

БЕЗПЕКОВИЙ АСПЕКТ ЦИФРОВОЇ ДИПЛОМАТІЇ

Матчук Я. Ю.

аспірант кафедри міжнародної інформації

Інституту міжнародних відносин

Київського національного університету імені Тараса Шевченка

Розвиток новітніх технологій сприяв трансформації стратегії зовнішньополітичної комунікації міжнародних акторів, що дозволило ефективніше просувати та забезпечувати національні інтереси на міжнародній арені. Поступово в науковий обіг було введено термін «цифрова дипломатія» та сформульовано концептуальні підходи для вивчення цього явища. Тому актуальність дослідження визначається науковою і політичною доцільністю з'ясування перспектив модернізації сфери зовнішньої політики з огляду на використання цифрової дипломатії як сучасного інструменту політичної діяльності держави. До того ж варто відзначити, що завдяки мережевим технологіям та їхній здатності до поєднання індивідуального, групового та масового типів комунікації, з'являється нова модель зовнішньополітичного спілкування, яка відрізняється значною різноманітністю форм і використанням сучасних інформаційно-комунікаційних технологій [1].

Сутність використання цифрової дипломатії у зовнішньополітичній діяльності держав полягає у створенні позитивного іміджу країни та зміцненні її міжнародної репутації, представленні національних інтересів і досягненні ключових цілей зовнішньої політики, а також просуванні культурних цінностей за допомогою сучасних технологій.

Вважаємо за потрібне охарактеризувати безпековий аспект цифрової дипломатії через наявність таких трендів розвитку міжнародних відносин, як:

- демократизація міжнародних відносин, яка проявляється у необхідності пошуку шляхів легітимізації політичних рішень, оскільки нині ефективна міжнародно-політична діяльність є неможливою без залучення підтримки населення та вибудови системи отримання зворотного зв'язку, тому актори міжнародних відносин намагаються встановити та підтримувати тісні взаємозв'язки з громадськістю. При цьому спостерігається вплив як громадськості на владні рішення, так і влади на громадські ініціативи, що стало можливим лише в умовах інтенсивного використання соціальних медіа як політичного інструменту. Тому дослідження міжнародного та національного інформаційного простору дозволяє прогнозувати реакцію міжнародних акторів та громадськості на зовнішньополітичні рішення, при цьому маніпуляція, викривлення та підробка інформації можуть негативно впливати на репутацію міжнародних акторів, а також сприяти дискредитації їхніх рішень або дій;

- посилення ролі особистості у сучасних міжнародних відносинах завдяки зростаючому використанню міжнародно-політичними діячами соціальних медіа для комунікації з аудиторією та нівелювання посередника у вигляді класичних медіа, що потребує посилення технічних заходів безпеки та дотримання правил приватності;

- інформатизація середовища міжнародної взаємодії, що проявляється у зміні ролі інформації, збереженні її цілісності та формуванні каналів її передачі, а тому швидкість поширення даних, забезпечення вільного доступу, управління та маніпуляція інформаційними ресурсами стали актуальними питаннями дотримання засади міжнародної та національної безпеки. Таким чином, мережа Інтернет та безпосередньо соціальні медіа перетворюються на додатковий простір поширення міжнародних позитивних та негативних взаємовпливів.

Виходячи з описаних трендів міжнародних відносин, можна виокремити такі підходи до вивчення безпекового аспекту в рамках цифрової дипломатії, як:

- аналіз системи збереження конфіденційності, цілісності, доступності та надійності інформації [2];

- дослідження захисту самої системи обробки і зберігання даних, що забезпечує конфіденційність, доступність і цілісність інформації [3].

Зазначимо, що у Законі України «Про основні засади забезпечення кібербезпеки України» 2017 р. подано таке визначення кібербезпеки, як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [4].

Таким чином, у Законі України відображено цілісне розуміння безпеки в цифровому середовищі як поєднання технічної та соціально-гуманітарної складових інформаційної діяльності, тобто захисту контенту інформації та дотримання безпеки інфраструктури. Тому у рамках дослідження цифрової дипломатії необхідно враховувати обидва безпекові аспекти, що дозволить представити ефективні рекомендації для міжнародних акторів у сфері зовнішньополітичної комунікації.

Список використаних джерел

1. Westcott N. Digital Diplomacy: The Impact of the Internet on International Relations [Text] / Nicholas Westcott. – London, 2008. – 20 p. – (Oxford Internet Institute).

2. Andress J. The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice [Text] / Jason Andress. - Oxford, 2014 - (Syngress).

3. Cybersecurity Issues and Challenges: In Brief / Congressional Research Service. -<<https://www.fas.org/sgp/crs/misc/R43831.pdf>.> - 2014.

4. Закон України Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) - Електронний ресурс - Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19>