є систематичним чи всебічним; кібератаки можуть бути лише одним із аспектів узгоджених зловмисних атак, направлених проти європейських держав-членів.

В світлі цього ухвалено Стратегію кібербезпеки ЄС на цифрове десятиліття, яка є ключовим компонентом формування цифрового майбутнього Європи, Плану Єврокомісії щодо відновлення Європи, Стратегії Союзу безпеки на 2020–2025 роки, Глобальної стратегії зовнішньої політики та політики безпеки ЄС та Стратегічного порядку денного Європейської Ради на 2019–2024 роки та визначає яким чином ЄС захищатиме своїх громадян, підприємства та установи від кіберзагро, яка спрямована на забезпечення глобальної та відкритої мережі Інтернет із потужним захистом для запобігання виникнення ризиків для безпеки та основних прав і свобод людей у Європі. Враховуючи прогрес, досягнутий під час виконання попередніх стратегій, вона містить конкретні пропозиції щодо розгортання трьох основних інструментів – регуляторного, інвестиційного та політичного – для застосування у трьох сферах діяльності НАТО: стійкість, технологічний суверенітет та лідерство; нарощування оперативного потенціалу для запобігання, стримування та регування; забезпечення глобального та відкритого кіберпростору.

Принцип всеосяжності (Comprehensive Approach) Україна визнає, що протидія інформаційній агресії – це завдання не лише для Збройних Сил, а й для всього державного апарату та суспільства. Це стимулює залучення МЗС, Мінцифри, СБУ, громадських організацій та медіа.

Акцент на стійкості (Resilience): Підхід НАТО зміщує фокус з лише реагування на запобігання та зміцнення здатності суспільства розпізнавати та протистояти маніпуляціям (медіаграмотність).

Стратегічні комунікації (StratCom): НАТО наголошує на важливості проактивного, єдиного та правдивого державного

нарративу. Україна інтенсивно працює над цим, щоб ефективно спростовувати дезінформацію.

Стратегія також має на меті встановити пріоритети в галузі розвитку штучного інтелекту, оскільки дана сфера в даний час розвивається найбільш стрімко і являє собою непередбачену і потенційно небезпечну технологію, пропонуючи певний баланс між державними гарантіями збереження персональних даних з одного боку та розвитком систем штучного інтелекту – з іншого.

Спираючись на «принцип повторення» як один з ключових принципів пропаганди інформаційних загроз розповсюджують свої нарративи системно, адаптуючи їх під зміни політичного порядку денного та поєднуючи з іншими дестабілізуючими процесами. Окрім поширення неправдивої, маніпулятивної інформації, широко використовує місцевих агентів країни агресора впливу для легітимізації своєї риторики та провокацій, втручається у внутрішні політичні процеси інших країн, надає фінансову підтримку відцентровим рухам, використовує корупцію як зброю, здійснює кібератаки, реалізує тиск у багатьох сферах від енергетики до культурної дипломатії. Така діяльність виходить за межі суто інформаційної політики, однак залишається з нею нерозривно пов'язаною, формуючи широкий горизонт гібридних загроз.

НАТО відповідає на таку ситуацію, формуючи декілька чітких напрямів контрзусиль. Наприклад, 2008р. поселення захисних спроможностей у кіберсфері є для Альянсу одним з пріоритетів, а в Естонії розташовано Об'єднаний центр передових технологій з кібероборони НАТО. Об'єднаний відділ розвідку і безпеки працює над глибшим розумінням та аналізом гібридних загроз.

Водночас Альянс прагне до побудови стійкої системи колективного захисту, тому активно розбудовує співпрацю з уповноваженими органами Європейського Союзу. Так, у 2016 році Генеральний секретар НАТО Єнс Столтенберг і президенти Європейської комісії і Ради Жан-Клод Юнкер і Дональд Туск підписали спільну декларацію, яка містила більше 70 пропозицій з протидії таким загрозам. У 2018 році ЄС визнав кіберпростір військовим полем діяльності та запустив Рамкову програму

кіберзахисту з шістьма основними цілями, серед яких – тісніша співпраця з НАТО для уникнення дублювання зусиль. Стратегічний компас ЄС, опублікований у 2022 році, підкреслює, що кіберпростір став ареною конкуренції, і містить заходи для зміцнення кібербезпеки, включаючи створення Європейського центру оборонних інновацій (HEDI). Російське вторгнення в Україну в 2022 році стало стимулом для ЄС, що призвело до нових ініціатив, таких як Координаційний центр кіберзахисту ЄС (EUCDCC) та нова оперативна мережа військових комп'ютерних груп реагування на надзвичайні ситуації (MICNET). ЄС також працює над підвищенням кіберстійкості через оновлену Директиву щодо безпеки мережі та інформаційних систем (NIS2) та Закон про кіберсолідарність.

При цьому основну відповідальність Альянс покладає на держави-учасниці, хоча й зазначає, що готовий надавати допомогу у рамках колективної оборони. Так, у підсумковому комюніке саміту НАТО, який пройшов у Брюсселі у червні 2021 року, зазначено, що «тоді як першочергова відповідальність за відповідь на гібридні загрози лежить на атакованій нації, НАТО готовий, за рішенням Ради, надати допомогу союзнику на будь-якому етапі гібридної кампанії, що проти нього [союзника] ведеться, включно з направленням групи підтримки з протидії гібридним загрозам. У випадку гібридної війни НАТО може прийняти рішення про застосування Статті 5 Вашингтонського договору...».

При цьому стратегія НАТО з протидії гібридним загрозам складається з трьох основних компонентів: готовності, запобігання та захисту. Згадане вище комюніке засвідчує: «НАТО та союзники продовжать готуватись до, запобігати та захищатись від гібридних атак... Ми посилюємо нашу ситуаційну обізнаність та розширюємо доступні нам інструменти для протидії гібридним загрозам, які включають дезінформаційні кампанії, розвиваючи всебічні превентивні та реактивні можливості». При цьому окремо увага приділяється кіберзагрозам, які визнаються «складними, руйнівними, примусовими та такими, що відбуваються все частіше». Для відповідей на такі загрози Альянс підтримує всеосяжну політику у сфері кібероборони, спрямовану на

формування вільного, відкритого, мирного та безпечного кіберпростору.

Базовими принципами для елементів готовності, запобігання та захисту залишаються необхідність спиратись на факти; значну роль відіграють стратегічні комунікації. Таким чином, Альянс усвідомлює комплексний характер гібридних загроз, серед яких інформаційні загрози є чинником для розуміння залученості України та набуття досвіду. Приділяючи багато уваги боротьбі з дезінформацією і створивши для цього спеціальний орган, НАТО прагне також до координації зусиль між різними відомствами, саме за допомогою цих стратегій, принципів, Україна бере активну та ефективну участь у боротьбі з інформаційними загрозами на частково прийнятій моделі підходу.

*Błażej Matula
Licencjat, Jagiellonian University,
International Relations*

UNITED24 AS A TOOL OF UKRAINIAN PUBLIC DIPLOMACY

Public diplomacy (PD), can be described as a set of actions aimed at fostering connections between people understood both as politicians and diplomats, as well as ordinary citizens. According to Mark Leonard, there are four goals of public diplomacy: “(1) Increasing people’s familiarity with one’s country, (2) Increasing people’s appreciation of one’s country, (3) Engaging people with one’s country, (4) Influencing people” (Leonard, 2002, p.9-10). The country conducting its own public diplomacy doesn’t only limit itself to creating a positive image, but also actively attempts to change commonly held unfavourable beliefs about it, and corrects them. Moreover, for some countries, a vital objective is to spread their own values around the world, encouraging the international community, as well as individual countries, if not to fully align with them, at least to modify their own set of beliefs. (Leonard, 2002, p.9-10). In the context of public diplomacy it is also important to remember its 3

dimensions. Mark Leonard writes about them as: “reactive, proactive, and relationship building”. (Leonard, 2002, p.10) The first dimension refers to the immediate response to the events, according to the state’s strategic priorities. The second one concerns periods of up to one year, and is about organizing set of events whose main goal is to disseminate consistent narrative, and therefore influence other societies. The third one, refers to periods of time longer than one year, and aims at long lasting dissemination, and acceptance of countries values. Each of mentioned dimensions is achieved by different tools. Leonard mentions three of them: “News management” – daily communication integrated with diplomatic goals, “Strategic communication” – resembles a planned communication campaign, and “Relationship building”, described as “developing lasting relationships with key individuals through scholarships, exchanges, training [...]” (Leonard, 2002 p.12-18). It is necessary to remember that public diplomacy can be lead both by diplomats, and by other entities that are independent from official policy makers. (Leonard, 2022, p.11)

The Ukrainian Ministry of Foreign Affairs perceived PD in 2021, as a “tool for building Ukraine’s resilience to hybrid threats, and effective way to promote positive image abroad”. The Public Diplomacy Strategy published a few months before the Russian full-scale invasion, included seven areas, among which was digital diplomacy (Ministry of Foreign Affairs of Ukraine, 2021). The dimensions of Ukrainian public diplomacy, focus on national security, the positive image of the country, and planned events. Tools necessary to obtain goals can be described as digital ones, which involve the usage of digital platforms or online communities. Ukrainian Prism mentions the importance of engaging big companies operating in the field of technology, and fostering cooperation between them and Ukrainian national institutions. (Ukrainian Prism, 2023)

The case of the United24, an initiative of the President of Ukraine Volodymyr Zelensky, is a good illustration of Ukrainian public diplomacy in practice. The project was launched in May 2022. Its primary goal was to serve as a digital fundraising platform to support Ukraine financially in the war effort. Between 05.05.2022, and 27.10.2025 \$

2 700 460 980 was raised (United24, 2025). A significant aspect of the United24 initiative is that people outside politics were invited to promote it, e.g. athletes like Andriy Shevchenko, actors like Hilary Swank, and academics like Timothy Snyder (United24, 2025).

The spectrum of United24 activity was soon broadened into online media. The fundraising platform is still ongoing and continues to accomplish its goals. In the meantime, United24media was created, which started functioning on YouTube, and the Instagram in July 2022. There is also United24News YouTube channel, with the oldest videos dating from April 2024. United24media is also present in the form of a website. All platforms are provided in English, except for the website, where Spanish is also available. It is also worth of mentioning the number of followers: United24media on Instagram – 764,000 followers, 5,888 posts; United24media on YouTube – 1.92 million of subscribers, 3.1 thousand films; United24News on YouTube – 42.5 thousand of subscribers, 1.4 thousand films, and United24media website with 1.7 million monthly visits (according to Similarweb).

All platforms provide the audience with an engaging visual format, through videos or photos, as well as meaningful messages in the form of written or spoken information. A good example are iconography showing maps of European countries, with an overlay indicating how much of Ukraine is currently occupied by Russia. (United24.media, 2025) Such presented issue influences the audience's imagination, and helps them to some extent to identify with Ukrainian perspective. Another example is a compilation of five short video interviews conducted with Russian POWs, and Ukrainian soldiers who survived Russian captivity. Each video is divided into two parts: the upper part shows the text spoken by one group, and the lower part by the other. Russian soldiers speak about how they are humanely treated and provided with, e.g., medical care. Ukrainians describe terrifying conditions in Russian captivity, and how they were tortured, or badly treated. This simple video compilation is highly effective in delivering a message. It creates a powerful symbolic division between those who suffer in this war while still behaving humanley, and those who violate all legal and human laws. (United24.media, 2025). It also helps audience choose the right side,

and quickly form an opinion based on videos. Therefore, United24media highly focuses on creating powerful messages that influence imagination, and appeal to symbolic thinking.

United24media's activity can be linked to two of the four goals of public diplomacy mentioned by Mark Leonardo. Particularly important in enhancing public awareness and recognition of Ukraine is sharing the country's history with non-Ukrainians, especially regarding Russian colonialism and imperialism. This is exemplified on Instagram in post titled: "Why Ukraine wants independence", which focuses on historical events such as the Holodomor, or Russian aggressive policy toward Ukraine. (united24.media, 2025). Recognition of Ukraine is also promoted through critical analysis of Russian culture. On the United24media website, there is an article dedicated to deconstructing Russian slogans like "traditional values". Readers can learn about the role of Russian Orthodox Church as propagandist, or abduction and denationalization of Ukrainian children (United24media, 2025).

The second goal of public diplomacy concerns fostering favourable attitudes toward Ukraine among people living in other countries. United24media primarily focuses on the Ukrainian army, its professionalism, and bravery. On YouTube, there are videos of successful ambushes on Russian columns of armed vehicles or effective drone attacks (United24, 2025). There are also longer videos resembling documentary films lasting around 40 minutes and depicting Ukrainian self-made weapons, with Ukrainian IT and engineering specialists as the main characters. (United24, 2025). Content dedicated to culture, is relatively limited compared to numerous materials about the war. A notable example is an Instagram post which tells about the Frankfurt Book Fair, where Ukrainian books were presented to the broader public in Germany (united24.media, 2025).

Goals described above are being achieved by two tools mentioned by Leonard: "News management", and "Strategic communication". The online website United24media contains the biggest section dedicated to news. Daily communication is also present on YouTube channel United24, where there is a live with updates on the war everyday. When it comes to the second tool, it can be stated that the entire United24media

initiative follows well planned communication campaign with clearly settled goals of informing about the reality of war in Ukraine, as well as promoting positive image of Ukrainian soldiers, and Ukrainian culture.

Bibliography:

1. Leonard, M., Stead, C. Smewing, C., 2002. *Public Diplomacy*. London: The Foreign Policy Centre.
2. United24Media (2025). Two realities of POW captivity: Torture for Ukrainians, Geneva for Russians. [online] Available at https://www.instagram.com/p/DPCKEmuDOXi/?utm_source=chatgpt.com [Accessed 28 Oct. 2025].
3. United24Media (2025). Compare temporarily occupied Ukrainian land by Russia to Europe. [online] Available at: https://www.instagram.com/p/DQAIOfodepN/?utm_source=chatgpt.com [Accessed 28 Oct. 2025].
4. United24Media (2025). Ukrainian books reach Frankfurt Book Fair. Here's what you can get there. [online] Available at: https://www.instagram.com/p/DPoS8IGDDoE/?utm_source=chatgpt.com [Accessed 28 Oct. 2025].
5. United24Media (2025). Why Ukraine wants independence: A history of Russian Aggression. [online] Available at: https://www.instagram.com/p/DNqje6As9g0/?utm_source=chatgpt.com [Accessed 28 Oct. 2025].
6. United24Media (2025). Top Ukrainian Secret Weapons: long range drones, AI turret, fiber optic FPV, ground drones. [online] Available at: <https://www.youtube.com/watch?v=g22pP-fkjgQ> [Accessed 28 Oct. 2025].
7. United24Media (2025). Ukraine War: leopard 2 'meets' the enemy in Pokrovsk. [online] Available at: <https://www.youtube.com/watch?v=yZ9DEKefTFM> [Accessed 28 Oct. 2025].
8. United24Media (2025). The ugly truth behind the "Traditional Values" Russia Sells. [online] Available at: <https://united24media.com/anti-fake/the-ugly-truth-behind-the->

- traditional-values-russia-sells-11690?utm_source=chatgpt.com [Accessed 28 Oct. 2025].
9. Ukrainian Prism (2023). EU's and Ukraine's approaches to digital diplomacy in the geopolitics of technologies. [online] Available at: <http://prismua.org/en/english-eus-and-ukraines-approaches-to-digital-diplomacy-in-the-geopolitics-of-technologies/> [Accessed 28 Oct. 2025].
 10. Ministry of Foreign Affairs of Ukraine (2021). Public Diplomacy: a tool for building Ukraine's resilience to hybrid threats and effective way to promote positive image abroad. [online] Available at: <https://mfa.gov.ua/en/news/public-diplomacy-tool-building-ukraines-resilience-hybrid-threats-and-effective-way-promote-positive-image-abroad> [Accessed 29 Oct. 2025].

Solomiia Melnyk
Studentka Wydziału Prawa
Zachodnioukraińskiego Uniwersytetu Narodowego¹

DZIEDZICZENIE AKTYWÓW CYFROWYCH W PRAWIE PRYWATNYM MIĘDZYNARODOWYM: OBECNE WYZWANIA I PERSPEKTYWY HARMONIZACJI

Zarys problemu. Globalne procesy wynikające z aktywnego wdrażania cyfryzacji w najważniejszych dziedzinach życia publicznego doprowadziły do pojawienia się nowych przedmiotów stosunków prywatnoprawnych - aktywów cyfrowych. Zgodnie z art. 1218 Kodeksu cywilnego Ukrainy (dalej - k.c. Ukrainy), spadek obejmuje wszystkie prawa i obowiązki, które należały do spadkodawcy i nie wygasły w wyniku śmierci [5]. Aktywy cyfrowe są zatem również przedmiotem

¹ Kierownik naukowy: kandydat nauk prawnych, docent, kierownik katedry prawa międzynarodowego i europejskiego Zachodnioukraińskiego Uniwersytetu Narodowego Liudmyla Savanets

dziedziczenia. Chociaż k. c. Ukrainy został zmieniony w 2023 r., aby zapewnić, że aktywy cyfrowe istniejące w środowisku cyfrowym są przedmiotem praw cywilnych, kwestia ich regulacji prawnej nie jest wystarczająco uregulowana w prawie materialnym Ukrainy a większości innych państw. Z wprowadzeniem nowych przedmiotów praw cywilnych podlegających dziedziczeniu pojawiają się luki prawne. W związku z tym zastosowanie metody materialnej jest praktycznie niemożliwe.

Prezentacja głównego materiału. Ukraińskie prawo prywatne międzynarodowe ze względu na globalne zmiany wymaga rekodyfikacji. Jak zauważył A. S. Dovgert: „Światowa (szczególnie europejska) tendencja do unifikacji i harmonizacji prawa prywatnego międzynarodowego jest istotnym czynnikiem współczesnej rekodyfikacji prawa prywatnego międzynarodowego w wielu krajach” [2, s. 124-126]. Ponieważ Ukraina już podejmuje aktywne kroki w kierunku integracji europejskiej, włącznie z harmonizacją swojego ustawodawstwa z prawem UE, oczywiste jest, że ten proces prędzej czy później doprowadzi do rekodyfikacji wielu dziedzin prawa, no i oczywiście ukraińskiego prawa spadkowego. Ponadto A. S. Dovgert wskazał na „istniejące oczekiwanie wpływu modernizacji kodyfikacji prawa prywatnego międzynarodowego na bardziej efektywne współdziałanie systemu prawnego Ukrainy z systemami prawnymi świata, a tym samym przyczyni się do rozwoju międzynarodowych stosunków gospodarczych i innych” [2, s. 129-130].

Pilność rekodyfikacji ukraińskiego prawa prywatnego międzynarodowego wynika z braku regulacji wielu transgranicznych stosunków prawnych, w tym dziedziczenia aktywów cyfrowych. Aktywa te mają charakter transgraniczny, gdyż istnieją wirtualnie i nie podlegają klasycznej zasadzie *lex rei sitae*. Ukraińskie prawo nie definiuje „aktywów cyfrowych”, a jedynie posługuje się pojęciem „aktywów wirtualnych”. Zgodnie z pkt. 1 cz.1 art. 1 Ustawy Ukrainy „O aktywach wirtualnych”, aktywa wirtualne to dobra niematerialne, które są przedmiotem praw cywilnych, mają wartość i są wyrażone przez zbiór danych w formie elektronicznej [3]. Jednak od czasu jej przyjęcia ustawa została «zamrożona» i nie weszła w życie, co wskazuje na

nieformowane ustawodawstwo dla regulacji aktywów wirtualnych w Ukrainie [6, s. 614]. Wśród rodzajów aktywów cyfrowych ustawa ta rozróżnia aktywa zabezpieczone i niezabezpieczone [3].

W krajach *common law* regulowanie takich przedmiotów praw cywilnych rozpoczęło się znacznie wcześniej niż w krajach prawa kontynentalnego. W szczególności, w Stanach Zjednoczonych Ameryki początkowym etapem regulacji prawnej zasobów cyfrowych było przyjęcie w latach 80-tych XX wieku następujących aktów prawnych: «Information Retention Act» oraz «Computer Fraud and Abuse Act». Ustawy te nie zawierają jasnej i zwięzłej definicji „aktywów cyfrowych”, ale nadal obowiązują i stały się podstawą amerykańskiego ustawodawstwa w tym zakresie [1]. W krajach *common law* do aktywów cyfrowych zalicza się kryptowaluty, tokeny zabezpieczające, konta w mediach społecznościowych czy treści cyfrowe. W Polsce są to wszelkie dane o wartości zapisanej cyfrowo – m.in. waluty, tokeny, dokumenty i zasoby online. Technologia blockchain wspiera ich rozwój, zapewniając bezpieczeństwo, przejrzystość i decentralizację [8].

Międzynarodowe akty prawne są również wykorzystywane w regulacjach prawnych dotyczących aktywów cyfrowych, choć nie ma ich zbyt wiele. Na przykład na poziomie UE takie stosunki prawne reguluje Rozporządzenie (UE) 2023/1114 w sprawie korzystania z kryptowalut (MiCA). W ostatnich latach społeczność międzynarodowa aktywnie angażowała się w opracowywanie aktów prawa miękkiego, takich jak UNIDROIT Principles on Digital Assets and Private Law 2023. W szczególności druga zasada („Definicje”) Zasad UNIDROIT dotyczących aktywów cyfrowych i prawa prywatnego stanowi, że aktywa cyfrowe oznaczają zapis elektroniczny, który może podlegać kontroli [10].

W rzeczywistości pierwszym konfliktem interesów w zakresie dziedziczenia aktywów cyfrowych jest to, że prawo materialne różnych państw nie ma jednolitego poglądu na charakter prawny i treść aktywów wirtualnych. Chociaż istnieją pewne ogólne tendencje w definiowaniu pojęcia „aktywów cyfrowych”, nieporozumienia pojawiają się już na etapie rozróżniania rodzajów tych przedmiotów praw cywilnych [6, s. 617]. Kolejnym problemem jest brak odrębnego przepisu kolizyjnego w ustawie Ukrainy „O prawie prywatnym międzynarodowym”

dotyczącego dziedziczenia aktywów cyfrowych jako przedmiotów praw cywilnych. W szczególności art. 71 ustawy reguluje stosunki dziedziczenia nieruchomości i ruchomości, co nie obejmuje aktywów cyfrowych. Pojęcie aktywów cyfrowych jest zawarte w art. 179¹ k.c. Ukrainy, i znaczy to dobro (jako rzecz), które jest tworzone i istnieje wyłącznie w środowisku cyfrowym i ma wartość majątkową [5]. W związku z tym jedyną zasadą, która może zostać zastosowana, jest art. 70 ustawy Ukrainy „O prawie prywatnym międzynarodowym”, która stanowi, że stosunki spadkowe podlegają prawu państwa, w którym spadkodawca miał ostatnie miejsce zamieszkania, chyba że spadkodawca wybrał w testamencie prawo państwa, którego był obywatelem [4]. W rezultacie norma kolizyjna odnosi się do prawa materialnego państwa miejsca zamieszkania (*lex domicilii*) lub prawa państwa obywatelstwa (*lex patriae*).

Nie każde państwo posiada przepisy regulujące dziedziczenie aktywów cyfrowych. W USA większość stanów przyjęła ustawę Revised Uniform Fiduciary Access to Digital Assets Act, która umożliwia spadkobiercom dostęp do kont, e-maili i kryptowalut na podstawie testamentu, jeśli brak innych narzędzi zapewniających taki dostęp [11]. Korzystanie z narzędzi online zwykle odnosi się do kont w mediach społecznościowych. Google oferuje Inactive Account Manager, który pozwala wyznaczyć zaufaną osobę do dostępu po okresie nieaktywności. Facebook ma funkcję Legacy Contact, umożliwiającą zarządzanie kontem po śmierci użytkownika – można dodać post lub zmienić zdjęcie profilowe, ale bez dostępu do wiadomości i usuwania treści [11].

W Polsce, jak również w Ukrainie, kwestie kolizyjnoprawne dotyczące dziedziczenia aktywów cyfrowych nie są wystarczająco uregulowane. Przykładowo, art. 922 polskiego k. c. stanowi, że przedmiotem dziedziczenia są prawa i obowiązki majątkowe zmarłego, ale nie należą do spadku prawa i obowiązki zmarłego ściśle związane z jego osobą, jak również prawa, które z chwilą jego śmierci przechodzą na oznaczone osoby niezależnie od tego, czy są one spadkobiercami [9]. Przepisy są niejasne, więc nie wiadomo, czy aktywa cyfrowe wchodzą do spadku z mocy prawa, więc można je dziedziczyć tylko przez

testament. W Ukrainie ustawa „O aktywach wirtualnych” jeszcze nie obowiązuje i dotyczy tylko transakcji dwustronnych, więc nie obejmuje dziedziczenia. Oznacza to, że dziedziczenie aktywów cyfrowych w Ukrainie nie jest obecnie uregulowane.

Kolejnym problemem w dziedziczeniu aktywów cyfrowych jest ustalenie ich własności, ponieważ nie potwierdza jej żaden dokument, a jedynie dane z rejestrów i platform. Brakuje scentralizowanego rejestru aktywów i ich właścicieli. Trudny jest też dostęp spadkobierców do kont, gdy ograniczają go wcześniej ustalone zasady ochrony danych, co prowadzi do konfliktu między prawem spadkowym a ochroną danych osobowych.

Problemy te wymagają pilnych rozwiązań, gdyż wraz z cyfryzacją rośnie liczba dziedziczonych aktywów cyfrowych, których obecne prawo nie reguluje. Niezbędne są zmiany w prawie materialnym i procesowym, ujednoczenie zasad dziedziczenia transgranicznego oraz stworzenie jednolitego rejestru aktywów cyfrowych. Najlepszym rozwiązaniem byłoby przyjęcie zaleceń typu Zasad UNIDROIT, ponieważ stworzenie jednej skutecznej konwencji w tej dziedzinie, która bezpośrednio regulowałaby obrót aktywami cyfrowymi, nie mówiąc już o ich dziedziczeniu, jest na razie nierealne.

Wywód. Kwestie kolizyjne przy dziedziczeniu aktywów cyfrowych pozostają nierozwiązane z powodu braku jednolitego podejścia do ich charakteru prawnego. W Ukrainie brak regulacji w tym zakresie utrudnia stosowanie prawa spadkowego. Niezbędna jest harmonizacja przepisów, rekodyfikacja prawa prywatnego międzynarodowego, stworzenie rejestru aktywów cyfrowych oraz opracowanie norm kolizyjnych. Najlepszym rozwiązaniem byłoby przyjęcie międzynarodowych aktów „soft law”, które ujednoczyłyby standardy regulacji w tej dziedzinie.

Lista źródeł:

1. Білінський Д. О., Кучерявенко М. П., Смичок Є. М. Цифрові активи як об'єкт правового регулювання: науково-правовий висновок. URL: <https://cifrov-aktivi-yak-obkt-pravovogo-regulyuvannya> (data dostępu: 01.04.2025).

2. Довгерт А. Міжнародне приватне право: зміна концепції. Київ: Алерта, 2024. 256 с.
3. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (data dostępu: 01.04.2025).
4. Про міжнародне приватне право: Закон України від 23 червня 2005 року №2709-IV. URL: <https://zakon.rada.gov.ua/laws/...> (data dostępu: 01.04.2025).
5. Цивільний кодекс України: Закон України від 16.01.2003 року №435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (data dostępu: 01.04.2025).
6. Цукан С. В. Поняття, правова природа та класифікація віртуальних активів. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. Ужгород. 2023. Вип. 80. Ч. 1. С. 613-618. URL: <https://visnyk-juris-uzhnu.co...> (data dostępu: 01.04.2025).
7. Чупрій Д. Ю. Правова природа акаунтів як потенційних об'єктів спадкування. *Актуальні проблеми вітчизняної юриспруденції*. Дніпро. 2023. Вип. 1. С. 54-59. URL: http://www.apnl.dnu.in.ua/1_2023/9.pdf (data dostępu: 01.04.2025).
8. Aktywno cyfrowe. URL: <https://cinkciarz.pl/kryptowalut...> (data dostępu: 01.04.2025).
9. Kodeks cywilny: ustawa z dnia 23 kwietnia 1964 r. Nr. 16 poz. 93. URL: <https://isap.sejm.gov.pl/isap.nsf...> (data dostępu: 01.04.2025).
10. UNIDROIT Digital Assets and Private Law Principle 2(2). URL: <https://www.unidroit.org...> (data dostępu: 01.04.2025).
11. What is RUFADAA? URL: <https://trustandwill.com/learn/what-is-rufada...> (data dostępu: 01.04.2025).

*Марія Павлюх
кандидат наук із соціальних комунікацій
докторантка кафедри політології та публічного управління
Волинського національного університету імені Лесі Українки*

ІНФОРМАЦІЙНА БЕЗПЕКА У ПОЛЬСЬКОМУ МЕДІАПРОСТОРИ: НАРАТИВИ РОСІЙСЬКОЇ ПРОПАГАНДИ (НА ПРИКЛАДІ БЛОГЕРА МЕРЕЖІ «X» МАРТИНА ДЕМІРОВА)

Інформаційна безпека та захист інформації займають важливе місце у міжнародних відносинах, адже сьогодні медіапростір дедалі частіше насичений дезінформацією і фейками, які негативно впливають на міжнародні відносини. Велика кількість дезінформації про російсько-українську війну у польському медіапросторі свідчить про активність російської пропаганди, яка має на меті зіпсувати українсько-польські стосунки, послабити міжнародну допомогу Україні, створити негативні образи Польщі та України на світовій арені. Польща – близький сусід та головний партнер України, тому вивчення дезінформації польського медіапростору про російсько-українську війну має стратегічне значення для Польщі і України, зокрема.

У багатьох споживачів медійного контенту відсутні навички інформаційної безпеки та критичного мислення, які є основою «правильного прочитання і споживання інформації» у соціальних мережах. У польському медійному полі зростає кількість каналів та ЗМІ, які поширюють антиукраїнську риторику і проросійські наративи. Чималу кількість проросійських наративів містять популярні блоги з великим охопленням підписників. Особливою активністю виділяється мережа X, в якій часто можна зустріти антиукраїнську риторику і відверту неприязнь до України з боку відомих польських діячів. Піком поширення негативних фейків, дезінформації про Україну стали президентські вибори у Польщі, які відбувалися на весні 2025 року: польські мережі рясніли антиукраїнськими заголовками.

За дослідженням польського фактчекінгового об'єднання «Демагог» та Інституту моніторингу ЗМІ за 2024 рік виявлено 327 тис. антиукраїнських записів у польськомовному інтернеті. З кожним роком їхня чисельність зростає. У листопаді 2024 року таких записів було 36 тисяч, у грудні – 33 тисячі. Експерти Польського інституту міжнародних досліджень зазначають, що один із провідних напрямів проросійської дезінформації – спекуляція на темах: Волинської трагедії, образі Степана Бандери та УПА [3].

Минулого року в польському інтернеті з'явилося понад 300 тис. коментарів з нападами на українців, розпалюванням міжнаціональної ворожнечі, що на 13% більше, ніж 2023 року. Антиукраїнський контент охопив понад 75 мільйонів потенційних контактів; саме стільки разів користувачі могли зустріти неправдиві та ненависні повідомлення про українців [3].

Дослідники Варшавського університету зазначають, що масштабність постів, орієнтованих на українців, виливається в антиукраїнські настрої поляків. Це підтвердило нещодавнє опитування CBOS, яке продемонструвало, що 38% поляків сказали, що не люблять українців, тоді як лише 30% заявили, що симпатизують українцям. Відсоток людей, які сказали, що їм подобаються українці знизився на 10 пунктів, ніж рік тому, і на 21 пункт, ніж у 2023 році [3].

Польські медіа та окремі блогери на медійних майданчиках збирають чисельну аудиторію, поширюючи російську пропаганду. Одним із російських симпатиків є Мартін Деміров (Martin Demirow), відео якого набирають до 500 тис. переглядів. Блогер має 20,1 тис. підписників та опублікував 67,5 тис. дописів від жовтня 2022 року. У шапці профілю подано коротке резюме про самого блогера, який «шукає, перекладає чи коментує статті (польські та іноземні), що піддаються цензурі». Частота публікацій досить висока – кілька відео та 3–4 пости протягом доби. Характер публікацій і відео – відверто антиукраїнський та проросійський [1].

Видання «Worldcrunch Today» повідомляє про цього блогера такі відомості: «Мартін Деміров подає себе «словаком, який цікавиться Польщею». Він прирівнює українців і прихильників Степана

Бандери (керівника УПА, війська якого знищили десятки тисяч поляків після Другої світової війни) до нацистів. Його попередній акаунт заблокували, але Деміров повернувся з новим, де у нього майже 2 мільйони підписників» [1].

Наративи, які поширює Мартін Деміров

У всіх своїх постах, коментарях та публікаціях Мартін Деміров поширює російсько-радянські наративи, що розхитують політичну ситуацію та інформаційну безпеку в Польщі, загострюють польсько-українські відносини, формують симпатію до російських окупантів. Популярним наративом російської пропаганди, яку поширює сторінка Мартіна є твердження про те, що *Крим – це російська територія*, а кримчани хочуть бути в Росії [2; 2.04.2025]. Іншим важливим наративом, що поширює сторінка Мартіна є ототожнення влади України із тоталітарним режимом: *«бандерівський режим», «нацистський режим», а президента України Зеленського ототожнено із нацистами, зокрема із Гітлером* [2; 5.04.2025].

Мартін Деміров поширив статтю Ростислава Іщенка *«Укрогенез та укроцид»* (пост від 24 квітня 2025) [2], в якій знаходимо усі антиукраїнські наративи російської пропаганди. До прикладу, *українці є росіянами* («Як можна говорити про створення окремої нації, якщо 90% населення України мають найближчих родичів у Росії: матір, батька, сина, дочку, брата. Чи належать вони до різних народів? Як можна говорити про націю, якщо її представники стверджують, що мають «давню мову», але ні самі її не знають, ні їхні предки ніколи нею не розмовляли, а тепер вивчають її на зло росіянам, з якими вони воюють, але розмовляють однією мовою та є родичами?») [2].

Особливо важливими є такі наративи: *українська мова – національна* («Гаразд, можливо, два брати усвідомили, що вони окремі нації, батько і син, мати і дочка також. Можливо, зараз вони вивчать «національну» мову, і їхні онуки визнають її рідною»); *Україна не має власних територій, Львів – то польське місто* («Але нація все ж повинна мати свою національну територію та економіку, без цього неможливо створити національну державу. І у них є чужа

територія: Львів – польське місто, а Київ, Харків, Одеса, Херсон, Дніпропетровськ, Запоріжжя – російські»), тому що саме цими нарративами люблять спекулювати російські пропагандисти [2].

Наратив: *Україна – злодійська, корумпована держава* («Економіки взагалі немає – те, що вони самі усядкуювали, було повністю вкрадено, а те, що не змогли вкрасти та продати – вони знищили. Вони також повністю знищили державу, яку усядкуювали, а не створили самі») має на меті принизити державу, яка через війну переживає важку кризу [2].

Наратив: *Україна – нацистська держава* («Де житиме ця «нація», що вона їстиме та питиме? Зрештою, нація має мету – національну ідею. Хтось хоче літати до зірок, хтось хоче їсти гамбургер щодня, хтось буде тисячолітній Рейх») має на меті створення негативного образу нашої держави серед європейців, що різко засуджують нацистські теорії [2].

Наративи: *нема української національної ідеї, українці ніколи не стануть європейцями* («Національна ідея «великих українців» полягає в розчиненні в європейському морі, а не в тому, щоб посправжньому увійти до «сім'ї народів», як це зробили самі поляки, румуни, болгари, чехи та угорці, хоча й за величезні гроші для себе») мають на меті налаштувати європейських партнерів проти України. Подібним наративом є *українці прагнуть в ЄС задля пільг* («Ні, їхня мета – асимілюватися, стати ким завгодно (хто б їм не надав громадянство) – португальцем, французом, німцем, турком чи арабом, або навіть негром, аби лише приєднатися до європейців – отримувачів пільг. Але одержувачі соціальної допомоги не є нацією – вони бомжі, маргіналізовані, але не нація»; «Росіяни реєструються як росіяни, а потім як українці, щоб далі стати одержувачами європейської соціальної допомоги») [2].

Наратив: *українці не мають власної території* («Більшість народилися росіянами, але в якийсь момент вони перестали ними бути... Якщо вони є нацією, то місце, де вони народилися та живуть, це їхня національна територія, захист якої є їхнім священним обов'язком, але якщо вони не є нацією, то вони зрадники-втікачі через українізм від російської нації до європейських благ і не мають

жодних прав на російську національну територію») має на меті закріпити думку про те, що вся територія України – це російські території [2].

Наратив: *українські біженці – зрадники* («І взагалі, вважати біженців з нації окремою нацією – це свого роду ганьба. У цьому сенсі переселенці – це нація. Вони теж втекли, теж на Захід, вони теж хочуть долучитися до родини європейських народів, тільки вони справедливо вважають, що немає потреби вчити українську, достатньо просто відмовитися від російської назви») має на меті сформувати ненависть до переселенців.

Автор перепостив відео нічної ракетної атаки на Київ 24 квітня 2025 з підписом: «знищення великої військової бази бандерівців-нацистів» (пост від 24 квітня). Цей пост містить кілька проросійських наративів: *бандерівці-нацисти воюють, росіяни знищують тільки військові бази, росіяни не воюють проти мирного населення* (внаслідок атаки загинуло понад 12-ти мирних осіб та понад ста травмовані) [2].

Великого значення мають стереотипи та спекулювання на темі Волинської трагедії. Зокрема, Мартін Деміров пише, що українці не хочуть допустити поляків до ексгумації тіл та забороняють будь-яке перепоховання вбитих поляків загонами УПА (1942 – 1943 рр.). На думку блогера, *українці ніколи не будуть в ЄС*, тому що прагнуть тільки соціальних виплат, а на свободи, етику чи мораль їм наплювати. Загальний образ України на сторінці Демірова подано через ілюстрацію (пост від 23 квітня 2025) [2] брудної свині із синьо-жовтим прапором, яка голосно кричить.

Список використаних джерел та літератури

1. Павлюх М. Проросійська пропаганда сторінки Мартіна Демірова в польському інфопросторі: наративи та небезпека дезінформації. 29 квітня 2025. *Україно-польська медіаплатформа*. https://upmp.news/post_blog/prorosijska-propaganda-storinky-martina-demirova-v-polskomu-infoprostoru-naratyvy-ta-nebezpeka-dezinformatsiy/
2. Demirov M. <https://x.com/MartinDemirov>

3. Nodzinska P. Tracking The Flood Of Anti-Ukraine Propaganda Across The Border In Poland. *Worldcrunch*. URL: https://worldcrunch.com/focus/russia-ukraine-war/anti-ukraine-in-poland-far-right/?fbclid=IwY2xjawN1qqlleHRuA2FlbQIxMABicmlkETFIZFc1Z1RUT2U2b0dlbDlXAR57HI_50yajcAdMMVTuRpYioWRoG9_B41zRR-gubW-ypii8_D36A70fjY9JQ_aem_aVSxvL8HJH9gr3IMsku-hQ

Іван Панкевич
доктор юридичних наук, професор
Зеленогурський університет,
Маркіян Панкевич
студент
Ягеллонський університет у Кракові

ДІДЖИТАЛІЗАЦІЯ ВИБОРІВ: ЄВРОПЕЙСЬКИЙ ДОСВІД

Інформаційні технології пронизують все більше сфер нашого життя. При цьому йдеться й про ті сфери, щодо яких ще нещодавно, видавалось би, неможливим є впровадження діджиталізації. Наприклад, Албанія стала першою державою у світі, де призначено віртуальну міністерку, якою керує штучний інтелект, а її прем'єр-міністр Еді Рама заявив, що завдяки цьому державні тендери будуть на 100 % некорупційними й всі державні кошти, що проходять тендерну процедуру, будуть на 100 % прозорими [1]. Україна також не стоїть осторонь процесів діджиталізації, зокрема з 2019 року в уряді з'явилася посада віце-прем'єр-міністра - міністра цифрової трансформації. Доволі активно обговорюється й проблема ширшого запровадження інформаційних технологій у виборчий процес. Йдеться про те, що, з огляду на триваючу вже майже чотири роки російсько-українську війну, наслідком якої став виїзд значної частини українських громадян за кордон, на порядку денному постало питання використання електронного голосування, як засобу підвищення участі громадян у виборах. Щоправда, за твердженням

віце-прем'єр-міністра – міністра цифрової трансформації України Михайла Федорова, електронне голосування через застосунок «Дія» наразі не розглядається. «Ми не працюємо над цим. Для цього необхідне рішення ЦВК, зміни в законодавстві – і всі про це дізнаються. Але зважаючи на кібервійну, це не є пріоритетом ані на цей рік, ані на наступний» [2]. Додатковим аргументом для відтермінування впровадження такого голосування є, на наш погляд, й те, що досягнення високого рівня цифрової грамотності більшістю українських громадян залишає бажати кращого. Крім того, Україна на сьогодні є технічно не готовою до проведення масштабного електронного голосування. Це підтвердило, наприклад, голосування на пісенному конкурсі Євробачення у 2024 році, яке завершилося технічною проблемою в мобільному додатку «Дія» [3]. Іншим підтвердженням такого висновку стали наслідки здійсненої росіянами у грудні 2023 року хакерської атаки на сервери найбільшого оператора мобільного зв'язку в Україні, яким є «Київстар», внаслідок чого протягом майже трьох діб не працював мобільний зв'язок та інтернет [4]. Не менш важливою у контексті проведення виборів в Україні є й значна недовіра громадськості до онлайн-голосування.

Якщо вести мову про європейський досвід успішної діджиталізації надання послуг загалом та застосування електронного голосування зокрема, то тут найкращим прикладом слугуватиме Естонія. Проте ця держава запровадила електронне голосування лише після багатьох років використання онлайн-сервісів соціального страхування, податків та реєстрації майна, тобто після багаторічної «апробації» діджиталізації у наданні держаних послуг. Щодо електронного голосування, то воно було запроваджено у виборчий процес в Естонії ще у 2005 році. Двадцять років тому лише 9 287 виборців (тобто лише 2 %) проголосували онлайн, а на парламентських виборах навесні 2023 року в Естонії вперше в історії онлайн вже проголосували понад 50 % виборців, які взяли в них участь [5]. Однак необхідно пам'ятати, що кількість виборців в Естонії є значно меншою, ніж в Україні, і вона є найбільш діджиталізованою європейською державою. У той же час,

незважаючи на усі застосовувані «запобіжники» від виборчих фальсифікацій, за результатами останніх парламентських виборів, що відбулися 6 березня 2023 року, Консервативна народна партія Естонії (EKRE), яка програла ці вибори, звернулася до Держсуду з проханням визнати результати електронного голосування на виборах до Рійгікогу недійсними. Партія вважає процес визначення результатів виборів неправомірним, звертаючи увагу на те, що під час е-голосування виникла низка аномалій і технічних проблем, які ставлять під сумнів надійність інфраструктури, використовуваної під час електронного голосування [6].

Серед держав – членів Європейського Союзу є також й ті, які набагато обережніше ставляться до питання діджиталізації, у тому числі й до запровадження електронного голосування. До їх числа належить, зокрема, Німеччина, яка на сьогодні відмовилася від електронного голосування. Подібна ситуація має місце у Франції, яка свого часу запровадила механізм електронного голосування, але пізніше відмовилася від нього через посилення кібератак.

Аналізуючи можливість застосування в Україні та інших європейських державах електронного голосування вважаємо, що впровадження сучасних інформаційних технологій у виборчий процес, безсумнівно, розширить можливості голосування. Проте активне використання електронного голосування стане можливим лише після запровадження відповідних гарантій від несанкціонованого доступу до баз даних. На сьогодні ніхто в будь-якій державі не може гарантувати, що виборчий процес буде ефективно захищеним від кібератак. Нещодавнім підтвердженням цього висновку стала масштабна атака кіберфахівців Головного управління розвідки Міністерства оборони України на ресурси російської ЦВК. Метою кібератаки стало перешкоджання електронному голосуванню на російських виборах, які окупаційна влада проводить у тому числі на тимчасово окупованих територіях України. Внаслідок атаки деякий час була паралізована робота цифрових сервісів, на яких проводилося онлайн-голосування і багато росіян не змогли проголосувати на виборах міських голів та губернаторів в регіонах рф [7].

Список джерел і літератури:

1. Албанія стала першою країною у світі, де призначили ШІ-міністра. Газета «Високий Замок», 12.09.2025 р.
2. Цифровізація залишається важливим напрямком, але вибори наразі не є пріоритетом. URL: <https://zn.ua/ukr/POLITICS/vivoriv-cherez-diju-ne-bude-tse-ne-na-porjadku-dennomu-fedorov.html>.
3. У застосунку «Дія» стався збій через голосування в нацвдборі на Євробачення-2024. URL: <https://forbes.ua/news/u-zastosunku-diya-stavsya-zbiy-cherez-golosuvannya-v-natsvidbori-na-evrobachennya-2024-03022024-18976>.
4. СБУ ідентифікувала хакерів російського ГРУ, які атакували “Київстар”: матеріали справи передадуть в Гаагу. URL: <https://suspilne.media/720596-sbu-identifikuvala-hakeriv-rosijskogo-gru-aki-atakuvali-kiivstar-peredast-materiali-spravi-v-gaagu/>.
5. Вибори в Естонії: вперше в історії понад 50 % виборців голосували онлайн. URL: <https://www.eurointegration.com.ua/news/2023/03/6/7157420/>
6. В Естонії консерватори вимагають у суді анулювати результати е-голосування. URL: <https://www.eurointegration.com.ua/news/2023/03/9/7157656/>.
7. Кіберпомста від ГУР в дії: ресурси російської ЦВК паралізувала масштабна атака. URL: <https://www.obozrevatel.com/ukr/novosti-obshchestvo/kiberpomsta-vid-gur-v-dii-resursi-rosijskoi-tsvk-paralizuvala-masshtabna-ataka.html>.

*Костянтин Поліщук
кандидат політичних наук, доцент
Львівський національний університет
імені Івана Франка*

ПОНЯТТЯ ТА ІНСТРУМЕНТИ АНАЛІЗУ Й ВИМІРЮВАННЯ ЕФЕКТИВНОСТІ ЦИФРОВОГО ДИПЛОМАТИЧНОГО ВПЛИВУ

Переважаюча більшість науковців та дослідників цифрової дипломатії визнають складність вимірювання м'якої сили, дипломатії загалом та (цифрового) дипломатичного впливу зокрема, оцінки ефективності якого надто зосереджуються на результатах діяльності (так звані Ключові Показники Ефективності (англ. KPI – Key Performance Indicators)), а не на доказах фактичного впливу суб'єктів дипломатичної діяльності. У фаховій літературі рекомендується використовувати індивідуальні, прив'язані до відповідного контексту оцінки, щоб враховувати специфіку відповідних політичних, соціальних, економічних та інших обставин, дипломатичної роботи та зовнішньополітичних пріоритетів відповідної держави. Грунтуючись на теорії змін, вони спираються на оцінку проміжних цілей як «замінника» начебто невимірюваного довгострокового впливу та на аналіз наслідків, а не на визначення причинно-наслідкових зв'язків, що, власне, спричинили відповідний результат.

Якщо говорити про м'яку силу як про дипломатичну здатність держави домагатися своїх цілей за рахунок привабливості власної культури, суспільно-політичних цінностей тощо, то вона може вимірюватися за допомогою індексів, які відображають активи, ресурси м'якої сили, але не конверсію цих активів у реальний вплив. Так, міжнародна консалтингова ПР-агенція «Brand Finance» щорічно складає комплексний багатофакторний індекс м'якої сили «Global Soft Power Index», у рамках якого на основі 55 (суб)індикаторів рейтинуються 193 країн світу. Серед досліджуваних показників зокрема впливовість, впізнаваність та репутація країн, а також їхня «успішність» у таких сферах як бізнес

і торгівля, медіа і комунікації, культура та спадщина, освіта і наука, люди і цінності, сталий розвиток, міжнародні відносини та урядування¹. Утім даний індекс вимірює скоріше сприйняття національних брендів, що охоплює думку 100 тисяч респондентів. Існує безліч способів оцінки внеску відповідних заходів у м'яку силу, але вони не включають аналіз показників як таких. Натомість вони схиляються до партисипативних моделей оцінки, наприклад, до моделі культурної цінності (теорія культурних вимірів Хофстеде), яка використовується для розуміння та ідентифікації того, як різні групи сприймають і оцінюють часто складні та різноманітні цінності.

Якщо говорити про традиційну дипломатію, то оцінка її впливу передбачає побудову теорії змін, а потім визначення умов, які необхідно виконати для того, щоб зміни відбулися. В окремих випадках використовуються такі показники результативності, як участь у засіданнях або включення питань до їхнього порядку денного. Виокремлюючи публічну дипломатію, то вона часто оцінюється за її результатами, такими як кількість людей, які відвідали захід, або кількість публікацій у пресі, що висвітлюють захід. Іноді для оцінки впливу на учасників використовуються опитування громадської думки. Тоді як цифрова дипломатія відкриває можливість для оцінки таких показників, як кількість уподобань, рівень залученості аудиторії, тональність повідомлень або зміст коментарів до публікацій у соціальних мережах.

Зокрема, Стратегія публічної дипломатії МЗС України 2021-2025² визначає систему моніторингу та оцінювання виконання стратегічних цілей української публічної (цифрової) дипломатії на основі цілої низки кількісних індикаторів, зокрема: кількість ключових світових подій, де представлена Україна; показники охоплення подій; кількість проектів і кампаній на міжнародних цифрових платформах; показники охоплення проектів і кампаній;

¹ Глобальний індекс м'якої сили. URL: <https://brandirectory.com/softpower>

² Стратегія публічної дипломатії МЗС України 2021-2025. URL: <https://mfa.gov.ua/pro-ministerstvo/strategiyi-mzs>

кількість згадок про Україну в міжнародних ЗМІ з урахуванням частки позитивних; кількість іміджевих заходів; показники охоплення заходів; відсоток респондентів, які знають про Україну; зміна прямих асоціацій з Україною. Інструментами вимірювання цих показників вказані дослідження громадської думки, медіа-моніторинг, інструменти онлайн-аналітики, звітність, статистичні дані.

На сьогодні у сфері дослідження публічної (цифрової) дипломатії склалися чотири підходи до вимірювання її впливу: на основі моделей процесу, результатів (output/outcomes), сприйняття і мережовості¹. Вплив на іноземну громадськість вимірюється за допомогою таких методів, як кількість сантиметрів/знаків/рядків у друкованих виданнях, ефірний час, опитування, фокус-групи, глибинні інтерв'ю, аналіз медіа-контенту, підрахунок кількості учасників заходів, спостереження за учасниками та відстеження в Інтернеті. Також можна виміряти діяльність персоналу, залученого до кампаній. Цей підхід вимірює діяльність кампанії, а не її результати, і називається «оцінкою процесу» або «самопредставленням».

Модель результатів спочатку встановлює досяжні та вимірювані цілі, оцінює діяльність та процеси, пов'язані з кампанією (виділені ресурси, отримані результати, що учасники дізналися після участі в кампанії). Потім результати аналізуються з метою виявлення будь-яких помітних змін у політичному середовищі або поведінці учасників, а потім переоцінюються, щоб перевірити, чи були ресурси розподілені належним чином.

Модель сприйняття передбачає опитування громадської думки, анкетування до і після, фокус-групи та якісні інтерв'ю, які збирають дані про ставлення та думки іноземних громадян, щоб зрозуміти, чи змінюють політика або кампанії спосіб мислення людей. Метою є не оцінка конкретних соціальних змін або здатності організації

¹ Hicks, J. (2021). Defining and Measuring Diplomatic Influence. K4D Helpdesk Report 950. Brighton, UK: Institute of Development Studies. URL: <https://doi.org/10.19088/K4D.2021.032>

досягати результатів, а скоріше оцінка знань та цінностей, які, як вважається, мотивують зміни. Ця модель дає дані, які можуть допомогти виявити цінності, норми та стереотипи, що, як вважається, мотивують або перешкоджають досягненню бажаних результатів.

Стратегії публічної (цифрової) дипломатії в рамках моделей мережовості спрямовані на виявлення «ключових впливових осіб» — інфлюенсерів, які з огляду на статус лідера громадської думки у відповідній сфері, виступають «хабами» з доступом до великої кількості «вузлів» у мережі. Мережева модель оцінки зосереджується на цих відносинах, або через сприйняття (опитування), оцінку зв'язків та обмінів, або через ступінь управління відносинами.

Оскільки цифрова дипломатія щоразу більше та активніше освоює алгоритмічні моделі збору, систематизації, аналізу та стратегічного поширення (великих) даних, аналіз яких дає можливість проводити моніторинг і контролювати зміни в політичних структурах і громадській думці, усі ці підходи є доволі прикладними у контексті вимірювання ефективності саме цифрової дипломатії. Величезна кількість великих даних (*big data*), отриманих через соціальні медіа, надає унікальну можливість використовувати метод аналізу соціальних мереж для фіксації «мереж коментарів» та моделей взаємодії серед громадськості на сторінках у соціальних медіа, застосовувати моделювання тем для виявлення громадської думки та настроїв (метод тематичного моделювання), послуговуватися аналізом тональності текстів для виявлення контекстуальної полярності контенту, визначенні його позитивності, негативності чи нейтральності. З огляду на ефективність та популярність сучасних технологій, моделей та алгоритмів аналізу та використання даних у сфері бізнесу світова дипломатія усе більше та активніше бере на озброєння та запозичує такі *data driven* моделі, що включають збирання інформації від аудиторій, її накопичення, аналіз, прийняття рішень на основі результатів аналізу, взаємодія з аудиторією, очікування реакції, мобілізації дій після чого йде повторне збирання інформації.

Окремим перспективним показником ефективності цифрової дипломатії є показник центральності або близькості до центру, який можна використовувати для виявлення найвпливовішої особи (осіб) у соціальній мережі, себто ключових вузлів та взаємозв'язків між ними. Ці мережі часто описують у вигляді соціальних мережевих діаграм, де вузли подано у вигляді точок, а зв'язки – у вигляді ліній, які у підсумку дозволяють простежити значущість/впливовість тих чи інших вузлів чи груп вузлів у відповідній мережі, проаналізувати індивідуальні та групові структури взаємозв'язків, використання засобів масової інформації та комунікації у поширенні відповідних наративів чи контрнативів, розпізнати стратегії ключових акторів у відповідній мережі. Інші, більш глибокі і диференційовані різновиди та модифікації показника центральності (за посередництвом, за близькістю, за впливовістю, альфа-центральності і центральності за степенем) дозволяють ще глибше проаналізувати ефективність цифрового дипломатичного впливу та розробляти практичні рекомендаційні алгоритми для переслідування і досягнення, зокрема, зовнішньополітичних цілей держави.

Комплексним підходом та свого роду прототипною моделлю для визначення цифрового дипломатичного впливу можна вважати Індекс цифрової дипломатії від французької консалтингової компанії «Reputation Squad».¹ Дані, використані для складання індексу ґрунтуються на присутності та активності дипломатичних представників щоправда лиш 20 країн (G20) у соціальній мережі «X», зокрема через особисті цифрові профілі лідерів країн, міністерств закордонних справ, міністрів закордонних справ, посольств країн в інших країнах G20. Він розраховується на основі зваженої комбінації дев'яти наступних показників: охоплення дипломатичної мережі (кількість органічних регулярних підписників), гучність (середня кількість повідомлень в день), мовна диверсифікація, глобальна видимість країни (кількість згадок), відповідність формату (співвідношення тексту, візуалу, відео),

¹ Індекс цифрової дипломатії. URL: <https://digital-diplomacy-index.com/index/>

ефективність повідомлень (кількість уподобань, репостів, залученість), чинник лідера держави (особистісний фактор), дипломатична вага (кількість згадок про країну іншими), динаміка моменту (кількість нових підписників за останні 30 днів), і, власне, згадана вище дипломатична центральність як один з ключових індикаторів цифрового дипломатичного впливу.

*Світлана Прийма
кандидат економічних наук, доцент
Львівський національний університет
імені Івана Франка*

УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Цифрові технології стрімко інтегруються не лише в наше повсякденне життя, а й у бізнес-процеси, виробничі системи, управління підприємствами. Цифровізація відкриває нові можливості для компаній, але водночас створює комплекс ризиків, які можуть негативно вплинути на фінансову стабільність, репутацію та діяльність підприємства. До таких ризиків відносять: кіберзагрози та порушення безпеки даних; операційні збої (наприклад, відмови або некоректна робота інформаційних систем); відтік клієнтів, викликаний складнощами адаптації або незадоволеністю новими цифровими рішеннями; фінансові втрати та репутаційні ризики, що можуть стати наслідком вищезазначених проблем [3, 4].

Потрібно враховувати, що цифрова трансформація відбувається в умовах політико-економічної нестабільності та воєнних дій, що зумовлює значне зростання ризиків та формування нових невизначеностей у сфері господарської діяльності. Такі умови вимагають своєчасного та адекватного реагування на загрози. Тому розробка ефективної системи управління ризиками є необхідною умовою успішної реалізації цифрових проєктів.

Управління ризиками передбачає системний процес: від ідентифікації та оцінки ризиків до розробки стратегій реагування і постійного моніторингу [2, 3]. Використання інструментів, таких як матриця ризиків, SWOT-аналіз, сценарне планування та страхування ризиків, дозволяє підприємствам мінімізувати негативні наслідки та забезпечити стійкість у цифровій економіці [5, 6].

З усіх перерахованих інструментів, особливу практичну цінність у контексті візуалізації та значущості цифрових загроз має матриця ризиків. Цей інструмент допомагає визначити пріоритетність ризиків на основі ймовірності їх виникнення та серйозності наслідків і служить основою для розробки дій, що можуть запобігти ризикам або мінімізувати наслідки [1]. Матриця ризиків дає змогу менеджерам ідентифікувати ризики, виділити ті, що мають найбільший вплив, спростити вибір стратегій реагування на них. Застосовуючи матрицю ризиків, компанії можуть краще фокусуватися на найважливіших загрозах і швидко розробляти план управління ризиками.

Варто підкреслити, що матриця ризиків це гнучкий інструмент. Її структура та зміст прямо залежать від специфіки галузі, масштабу підприємства та типу цифрових загроз, з якими воно стикається.

Пропонується побудувати матрицю ризиків для антикризового управління діяльністю підприємства в умовах цифрової трансформації розміром 5×5, де ймовірність виникнення ризику візьмемо як: дуже низька, низька, середня, висока, дуже висока. Рівень наслідків: незначні, малі, суттєві, серйозні, катастрофічні. Стратегії управління ризиками, які можна обрати залежно від комбінації параметрів: 1 – прийняття ризику (голуба область); 2 – створення резервів (бежева область), 3 – страхування або розподіл ризику (рожева область); 4 – уникнення ризику (червона область) (рис.1).

Кіберзагрози, що мають високу ймовірність настання та потенційно серйозні наслідки, автоматично потрапляють у "червону область" і стають пріоритетом для розробки заходів захисту. Це дозволяє підприємству своєчасно концентруватись на

найбільших загрозах та розробляти ефективні стратегії реагування, інтегрувати їх у загальну систему антикризового управління.

Ймовірність	Дуже низька	1	1	2	2	3	<table border="1"> <tbody> <tr> <td>1: Прийняття ризику</td> </tr> <tr> <td>2: Резерви</td> </tr> <tr> <td>3: Страхування</td> </tr> <tr> <td>4: Уникнення</td> </tr> </tbody> </table>	1: Прийняття ризику	2: Резерви	3: Страхування	4: Уникнення
	1: Прийняття ризику										
	2: Резерви										
	3: Страхування										
	4: Уникнення										
Низька	1	2	2	3	3						
Середня	2	2	3	3	4						
Висока	2	3	3	4	4						
Дуже висока	3	3	4	4	4						
		Незначні	Малі	Суттєві	Серйозні	Катастрофічні					
		Наслідки									

Рис. 1. Матриця ризиків для антикризового управління діяльністю підприємства в умовах цифрової трансформації

Інтерпретація ризиків для цифрової трансформації підприємства згідно запропонованої матриці ризиків може бути представлена наступним чином:

- кіберзагрози та порушення безпеки даних → Висока ймовірність + Серйозні наслідки → Страхування / розподіл ризику;
- операційні збої (збій роботи інформаційних систем) → Середня ймовірність + Суттєві наслідки → Створення резервів;
- відтік клієнтів → Висока ймовірність + Великі наслідки → Уникнення ризику (зміна стратегії);
- фінансові втрати → Дуже висока ймовірність + Катастрофічні наслідки → Уникнення ризику;
- репутаційні ризики → Середня ймовірність + Серйозні наслідки → Страхування.

Ситуацію можна деталізувати, використавши шкалу оцінювання в матриці ризиків. Наприклад, як у таблиці 1.

Таблиця дає числові діапазони для ймовірності (%) і наслідків (у млн грн), а також пояснює, яку стратегію обрати залежно від комбінації параметрів. Тобто:

- якщо ризик має ймовірність 70% і збитки 6 млн грн, то він потрапляє в клітинку Висока ймовірність + Серйозні наслідки → код 4 → Уникнення ризику;
- якщо ризик 10% і збитки 0,5 млн грн, то це Дуже низька ймовірність + Малі наслідки → код 1 → Прийняття ризику.

Таблиця 1

Шкала оцінки ризиків

Ймовірність виникнення ризику	Рівень збитків	Рекомендована стратегія
Дуже низька (0–10%)	Незначні (до 0,5 млн грн)	Прийняття ризику
Низька (11–30%)	Малі (0,5–2 млн грн)	Створення резервів
Середня (31–60%)	Суттєві (2–5 млн грн)	Страховання або розподіл ризику
Висока (61–85%)	Серйозні (5–10 млн грн)	Страховання або уникнення ризику
Дуже висока (86–100%)	Катастрофічні (понад 10 млн грн)	Уникнення ризику

Отже, побудова матриці ризиків у контексті цифровізації підприємств є не формальністю, а ключовим інструментом ефективного управління. Насамперед, вона забезпечує систематизацію ризиків, що виникають під час трансформаційних процесів та дає змогу чітко класифікувати всі потенційні загрози. Такий підхід усуває хаотичність і забезпечує структуровану основу для ефективного управління безпекою бізнесу. Завдяки візуалізації ризиків на єдиній площині, керівництво може швидко зорієнтуватись які загрози потребують негайного реагування. Зрештою, матриця ризиків є потужним засобом для прийняття управлінських рішень, комунікації з керівництвом, партнерами, інвесторами.

Аналогічну матрицю можна використовувати для оцінки ризиків у інноваційних проєктах [4], для оцінки ризиків інвестицій, кредитних операцій, для прогнозування ризиків при виході на нові ринки, тощо.

Список використаних джерел і літератури:

1. Вжосек Д. Матриця ризиків: Ключовий інструмент в управлінні проектними ризиками URL: <https://surl.lu/iaicsoo>
2. Гудзь О. Є., Захаржевська А. А. Управління ризиками підприємств в умовах цифровізації: навчальний посібник. – Кропивницький : Видавець Лисенко В. Ф., 2023. – 176 с. URL: https://duikt.edu.ua/uploads/l_2322_63313494.pdf
3. Десятинюк О. М., Птащенко О. В. Управління ризиками в цифровій економіці: фінансова безпека та трансформаційні зміни. *European scientific journal of Economic and Financial innovation* №2(14) 2024. С. 238-245 URL: <https://journal.eae.com.ua/index.php/journal/article/view/338>
4. Зибарева О. В. Управління ризиками бізнес-проектів в умовах цифровізації. Електронний науково-практичний журнал «Проблеми сучасних трансформацій. Серія: економіка та управління». Номер 10. 2023. URL: <https://reicst.com.ua/pmt/article/view/2023-10-04-09>
5. Процес управління ризиками: 5 основних кроків URL: <https://surl.li/dsdroo>
6. Традиційне управління ризиками VS. Управління ризиками підприємства URL: <https://surl.li/pzkmhl>

*Agnieszka Sawicz
Dr hab., prof. UAM,
Uniwersytet im. A. Mickiewicza w Poznaniu*

ZARZĄDZANIE STRACHEM I ZARZĄDZANIE PAMIĘCIĄ JAKO NARZĘDZIA WOJNY HYBRYDOWEJ

Zarządzanie strachem pozwala kontrolować grupy ludzi za pomocą stosunkowo prostych, a jednocześnie skutecznych narzędzi. Wywoływanie, a następnie podtrzymywanie poczucia zagrożenia, jeszcze nigdy nie było tak łatwe, jak dziś, w dobie Internetu. Nauczyliśmy się żyć z COVID-19, ale wciąż wskazujemy nowe

zagrożenia, w tym związane z migrantami. To ich, według CBOS, najbardziej boją się dziś młodzi Polacy, choć w 2024 roku spośród podejrzanych o popełnienie przestępstwa w Polsce obcokrajowcy stanowili 5%, a część z nich mogła zostać oczyszczona z zarzutów¹. Jednak dominującym lękiem, jakiego doświadcza 55% ogółu obywateli, jest strach przed wojną, potęgowany m.in. przez naruszenia polskiej przestrzeni powietrznej przez rosyjskie drony. Obecnie 63% respondentów uważa, że Polska nie jest w pełni bezpiecznym krajem. Co znamienne mniej, bo 47% udzieliło takiej odpowiedzi w 2014 roku, po rozpoczęciu przez Rosję okupacji Krymu². Najwyraźniej wówczas pewną rolę w postrzeganiu potencjalnego zagrożenia mogły odegrać tak odległość od Polski, jak i wiara w zapewnienia Moskwy, że to mieszkańcy półwyspu zadecydowali o zmianie granic.

Dziś, bojąc się bezpośredniego zagrożenia chcemy wierzyć, że dysponujemy silną armią, która będzie mogła nas obronić – według IBRIŚ aż 93% Polaków ma zaufanie do Wojska Polskiego³, o którego finansowaniu, modernizacji technicznej i rozbudowie regularnie informują rządzący, a w ślad za nimi media. Co interesujące, ufając polskim żołnierzom mamy jednocześnie stosunkowo niewielkie przekonanie, że NATO udzieliłoby Polsce pomocy w obronie granic. Według CBOS sądzi tak jedynie 68% pytanych. Aż 24% obywateli nie wierzy sojusznikom⁴, podczas gdy w marcu 2022 roku, kiedy

¹ K. Fejfer, *Czego boją się dziś młodzi Polacy? Trzy główne "strachy"*, <https://www.money.pl/gospodarka/czego-boja-sie-dzis-mlodzi-polacy-trzy-glowne-strachy-7190227452676704a.html>; *Jaki procent podejrzanych o popełnienie przestępstwa to obcokrajowcy? Szef MSWiA podaje dane*, <https://www.pap.pl/aktualnosci/jaki-procent-podejrzanych-o-popełnienie-przestępstwa-obcokrajowcy-szef-mswia-podaje>

² F. Madejski, *Tylu Polaków widzi zagrożenie dla niepodległości kraju. Rosnące obawy*, <https://businessinsider.com.pl/wiadomosci/63-proc-polakow-widzi-zagrozenie-kraju-sondaz-pokazuje-obawy/3c4kksg>

³ *Sondaż: Ogromne zaufanie Polaków do wojska. Do UE jest najniższe od lat*, https://biznes.interia.pl/polityka/news-sondaz-ogromne-zaufanie-polakow-do-wojska-do-ue-jest-najnizs.nId,22420291#google_vignette

⁴ *CBOS: 63 proc. badanych dostrzega zagrożenie dla niepodległości Polski*, <https://www.pap.pl/aktualnosci/cbos-63-proc-badanych-dostrzega-zagrozenie-dla-niepodleglosci-polski-26-proc-jest>

pełnoskalowa wojna Rosji przeciw Ukrainie była sytuacją stosunkowo nową i dla wielu jeszcze zaskakującą, w moc sojuszu wierzyło 81% Polaków¹.

Należałoby więc zadać pytanie, co wydarzyło się na przestrzeni tych lat, że tak znacząco zmienił się stosunek Polaków do Paktu Północnoatlantyckiego. Czy odpowiada za to tylko niekonsekwentna polityka Donalda Trumpa, który nie może się zdecydować co myśli o NATO i roli, jaką USA miałyby w nim pełnić? Gdy obywateli Polski zapytano, czy armia amerykańska udzieliłaby nam pomocy otrzymano 63,8% odpowiedzi twierdzących, a 25,8% ankietowanych wyrażało przeciwną opinię². Jesteśmy więc sceptyczni wobec największego i najsilniejszego sojusznika, a to dobra wiadomość dla Kremla, który cieszy się z każdego pęknięcia pomiędzy swoimi wrogami. Trzeba wszakże podkreślić, że powyższe deklaracje stoją w pewnej sprzeczności z wynikami badań United Surveys z września 2025 roku. Aż 92,2% respondentów stwierdziło wtedy, że „NATO powinno zwiększyć obecność militarną na granicach z Rosją w odpowiedzi na naruszanie przestrzeni powietrznej”³. Mamy więc konkretne oczekiwania i równocześnie sądzimy, że nie zostaną one spełnione. Takie rozbieżności w deklaracjach dowodzą, jak łatwo manipulować nastrojami i zarządzać strachem, aby osiągnąć oczekiwane rezultaty – brak wiary w moc sojuszy, ale także w zakresie społecznego poparcia dla relacji Polski z państwami członkowskimi NATO czy Unii Europejskiej. Według raportu przygotowanego przez European Movement International we współpracy z firmą badawczą Savanta tylko 34% Polaków sądzi, że członkostwo w UE ma pozytywny wpływ na ich kraj. Jest to najniższy

¹ J. Ceglarsz, *Oto zaufanie Polaków do armii. Rzadko jesteśmy tak jednomyslni*, <https://businessinsider.com.pl/wiadomosci/oto-zaufanie-polakow-do-armii-rzadko-jestesmy-tak-jednomyslni-sondaz/cyew17n>

² *Czy Ameryka obroni Polskę? Polacy wierzą w armię USA*, <https://wiadomosci.onet.pl/swiat/czy-ameryka-obroni-polske-polacy-wierza-w-armie-usa-sondaz/72n7zyz>

³ *Polacy jednomyslni: NATO powinno wzmocnić granicę z Rosją*, <https://wiadomosci.wp.pl/polacy-jednomyslni-nato-powinno-wzmocnic-granice-z-rosja-7207079069547392a>

wynik wśród siedmiu analizowanych państw członkowskich Unii Europejskiej¹.

Przykładem umiejętnego kształtowania społecznych emocji jest stosunek Polaków do sąsiadów. We wrześniu 2025 roku 59,1% pytanym było przekonanych, że Niemcy powinny zapłacić Polsce reparacje za szkody wyrządzone podczas II wojny światowej². Dla porównania w 2011 roku 31,1% Polaków było przeciwnych rozliczaniu Rosjan ze zbrodni katyńskiej w imię zachowania dobrych relacji z Federacją Rosyjską. To niemało, nawet, jeśli 43% uważało, że Polska powinna dochodzić swoich praw³. Jednocześnie 57% Polaków chciało usłyszeć przeprosiny za zamordowanie polskich oficerów w Katyniu, ale tylko 26% ankietowanych oczekiwało reparacji⁴. Powtórzmy – reparacji od Niemiec chce ponad połowa obywateli Polski.

Czy odpowiada za to polityka, czy może niedostatki edukacji otwierające drogę kremlowskiej propagandzie? W 2008 roku zaledwie co drugi Polak wiedział, że 17 września 1939 roku Polskę zaatakowała Armia Czerwona⁵, a na przestrzeni lat 2010-2017 z dwóch do dziesięciu procent wzrósł odsetek osób, które niczego nie wiedzą o mordach dokonanych w Katyniu⁶. Można byłoby postawić pytanie, czy to Moskwa przekonała nas, że nie powinniśmy zajmować się historią, jeśli jest to historia rosyjska. Wydarzenia na Wołyniu wciąż są bowiem

¹ Z. Grosse, *Rozczarowanie demokracją w UE rośnie. Co o Unii myślą Polacy?*, <https://euractiv.pl/section/praca-i-polityka-spoleczna/news/rozczarowanie-demokracja-w-ue-rosnie-co-o-unii-mysla-polacy/>

² *Zapytali Polaków o reparacje od Niemiec. Większość nie ma wątpliwości*, <https://www.polsatnews.pl/wiadomosc/2025-09-28/zapytali-polakow-o-reparacje-od-niemiec-wiekszosc-nie-ma-watpliwosci/>

³ *Sondaż: co trzeci Polak woli Rosję niż Katyń*, <https://www.newsweek.pl/polska/sondaz-o-katyniu-co-trzeci-polak-woli-rosje-niz-katyn/735nw0r>

⁴ *Polacy chcą, żeby Rosja przeprosiła za Katyń*, <https://wiadomosci.wp.pl/polacy-chca-zeby-rosja-przeprosila-za-katyn-6037846016889985a>

⁵ *Co zdarzyło się 17 września? Nie wiem*, <https://wydarzenia.interia.pl/kraj/news-co-zdarzylo-sie-17-wrzesnia-nie-wiem,nld,846555>

⁶ Z. Maciejczak, M. Modzelewska, R. Wiśniewski, *Pamięć o Zbrodni Katyńskiej w Polsce*, Narodowe Centrum Kultury, Warszawa 2018, <https://pamietamkatyn1940.pl/wp-content/uploads/2020/04/pamiec-o-zbrodni-katynskiej-w-polsce-raport.pdf>, s. 11.

tematem gorących dyskusji politycznych i społecznych, a w grudniu 2024 roku 67,4% ankietowanych nie wierzyło w szczerość ukraińskich intencji w sprawie upamiętnienia ofiar rzezi wołyńskiej, ekshumacji i rozliczenia historycznego¹, co ma bezpośrednie przełożenie na uzależnienie przez 50,2% Polaków zgody na przystąpienie Ukrainy do NATO lub Unii Europejskiej od zamknięcia spraw ekshumacji². W obliczu wojny, której tak się boimy, wciąż przedkładamy kwestie historyczne nad bezpieczeństwo.

W 2023 roku 82% Polaków nie darzyło Rosjan sympatią. Rok później grupa ta zmalała do 76%. W roku 2025 już tylko 72% „nie lubi” Rosjan. W tym samym czasie o 2%, z sześciu do ośmiu, wzrósł odsetek tych, którzy odnoszą się życzliwie do mieszkańców kraju, który nam zagraża³.

Sympatia do Ukraińców między rokiem 2023 a 2025 stopniała z 51% do 30%. Poziom niechęci wzrósł z 17% do 38%. Za te nastroje niekoniecznie odpowiadają sami Ukraińcy, tak jak Rosjanie nie zapracowali, by nagle zacząć darzyć ich sympatią. Ktoś jednak umiejętnie podsycy animozje wobec sojuszników i kreuje pozytywny wizerunek tych, których działania są zagrożeniem dla bezpieczeństwa. I dobrze byłoby zastanowić się, dlaczego ulegamy takim podszeptom, które nie muszą być racjonalne, ale bazują na emocjach i strachu, nie zawsze mającym uzasadnione podstawy.

¹ S.Przybył, *Czy Polacy wierzą w ukraińskie intencje w sprawie Wołynia? Najnowszy sondaż*, <https://wydarzenia.interia.pl/zagranica/news-czy-polacy-wierza-w-ukrainskie-intencje-w-sprawie-wolynia-na,nld,7880472>

² *Ekshumacje ofiar Wołynia to problem w relacjach z Ukrainą. Nowy sondaż*, <https://wiadomosci.onet.pl/kraj/sondaz-ekshumacje-ofiar-wolynia-to-problem-w-relacjach-z-ukraina/kyndjmr>

³ *Stosunek Polaków do innych narodów*, CBOS, komunikat z badań, nr 13/2025, oprac. M. Omyła-Rudzka, https://www.cbos.pl/SPISKOM.POL/2025/K_013_25.PDF, s. 4-5.

*Михайло Сінаюк
студент
Львівський національний університет
імені Івана Франка
ORCID ID: 0009-0009-2254-7430*

СИСТЕМА ЦИФРОВОЇ ПРОПАГАНДИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ТА СТРАТЕГІЯ ПРОАКТИВНОЇ ПРОТИДІЇ

Російська цифрова пропаганда — це цілісний, ієрархічно вибудований механізм, де кожен рівень виконує визначену функцію для забезпечення максимальної ефективності впливу. Попри уявлення про хаос ботомереж і Telegram-каналів, ідеться про системну архітектуру, що об'єднує державні інституції, спецслужби, глобальні медіа та проксі-структури за кордоном.

На вершині пропагандистської вертикалі стоять російські спецслужби — ГУ ГШ, ФСБ та СЗР. Вони не лише організовують кібероперації (злами, витоки даних, дезінформаційні кампанії), а й визначають стратегічні теми, тестують нові наративи та координують поширення через підконтрольні медіа. "Фабрика тролів" та подібні структури є нижньою ланкою, що реалізує вказівки центрів управління, забезпечуючи синхронність меседжів у державних ЗМІ та соцмережах.

Середній рівень займають глобальні медіапроекти — RT та Sputnik, які "перекладають" внутрішню пропаганду на міжнародний контекст, створюючи ілюзію альтернативної, "легітимної" точки зору. Їхня мета — не переконання, а релятивізація істини: підваження довіри до будь-яких фактів через постійне порівняння, відволікання уваги ("whataboutism") і зміщення фокусу на недоліки Заходу.

Окремий контур — Telegram-канали, що стали головним майданчиком гібридного впливу завдяки анонімності та швидкості. Мережі "воєнкорів", чиновників і фейкових "інсайдерів" формують спільний інформаційний простір. Навіть канали, які зовні виглядають опозиційними, отримують темники з одних центрів. Це дає змогу

запускати узгоджені хвилі дезінформації — наприклад, про "зраду", "паніку" чи "втечу українського керівництва".

Важливою ланкою є підтримка екстремістських рухів за кордоном — ультраправих, ультралівих, антиглобалістів чи антивакцинатарів. Через фінансування та медійну допомогу Росія інтегрує свої наративи у місцеві політичні дискурси, підриваючи стабільність західних демократій і просуваючи ідеї "загниваючого Заходу" чи "нацистів в Україні".

Російська пропаганда принципово агресивна й наступальна. Вона не обороняє позицію, а атакує, використовуючи дегуманізацію ("нацисти", "сатаністи", "маріонетки Заходу") як засіб виправдання воєнних злочинів. Агресія є постійною, незалежно від реальної ситуації на фронті. Наступальний підхід полягає у проактивному створенні подій: ще до обстрілів запускаються наративи про "підготовку українських провокацій", що дозволяє РФ виглядати "реакцією на загрозу". Таким чином, пропаганда не відображає реальність, а конструює її наперед, забезпечуючи інформаційну перевагу.

Найвищий рівень цієї системи — формування дискурсу. Росія зсуває фокус із фактів на сумніви: замість "ракета зруйнувала будинок" обговорюють "чий це ракети" або "чим Захід спровокував Росію". Так Москва контролює порядок денний, змушуючи світ реагувати на вигадані теми. Для Заходу це означає підрив політичної волі допомагати Україні, для Глобального Півдня — зміцнення антизахідної солідарності через наративи про "боротьбу проти неоколоніалізму" та "санкційний голод".

Україна та її партнери досі переважно діють реактивно, спростовуючи російські фейки. Але така модель прирікає на постійну оборону: будь-яке спростування легітимізує "вкид" як тему для обговорення. Щоб зламати цей цикл, потрібно перейти до наступальної комунікації — формування власних рамок дискурсу, у яких російська сторона буде змушена реагувати.

Основою нової стратегії має стати аксіологічне лідерство, тобто створення морально сильних, позитивних і універсальних наративів,

які апелюють до загальнолюдських цінностей. Серед можливих напрямів:

- Образ захисниці християнства. На тлі популярності релігійного консерватизму у світі слід позиціонувати Україну як продовжувачку справжніх християнських традицій і спадкоємицю Русі, а Росію — як псевдохристиянську, кланово-ісламізовану державу;
- Позиція сили, а не жертви. Демонструвати ефективність українських ударів по військових об'єктах РФ, підкреслюючи здатність України діяти активно та впевнено;
- Дискурс майбутнього. Просувати образ України як модерної, інноваційної, європейської держави, що здатна побудувати "оновлену Європу" — із врахуванням помилок старої.

Наступальність також означає створення інформаційних дилем для російської системи: підриє ключових міфів (наприклад, про "єдність народів Росії", розкриваючи регіональну нерівність і конфлікти еліт), звернення безпосередньо до російської аудиторії з фактами, які важко спростувати без саморуйнування інших наративів (втрати, корупція, збагачення верхівки), перевантаження пропагандистської машини великою кількістю достовірних, деталізованих повідомлень, що унеможлиблює централізовану реакцію.

Висновки

Російська цифрова пропаганда — це не хаотичний шум, а добре організована система, інтегрована в державну структуру та спрямована на контроль глобального дискурсу. Її агресивний і наступальний характер робить неефективною будь-яку суто оборонну реакцію. Тому Україна та її союзники мають перейти від реактивного спростування до наступального формування порядку денного — будуючи власні морально сильні, проєвропейські та релігійно-ціннісні наративи. Лише ставши активними архітекторами інформаційного поля, а не його спостерігачами, можна виснажити російську пропаганду, перетворивши інформаційну протидію на інструмент політичного й морального лідерства.

*Віталій Ткачук
аспірант спеціальності "С2-Політологія"
Львівський національний університет
імені Івана Франка*

ЕТИЧНІ РАМКИ ЦИФРОВОЇ АКТИВНОСТІ СУБ'ЄКТІВ ПОЛІТИЧНИХ ПРОЦЕСІВ

Етика цифрової активності охоплює багато проблем, таких як поширення дезінформації, зловживання даними, маніпулювання громадською думкою, мікро-таргетинг, відсутність прозорості. Перелічені елементи мають спершу непомітний, втім, безпосередній вплив на етичні рамки цифрової діяльності політиків в питаннях комунікації, оскільки вони розширюють рамки допустимого. Під "допустимим" мають на увазі методи та інструменти, які політичний суб'єкт може використовувати в особистих цілях, при цьому не отримуючи негативної реакції. На суб'єктивну думку автора, сучасна "атмосфера" у соціальних мережах щодо політичних дискусій є відверто ворожою. Глобальна політична ситуація нараховує велику кількість соціальних, економічних та екологічних проблем, чим користуються окремі суб'єкти. Це також формує середовище, у якому такі політики як Урсула фон дер Ляєн та Еммануель Макрон, які дотримуються вивіреного та поміркованого стилю спілкування, виглядають не надто впевнено у порівнянні з прихильниками агресивної комунікації, таких як Дональд Трамп та Андрес Мануель Лопес.

Для українських дипломатів, перебування у такому цифровому середовищі означає, що вони часто змушені мати справу з різного роду провокаціями. Однією з найчастіших тем таких провокацій є заяви щодо некомпетентності або недобросовісності окремих політичних суб'єктів. Прикладом такого є публікація Ілоном Маском у жовтні 2023 року мему з Володимиром Зеленським, що

висміював його прохання військової допомоги.¹ Також, частою темою атак у цифрових мережах є спільні болючі історичні епізоди між країнами, прикладами яких є висловлювання Кароля Навроцького, який заявляв, що не бачить місця для України в ЄС та НАТО «доки не будуть вирішені важливі цивілізаційні питання», або Гжегожа Брауна який пропагував конспірологічні теорії, такі як «українізація Польщі». Можна посперечатись, що активні реакції українськими суб'єктами політики на подібні гострі заяви, навіть якщо вони сформульовані у тактовній формі, є недоцільними, адже цифрове середовище дає змогу політику займатись більш звичною, нейтральною діяльністю, такою як представлення новин про законодавство та реформи або публікація дописів щодо прогресу виконання передвиборчих обіцянок. Утім, слід пам'ятати про вищезгаданий аспект у вигляді сучасної "атмосфери" у соціальних мережах, яка є виразно "токсичною" та грубою. Реалії є такими, що політики, як головні репрезенти своїх держав у сучасному цифровому середовищі, повинні відстоювати її честь, формувати її авторитет. Згадана "атмосфера" функціонує у доволі цинічній парадигмі, в рамках якої велика кількість користувачів відсторонено спостерігає за політичними дебатами, обираючи "правого" у конфлікті відповідно до власних ідеологічних переконань, а не базуючись на фактах та об'єктивності. Це, у свою чергу, може слугувати причиною того, що окремі політичні суб'єкти, усвідомлюючи описані реалії політичної дискусії в інтернеті, переступають через етичні норми, вдаючись до різних форм маніпуляцій та пропаганди. При цьому, ці ж самі суб'єкти можуть щиро вірити у допустимість таких методів, якщо, в їхньому уявленні, це дозволить закріпити позиції єдиновірного бачення або рішення щодо певної ситуації, що у свою чергу на благо усієї держави. Таким чином, виникають закономірні питання щодо того,

¹ x.com/elonmusk/status/1708629197617336398?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1708629197617336398%7Ctwgr%5E1403d2006636703b196c71c2d5c46319ea282889%7Ctwcon%5Es1_c10

чи існують які-небудь "етичні рамки" в цифровій діяльності як такі, і чи потрібні вони взагалі?

Для доведення потреби наявності етичних рамок розглянемо один кейс, а саме, скандальний випадок, коли 19 грудня 2024 року під час прес конференції у Брюсселі Володимир Зеленський різко відреагував на заяву Володимира Путіна про «технологічну дуель» над Києвом, а в також нецензурно висловившись про самого Путіна: «Люди гинуть, а йому "цікаво"... д*****б»¹. Цікавість даного випадку полягає у його демонстрації явища, яке притаманне сучасній цифровій політичній культурі, а саме «ефект натовпу», коли аудиторія підштовхує політика до дедалі різкіших заяв. Багато українців звичайно ж, підтримали Зеленського, але з об'єктивної точки зору, подібні висловлювання у виконанні президента держави є проблемними. Власне, проблематика саме цього випадку полягає не лише в тому, що подібні висловлювання легалізують образливу лексику у політичному дискурсі загалом, створюючи підґрунтя для більш токсичного середовища, а й в тому, що вони мають прямий вплив на підрив і без того дуже чутливої та складної програми переговорів з агресором щодо зупинення війни. Знову ж таки, цинічність як цифрового політичного середовища, так і геополітичної "гри" загалом диктує потребу контролювати емоції та бути поміркованим у висловлюваннях навіть у таких відверто "чорно-білих" подіях як війна України та росії. Згаданий вище «ефект натовпу» проявляє себе у масовому розповсюдженні репліки та її сприйняття аудиторією які демонструють, що така емоційна та ненормативна реакція дозволяє зміцнити довіру певної частини аудиторії за рахунок відчуття щирості та «людяності» лідера. Утім, як відзначають критики, коли перша особа держави демонструє тотальну неконтрольованість емоцій - це ніяким чином не допомагає покращити ситуацію.

Отож, вищенаведене спостереження демонструє, що політичні суб'єкти здатні впливати негативною цифровою активністю на рівень онлайн-дискусій, таким чином підтверджуючи потребу

¹ <https://x.com/ZelenskyyUa/status/1869795228955386102>

наявності чітких етичних рамок. Утім, що ж служитиме інструментом визначення цих самих рамок? Часто, найпершою ідеєю є створення спеціальної "системи оцінювання". Білл Адаір у своїй статті для Atlantic "Чого я не розумів про політичну брехню" пропонує створення спеціальної системи, що заснована на своєрідних "балах довіри". За його словами "Якщо політики брешуть, бо вважають, що це принесе їм більше користі, ніж шкоди, ми маємо змінити підхід. Технологічні та медійні компанії мають створити стимули для правдивих висловлювань і стримувальні заходи для брехні. Платформи всіх видів можуть встановлювати вищі тарифи на рекламу для кандидатів, які мають найгірші оцінки від факт-чекерів. Телевізійні мережі можуть позбавляти кандидатів часу для виступів під час дебатів, якщо їх спіймали на брехні." [1] Хоч у статті акцент зроблений на протидії дезінформації, а не на проблемі неетичної комунікації, запропонована методика викликає інтерес. Утім, на мою суб'єктивну думку, практичні спроби реалізувати подібні механізми є недоцільними і навіть дещо шкідливими з двох причин. По перше, управління такого роду механізмом гарантовано стане ціллю для різноманітних ворогуючих політичних таборів, а з урахуванням сучасної ситуації щодо цифрового дискурсу, наявність нового інструменту цензуру точно не сприятиме покращенню ситуації. По друге, імплементація таких засобів сама по собі матиме відверто принизливий характер, адже символізуватиме зізнання політичних суб'єктів у неспроможності діяти добросовісно без зовнішніх регуляторів.

Утім, це й не означає, що політикам і дипломатам дозволено діяти як їм заманеться, адже подібне розширення рамок допустимого в значній мірі й посприяло формуванню вищеописаного токсичного онлайн середовища. Оскільки політичні діячі не лише транслиють позицію держави, а й формують культуру спілкування в суспільстві, їхній стиль комунікації стає зразком для громадян, через що відхід від етичних рамок має ефект «доміно». Отож, замість зовнішніх обмежень, які врешті всерівно виглядатимуть як форма цензури, ключем є внутрішня культура самоконтролю політиків. Формування нових стандартів поведінки

вже відбувається через міжнародні етичні кодекси, такі як "Кодекс дій проти дезінформації ЄС" та "Регулювання прозорості та адресності політичної реклами (ТТРА)". Підсумовуючи, етичні рамки цифрової активності політичних діячів виступають не лише інструментом підтримки політичної культури, але й фактором безпеки держави у міжнародному вимірі. Саме тому питання етики онлайн-комунікацій має стати предметом не лише політичних дебатів, але й наукового осмислення, адже від їх дотримання залежить рівень довіри до політики загалом та ефективність міждержавного діалогу.

Список використаних джерел:

1. Білл Адаір : "What I Didn't Understand About Political Lying"
<https://www.theatlantic.com/ideas/archive/2024/10/political-lying-fact-checking-social-media/680184> 2024 р.
2. Наталія Шкворченко : "Політична токсичність у контрастивній перспективі"
<https://periodicals.karazin.ua/cognitiondiscourse/article/view/22240> 2023 р.

*Надія Харченко
Львівський національний університет
імені Івана Франка*

НОВИЙ ІНФОРМАЦІЙНИЙ ПОРЯДОК ЦИФРОВОЇ ДОБИ

Перехід у цифрову добу означає не лише технічну інфраструктурну трансформацію – він означає зміни в способах створення, обробки, поширення, споживання та контролю інформації. Цей процес формує новий інформаційний порядок – структуру влади, впливу, комунікації й культури, котра переосмислює традиційні поняття публічної сфери, демократії, приватності та знання.

Новий інформаційний порядок цифрової доби є глобальною системою організації, розповсюдження та споживання інформації, сформований під впливом поширення інтернету, цифрових технологій, великих даних, штучного інтелекту та соціальних мереж.

Якщо у ХХ ст. домінували традиційні ЗМІ (преса, радіо, телебачення), то у ХХІ ст. центральним елементом стала децентралізована цифрова екосистема, у якій інформація створюється та поширюється не тільки державними чи корпоративними структурами, а й мільярдами індивідуальних користувачів.

Однією з фундаментальних рис цифрової доби є безпрецедентні обсяги даних – збір, зберігання, обробка надвеликих масивів інформації (big data). Завдяки Інтернету речей (IoT), упровадженню сенсорних технологій і смартфонів миттєво виникають величезні обсяги даних, які стосуються найрізноманітніших сфер суспільного життя (енергетика, медицина, логістика, торгівля тощо) [1], а також інтегрують у складну інформаційну систему окремого індивіда.

Характерною особливістю сучасного інформаційного життя також є алгоритмічний контроль і персоналізація. Сьогодні користувачі бачать не «всю» інформацію, а тільки те, що відібрав алгоритм. Рекомендаційні системи, стрічки соціальних мереж, пошукові ранжування – усе це формує індивідуальні інформаційні простори, які можуть не перетинатися (т. зв. *filter bubbles*, або «бульбашки фільтрів», «інформаційні бульбашки»).

У класичних медіа існували професійні редакції й наскрізна система контролю якості. У рамках нового інформаційного порядку кожен може бути автором або куратором контенту (блогер, автор telegram-каналу, ведучий подкасту) – у такій системі якість контенту в рівній мірі залежатиме як від кваліфікації і відповідальності конкретного виконавця, так і від контролю якості інформаційного продукту, який здійснюється на організаційно-інституційному рівні. Це призвело до появи феномену децентралізованої медіа-комунікації, коли інформаційні потоки генеруються не лише професійними редакціями, а й мільйонами користувачів

соціальних мереж. Оскільки кожен суб'єкт інформаційних відносин (не залежно від рівня його організації та підпорядкування) може продукувати інформацію (а саме головне пропонувати власні погляди на те, як її слід розуміти) виникає боротьба за інтерпретацію фактів. Дезінформація, фейки, маніпулятивні алгоритми стають елементами стратегій акторів інформаційних відносин. При цьому, не всі мають рівний доступ до цифрових технологій, якісного інтернету, освіти, що дозволяє критично сприймати і відповідально реалізовувати інформацію. Це породжує новий розрив – цифровий розрив – між країнами, регіонами, соціальними групами. При цьому «цифровий розрив» слід розуміти не лише як нерівний доступ до можливостей користування цифровими технологіями, але також як розрив у спроможності критично, свідомо й відповідально використовувати нові можливості цифрових технологій.

У багатьох країнах владні еліти прагнуть установити контроль над функціонуванням цифрових платформ обміну повідомленнями, процесами поширення та споживання інформації, а також розробляють і впроваджують законодавство, що регулює збір і обробку даних, модерацію контенту та відповідальність платформ. Європейський GDPR-регламент, ініціативи з контролю над алгоритмами, локальні цифрові обмеження – усе це елементи, які формують рамки нового інформаційного порядку. Регуляція стає не пасивною, а активною: платформи змушені підкорятися вимогам модерації, перевірки даних, прозорості алгоритмів тощо.

Серед ключових рис нового інформаційного порядку варто виділити наступні:

- цифровізація: інформація оцифрована і доступна у глобальному масштабі в режимі реального часу;
- глобальна мережевість: інтернет та соціальні платформи створили умови для миттєвої комунікації між окремими індивідами, державами та культурами;

- децентралізація виробництва інформації: традиційні медіа втратили монополію, громадяни та локальні спільноти стають повноцінними виробниками новин і знань;
- конкуренція (війна) наративів: у світі співіснують різні рамки інтерпретації фактів, що визначає нові формати інформаційних війн та нові механізми маніпуляцій;
- алгоритмізація доступу: штучний інтелект і програмні алгоритми визначають, яку інформацію бачить користувач, що підвищує ризик формування інформаційних «бульбашок»;
- цифровий суверенітет: держави прагнуть контролювати інформаційні потоки та технології доступні їхнім громадянам (прикладом є правове регулювання даних у ЄС чи цифровий контроль у Китаї (система Great Firewall of China)).

З точки зору впливу нового інформаційного порядку на суспільство можна виділити наступні виміри:

1) політичний вимір: формування громадської думки дедалі більше залежить від соціальних медіа; з'являються нові форми політичного впливу: кіберкампанії, інтернет-пропаганда та цифровий активізм;

2) економічний вимір: дані стали «ною нафтою». Глобальні корпорації (Google, Meta, Amazon) отримали владу, яка часто співставна або перевищує вплив держав;

3) культурний вимір: національні культури трансформуються під тиском глобальних цифрових трендів, відбувається уніфікація способів комунікації, але одночасно відроджуються локальні ідентичності через цифрові платформи;

4) соціальний вимір: інформаційна перенасиченість сприяє поширенню дезінформації, фейків і цифрової залежності, що створює нові виклики для психології та освіти.

Таким чином, новий інформаційний порядок цифрової доби - це складне поєднання технологічних, соціальних, економічних і політичних змін. Він ставить перед суспільством вимогу усвідомленого вибору: якими мають бути межі свободи, приватності, контролю, інновацій. Переваги нового порядку - демократизація, інновації, швидкість - реально можуть змінювати

світ на краще. Однак без критичного ставлення, ефективних правових механізмів та етичної чутливості майбутні ризики, пов'язані з маніпуляціями та цифровим виключенням, можуть переважити.

Використані джерела:

1. Digital Transformation: The Information Age Accelerates – Part 2/5.
URL: <https://c3.ai/blog/digital-transformation-information-age-accelerates-part-2-5>

*Дарина Чижова
студентка 1-го курсу магістратури
Львівський національний університет
імені Івана Франка*

ЦИФРОВІ НАРАТИВИ СТРАТЕГІЧНОГО ЗАЛЯКУВАННЯ: КЕЙС РОСІЙСЬКОЇ «ЗБРОЇ СУДНОГО ДНЯ»

У сучасному інформаційному середовищі цифрові канали є не лише засобом поширення новин, а ключовим інструментом стратегічної комунікації. В умовах геополітичної напруги та гібридних загроз особливого значення набувають наративи, побудовані на залякуванні – коли держава використовує не лише військову силу, а й інформаційний вплив для тиску на міжнародну спільноту. Аналіз таких цифрових стратегій дозволяє зрозуміти, як формуються глобальні уявлення про силу і як цифрова дипломатія може протидіяти маніпуляціям.

Цифрові наративи – це послідовні історії, створені для впливу на уявлення, емоції та поведінку аудиторій через цифрові платформи. Стратегічне залякування передбачає демонстрацію сили або готовності її застосувати, аби змусити супротивника утриматися від певних дій. У сучасному вимірі воно охоплює як військові, так і інформаційні інструменти тиску, що поширюються через медіа, соціальні мережі та офіційні заяви.

Одним із найпомітніших прикладів такого поєднання сили та комунікаційного впливу є інформаційна кампанія Росії навколо так званої «зброї судного дня» – підводного комплексу *Poseidon*. Інформаційна кампанія навколо якого почала набирати обертів після публічної презентації російського пакета «суперзброй» президентом В. Путіним у 2018 році, коли Кремль офіційно назвав ці розробки елементом своєї стратегії стримування. З того часу повідомлення про *Poseidon* регулярно з'являлися в державних ЗМІ, у військових брифінгах та репортажах про випробування й «морські випробування» апарату, що створювало основу для ширшої інформаційної кампанії. Одночасно проєкт інтенсивно просувався через пропагандистські канали (TASS, RT), регіональні медіа, а також у більш гнучких цифрових середовищах таких, як Telegram-каналах, YouTube-роліках і соцмережах, де поширювалися візуальні рендера, «ексклюзивні» повідомлення про випробування і кадрові сюжети про підготовку носіїв (наприклад, підводного крейсера *Belgorod*). Ця суміш офіційних заяв і оперативних «витоків» створює постійну інформаційну хвилю, яка тримає тему в публічному полі.

Ключові меседжі, що просуваються російськими каналами, мають кілька повторюваних ліній: (1) технологічна унікальність і «невразливість» системи – вона нібито уникає існуючих систем ППО/ПРО; (2) здатність завдавати немислимих, катастрофічних втрат (сценарії «цунамі»/радіоактивного забруднення при підриві біля узбережжя); (3) демонстративний знак «стримування» – використання повідомлень як елементу зовнішньополітичного шантажу. Ці меседжі подаються в медіа через сильні образи (цифрові візуалізації, інтерактивні карти), розповіді про «перші партії» або «морські випробування» та інтерв'ю з «експертами», що формує візуально-звуковий наратив невідворотності загрози.

Ефект страху і «непереможності» створюється поєднанням технічної риторики й емоційних візуалів: деталізовані CGI-зображення апарату, заяви про «перші партії» чи «успішні випробування» та повідомлення про спеціалізовані носії (як от підводний крейсер *Belgorod*) активно поширювалися у 2018–2023

рр., що підсилювало суспільний і медійний інтерес до теми. Державні повідомлення підсилювалися прокремлівськими Telegram-каналами й блогами, які вели хроніку «успіхів», а «витоки» технічних кадрів або «ексклюзивні» фото використовувалися для створення враження оперативності та достовірності.

Ці наративи викликали реакції на різних рівнях. У міжнародному полі вони сприяли посиленню стратегії стримування і посиленню уваги з боку НАТО та окремих держав: оголошення нових «суперзброй» і повідомлення про випробування спонукали західних аналітиків і політиків до додаткових оцінок загроз і перегляду заходів колективної безпеки. Наприклад, аналітичні центри і ЗМІ в США та ЄС публікували технічні огляди та скептичні оцінки «гіперболізованих» заяв, а союзницькі структури посилювали розмови про модернізацію ППО та морських спроможностей. На рівні громадян загальнодоступні матеріали породжували або панічні уявлення про «невідворотну катастрофу», або, навпаки, сприймалися як елемент пропаганди – залежно від джерела інформації та рівня медіаграмотності аудиторії.

Водночас частина експертного співтовариства підкреслювала, що технічні обмеження і логістичні реалії значно обмежують практичну «катастрофічність» таких систем: навіть за сценарієм застосування, реальний тактичний і стратегічний ефект залежить від ряду факторів (надійність, навігація, кількість носіїв, реакція іншої сторони), що робить інформаційну кампанію більш ефективним інструментом політичного впливу, ніж сама зброя – тобто комунікаційний ефект часто перевищує технічну реальність. Ця дисбалансна комбінація технічної демонстрації й інформаційного нагнітання є ключовим механізмом, через який «зброя судного дня» працює як інструмент стратегічного залякування в цифровому просторі.

Узагальнюючи результати аналізу, можна зробити висновок, що стратегічне залякування дедалі частіше реалізується саме в інформаційному вимірі. Російська Федерація формує образ *Poseidon* не стільки як бойового засобу, скільки як символу «абсолютної сили», який впливає на емоційне сприйняття загроз і політичні

рішення супротивників. У цьому сенсі цифровий ядерний шантаж стає формою стратегічної комунікації, де зброя є лише приводом для конструювання страху, сумнівів і стратегічної невизначеності.

Таким чином, формування стійкості до інформаційного залякування стає не лише завданням оборонної політики, а й невід'ємною частиною цифрової дипломатії та міжнародної безпеки. Для держав, що протидіють гібридним загрозам, ключовим є не лише технологічний, а й комунікаційний аспект безпеки – здатність розпізнавати маніпуляції, будувати власні позитивні наративи й утверджувати довіру у глобальному цифровому просторі.

Використані джерела:

1. Dr. Zeeshan Faisal Khan, «STRATEGIC NARRATIVES IN COMMUNICATION: CRAFTING INFLUENCE AND POWER IN A GLOBALIZED WORLD». URL: <https://ijssbulletin.com/index.php/IJSSB/article/view/1137>
2. National Defense University, «Science of Military Strategy (2020 Ed.) Chapter 8: Strategic Deterrence». URL: <https://interpret.csis.org/translations/science-of-military-strategy-2020-ed-chapter-8-strategic-deterrence>
3. Silky Kaur, «One nuclear-armed Poseidon torpedo could decimate a coastal city. Russia wants 30 of them». URL: <https://thebulletin.org/2023/06/one-nuclear-armed-poseidon-torpedo-could-decimate-a-coastal-city-russia-wants-30-of-them>
4. Samuel Bendett, Mathieu Boulègue, «Advanced military technology in Russia». URL: <https://www.chathamhouse.org/2021/09/advanced-military-technology-russia/03-putins-super-weapons>
5. Franz-Stefan Gady, «Russia (Once Again) Announces Start of Sea Trials of 'Doomsday Weapon'». URL: <https://thediplomat.com/2018/12/russia-once-again-announces-start-of-sea-trials-of-doomsday-weapon>
6. Liana Fix, Steven Keil, «NATO and Russia after the Invasion of Ukraine». URL: <https://www.gmfus.org/news/nato-and-russia-after-invasion-ukraine>

7. Severin Pleyer, «Technological Hype Of New Nuclear Delivery Systems – The Neglect Of The Concept Of Deterrence». URL: <https://tdhj.org/blog/post/russia-nucleardelivery-kinzhal-poseidon-skyfall>

Roman Chuprin
Candidate of Political Sciences, Docent

SPORT AS A DIGITAL BATTLEFIELD: DATA, DIPLOMACY, AND FAILED NEUTRALITY IN THE RUSSIAN–UKRAINIAN WAR

In the modern world, international elite sport has become an integral and strategically important element of a state's soft power — a sphere where public attention, global media coverage, and the actions of well-known athletes can have immediate diplomatic and informational effects. The international sports arena, because of its visibility and emotional engagement, possesses enormous viral potential, making it a powerful tool for shaping global narratives and public opinion.

In the context of the Russian–Ukrainian war, the struggle to maintain the isolation of Russian sport has thus become not only a question of fairness and principle but also a vital front of modern diplomacy. Efforts to document and expose violations of political neutrality by Russian and Belarusian athletes — individuals often recognized worldwide — have served as a crucial instrument in countering Russian propaganda and amplifying Ukraine's voice internationally. These efforts have been grounded in the systematic collection and analysis of data from a wide range of digital sources, open media, and public databases, conducted jointly by civil society, investigative journalists, governmental institutions, and the National Olympic Committee (NOC) of Ukraine.

While some international sports federations have maintained a complete suspension of Russian and Belarusian athletes, others have allowed their return under a “neutral” status. A key challenge has been the divergence in policy between the International Olympic Committee (IOC), which issues recommendations on neutral participation, and

international sports federations, which implement these recommendations in practice.

Despite the evident importance of the issue, the IOC has provided no official follow-up, reporting, or statistical transparency regarding the significant number of failed neutrality verifications among Russian and Belarusian athletes admitted by international sport federations. This absence of official monitoring and public accountability prompted the author to conduct independent research aimed at identifying and quantifying the real scale of non-compliance. The resulting data not only fill a major informational gap but also offer Ukrainian sports institutions and diplomatic missions a factual foundation to reinforce their positions in the global effort to sustain the isolation of Russian sport.

The present study sets out to determine the extent to which the international sports federations' neutrality checks comply with IOC standards and to provide a quantitative assessment of their reliability based on actual IOC decisions regarding invitations to the 2024 Olympic Games in Paris.

The research examined the granting of neutral status to Russian and Belarusian athletes in 11 Olympic sports, including wrestling, judo, tennis, canoeing / kayaking, rowing, taekwondo, road cycling, swimming, shooting, trampoline, rowing, and modern pentathlon. The results show that more than 43% of the neutral statuses issued by international sport federations were not confirmed by the IOC during the final invitation process for the 2024 Olympic Games in Paris. In some sports, this proportion was dramatically higher — 100% of cases in modern pentathlon, 80% in taekwondo, 76% in judo, and 56% in wrestling. These findings indicate widespread inconsistencies in the application of neutrality criteria and the prevalence of formal or superficial reviews by international sport federations.

Particularly concerning are the practical consequences of improperly granted neutral statuses. Analysis of qualification tournaments in wrestling and taekwondo — disciplines where Olympic licenses were distributed through direct head-to-head matches — revealed that more than 60 athletes from 30 countries were negatively affected by the participation of Russian and Belarusian competitors who were later

denied IOC invitations. Among the affected nations were Austria, Azerbaijan, Bulgaria, Denmark, Estonia, France, Georgia, Germany, Greece, Hungary, India, Iran, Italy, Kazakhstan, Latvia, Lithuania, Mexico, Mongolia, Norway, People's Republic of China, Poland, the Republic of Korea, Romania, Serbia, Spain, Sweden, Switzerland, Ukraine, the United States, and Uzbekistan. These examples demonstrate that the issue has substantial international consequences and compromises the fairness and integrity of Olympic qualification processes.

The study further argues that many international federations systematically ignore evidence provided by the NOC of Ukraine and Ukrainian sports organizations regarding violations of neutrality, such as public support for the war, affiliation with military or security structures, or participation in propaganda events. The reluctance to respond to such information reflects not merely institutional weakness but a broader lack of political will to ensure adherence to ethical and legal principles. Particularly notable in this respect are the United World Wrestling and the International Judo Federation, which have repeatedly disregarded documented cases of non-neutral behavior by Russian and Belarusian athletes.

Another significant finding concerns the limitations of the IOC's neutrality criteria themselves. These criteria do not take into account the illegal visits of Russian and Belarusian athletes to occupied Ukrainian territories, training camps and recreational events there, or participation in competitions held in these areas — all of which constitute violations of international law. Such omissions allow athletes directly involved in or supportive of the occupation to maintain eligibility under the guise of neutrality.

Overall, the results of this research demonstrate that the concept of neutral status for Russian and Belarusian athletes has been fundamentally compromised. International sport federations either lack the institutional capacity or the political will to conduct thorough verification, while the IOC has no effective instruments to monitor compliance at the federation level. Furthermore, there is no international sports body capable of ensuring the integrity of neutrality checks, nor

could such a body, even in theory, possess sufficient authority to verify issues like border-crossing legality.

As a result, individuals affiliated with the Russian army, security agencies, and propaganda structures — as well as those who finance or publicly support Russia's war against Ukraine — continue to participate in international competitions under a neutral status. This undermines both the moral and political foundations of global sport.

The research concludes that the problem has transcended the boundaries of the sports community and cannot be resolved solely by sport institutions. Since it directly concerns issues of sovereignty, national security, and international law, the resolution of this problem requires coordinated diplomatic action and intergovernmental cooperation.

*Роман Шипка
Львівський національний університет
імені Івана Франка*

КІБЕРБЕЗПЕКА ТА ЦИФРОВА ДИПЛОМАТІЯ

У XXI столітті цифрова трансформація радикально змінила природу міжнародних відносин і поняття державного суверенітету. Кіберпростір став новим виміром глобальної політики, у якому переплітаються економічні, інформаційні та безпекові інтереси держав. У цьому контексті формується новий напрям міжнародної взаємодії — цифрова дипломатія, або кібердипломатія, що поєднує традиційні інструменти дипломатії з викликами цифрової епохи. Її головна мета — забезпечення миру, довіри та безпеки у кіберпросторі.

Традиційне розуміння суверенітету — контроль держави над територією та населенням — нині доповнюється поняттям цифрового суверенітету, тобто здатності держави захищати власну інформаційну інфраструктуру, дані та інформаційні потоки.

Кібератаки на критичну інфраструктуру (енергетичні системи, фінансовий сектор, охорону здоров'я) демонструють, що порушення цифрового суверенітету може мати наслідки, співмірні з актами збройної агресії. Такі інциденти, як атака WannaCry (2017) або злам системи SolarWinds (2020), засвідчили масштабність загроз і необхідність міждержавної співпраці у сфері кібербезпеки. Кібератаки в сучасному світі більше не є виключно технічною проблемою — вони стали елементом геополітичної конкуренції, що потребує дипломатичного врегулювання.

Можна сказати, що сучасний дипломат виконує подвійну функцію: з одного боку, він є миротворцем, який сприяє запобіганню конфліктам, а з іншого — захисником національного суверенітету в кіберпросторі.

Дипломати ведуть переговори щодо встановлення норм поведінки держав у кіберпросторі, сприяють запровадженню механізмів довіри (Confidence-Building Measures, CBMs) та координують міжнародну взаємодію під час кіберінцидентів.

Особливу роль відіграє публічна дипломатія, що через цифрові платформи формує позитивний міжнародний імідж держави, протидіє дезінформації та сприяє зміцненню довіри між суспільствами.

Формування міжнародних правил поведінки у кіберпросторі здійснюється через багатосторонні угоди та організації. Серед ключових документів і платформ:

- Будапештська конвенція про кіберзлочинність («*Convention on Cybercrime*», 2001) — перший міжнародний договір, що регулює співпрацю держав у протидії кіберзлочинам.
- Паризький заклик до довіри та безпеки у кіберпросторі («*Paris Call for Trust and Security in Cyberspace*», 2018) — багатостороння ініціатива, спрямована на зміцнення відповідальної поведінки держав та приватного сектору.
- Таллінський посібник (Tallinn Manual) — нормативне тлумачення застосування міжнародного гуманітарного права до кіберконфліктів.

- Група урядових експертів ООН (GGE) та Відкрита робоча група (OEWG) — основні форуми для розроблення глобальних кібернорм.

Ці ініціативи демонструють прагнення держав створити правову основу для відповідальної поведінки у кіберпросторі, хоча глобальний консенсус залишається складним через політичні суперечності.

Регіональні об'єднання дедалі активніше інтегрують питання кібербезпеки до своєї безпекової політики:

- НАТО визнало кіберпростір оперативним доменом і запровадило Програму колективного кіберзахисту, включно зі спільними навчаннями та інформаційним обміном.
- АСЕАН реалізує Стратегію кіберспівробітництва, спрямовану на гармонізацію національних політик і розвиток потенціалу держав-членів.
- Африканський Союз ухвалив Конвенцію про кібербезпеку та захист персональних даних, щоб подолати цифрову нерівність між країнами континенту.

Такі альянси сприяють зміцненню регіональної стабільності, але водночас виявляють розрив між рівнем цифрової готовності розвинених і країн, що розвиваються.

Близько 80% критичної цифрової інфраструктури належить приватним компаніям, тому без їхньої участі неможливо забезпечити кіберстійкість.

Публічно-приватні партнерства (PPP), зокрема Cybersecurity Tech Accord, об'єднують технологічні корпорації у зусиллях із протидії державним і кримінальним кібератакам. Такі моделі взаємодії сприяють обміну інформацією про загрози, створенню інноваційних засобів кіберзахисту, удосконаленню процесів атрибуції кібератак, розвитку спільних етичних стандартів у цифровій сфері.

Цей напрям цифрової дипломатії формує нову парадигму глобального врядування, де уряди, бізнес і громадянське суспільство співпрацюють на засадах довіри та відповідальності.

Цифровізація загострює низку етичних проблем:

- баланс між безпекою та приватністю у державній політиці;
- упередженість алгоритмів у системах штучного інтелекту;
- використання кіберзброї проти цивільних об'єктів;
- маніпуляції та дезінформація як інструмент політичного впливу.

Дипломати повинні розробляти міжнародні механізми, які поєднують етичні принципи з безпековими потребами. У цьому контексті зростає значення морального лідерства у зовнішній політиці та формування універсальних етичних норм використання технологій.

Розвиток штучного інтелекту (ШІ), блокчейну та квантових технологій докорінно змінює методи дипломатії:

- ШІ допомагає у прогнозуванні кіберризиків і моделюванні сценаріїв конфліктів, але його автономне використання потребує етичного контролю.
- Блокчейн створює можливості для прозорого моніторингу виконання міжнародних угод і перевірки достовірності даних.
- Квантові технології відкривають нову епоху в криптографії, але водночас ставлять під загрозу чинні стандарти безпеки.

Інноваційні технології мають бути не лише інструментом сили, а й засобом зміцнення довіри — через спільні наукові програми, стандарти етичного ШІ та розвиток «цифрових посольств».

Світова спільнота залишається розділеною між двома моделями управління кіберпростором:

- Відкрита модель Заходу, заснована на принципах прозорості, свободи інформації та багатостейкхолдерності.
- Суверенна модель, яку просувають авторитарні режими, наголошуючи на контролі держави над цифровими потоками.

Це протистояння поглиблює цифровий розкол, унаслідок якого країни, що розвиваються, залишаються поза процесом вироблення норм.

Подолати його можливо лише через програми нарощування потенціалу, освіти в галузі кібербезпеки та залучення менш розвинених держав до глобальних процесів прийняття рішень.

Майбутнє кібердипломатії визначатиметься кількома стратегічними тенденціями:

- Інституціоналізація — створення спеціалізованих кіберпосольств та підрозділів у МЗС.
- Міждисциплінарність — інтеграція знань із міжнародного права, технологій та етики.
- Етичне управління технологіями — розробка міжнародних стандартів прозорого використання ІІІ.
- Розвиток механізмів верифікації — впровадження систем на основі блокчейну для підтвердження фактів кібератак.
- Посилення довіри — створення платформ для обміну інформацією й проведення спільних кібернавчань.
- Інклюзивність — забезпечення рівноправної участі всіх держав, незалежно від рівня технологічного розвитку.

Кібербезпека та цифрова дипломатія становлять єдиний простір формування нової архітектури міжнародної безпеки. Вони покликані забезпечити баланс між національним суверенітетом і глобальною співпрацею, захистити права людини в цифровому середовищі та зміцнити довіру між державами.

Кібердипломатія є ключовим механізмом запобігання конфліктам у цифрову добу. Вона має спиратися на етичні принципи, інноваційні технології та інклюзивність. Міжнародна співпраця, багаторівнева взаємодія держав і приватного сектору, а також прозорість і довіра — необхідні умови глобальної цифрової безпеки. Отже, кібербезпека стає новою мовою миру, а цифрова дипломатія — інструментом захисту суверенітету та справедливості у глобальному цифровому порядку.