DOI https://doi.org/10.30525/978-9934-26-613-3-24

THE ROLE OF INSTITUTIONS IN SHAPING THE STATE'S INFORMATION POLICY IN TIMES OF WAR CRISES

РОЛЬ ІНСТИТУЦІЙ У ФОРМУВАННІ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ДЕРЖАВИ В УМОВАХ ВОЄННИХ КРИЗ

Sviderska O. I.
Candidate of Political Sciences,
Associate Professor
Military Institute of Taras Shevchenko
National University of Kyiv
Kyiv, Ukraine

Свідерська О. І.
кандидат політичних наук,
доцент
Військовий інститут Київського
національного університету імені
Тараса Шевченка
м. Київ, Україна

Вступ. Державна інформаційна політика в умовах воєнної кризи є першочерговим засобом підтримки соціальної згуртованості та довіри до інститутів. У ситуації, коли населення стикається з потоком суперечливої інформації, відсутність скоординованої державної позиції посилює відчуття невизначеності, підриває моральний стан населення і створює інформаційні ніші, які легко можна використати для поширення ворожих наративів. Сьогодні протидія дезінформації ускладнена різними підходами до цього процесу з боку основних акторів – державних інституцій, політичних сил, громадянського суспільства, окремих громадян та бізнес-корпорацій. Найбільший виклик полягає у практиці «подвійних стандартів», коли представники державних інституції, декларуючи захист суспільства від дезінформаційних загроз, використовують такі ж інструменти для просування власних наративів [1]. Фрагментація інформаційної політики в умовах воєнних криз створює проблему вироблення єдиної точки управління інформаційними потоками, яка б ґрунтувалася на інституційних правилах та стандартах кібербезпеки. Відповідно, конгруентна державна інформаційна політика мала б встановлювати правові та етичні рамки для діяльності в інформаційному просторі під час війни – від протидії ворожій пропаганді до захисту прав громадян та дотримання норм міжнародного гуманітарного права.

Наукові підходи до вивчення інформаційної політики спираються на різні концепції: від аналізу інформаційної війни, що відображено у роботах К. Келлі, А. Біденко, О. Тарабукін, теорії постіндустріального суспільства Д. Белла, теорії мережевого суспільства М. Кастельса до критики симулятивності й фрагментації сучасних комунікацій, про що

йдеться у роботах Р. Водак та М. Гудмен. С. Браман ж визначає інформаційну політику як комплекс правових, управлінських і комунікаційних практик, що формують суспільні відносини в інформаційному просторі.

Особливого значення інформаційна політика набуває у контексті інформаційної війни (цілеспрямованих злочинних дій, метою яких у загальному вигляді є дезінформація, деморалізація, та вибудовування «мовчазної покірності населення», що здійснюються державою-агресором [5, с. 62]. Інший аспект інформаційної (мережевої війни) пояснює К. Келлі, який наголошує, що мережева війна «передбачає формування нового способу мислення та нового типу конфліктів». У його розумінні – інформація це своєрідна зброя, яка здатна демонтувати одні реальності та створювати інші, а соціальні групи та держави однаково можуть впливати на великі політичні зміни «без єдиного пострілу» [4, с. 213].

У концепції постіндустріального суспільства Д. Белла, розуміння інформаційного суспільства полягає у віднайдені й встановлені системи значень, через які люди можуть співвідносити себе з навколишнім світом [6]. Таким чином звиклий спосіб людського існування дедалі більше перетворюється на систему знаків, кодів і шифрів [2, с. 194]. Інтернет-користувач наче перебуває у реальності, яка йому видається впорядкованою і керованою, однак, насправді – це оманлива проста ілюзія, котра підміняє собою реально складну й плюралістичну систему сучасних суспільств [10]. Усвідомлення значення інформаційного суспільства у формуванні інформаційної політики воюючої держави, пов’язане з тим, що воно трансформує політичний процес, породжуючи нову віртуальну масу, чия поведінка характеризується симулятивністю, фрагментарністю та поступовим нівелюванням традиційних інституцій [3]. Окремою проблемою є швидкість, з якою за допомогою використання соціальних мереж можна налаштувати цілі народи один проти одного.

Кампанії із дезінформації та поширенням мови ворожнечі, які проводить рф проти України зосереджені саме на цивільному населенню, що цілком узгоджується із російською концепцією «геополітичного інформаційного протиборства», ключовою метою якого є дестабілізація систем ухвалення рішень і механізмів управління у держави-противника, маніпулювання громадською думкою на глобальному, регіональному та національному рівнях, а також забезпечення інформаційної безпеки рф з метою збереження її впливу та ефективного функціонування у світовому інформаційному просторі. Тому поки світові лідери роздумують над червоними лініями інформаційних операцій, та про їхню відповідність міжнародному гуманітарному праву, дані Surfshark ще у 2023 році свідчили, що саме

рф стала світовим лідером за кількістю урядових запитів до Google щодо видалення контенту, що вказує на використання інституційних механізмів для контролю інформаційного простору. Різке зростання кількості таких запитів після 2014 року та особливо у 2022 році (понад 300%) демонструє, що агресія рф супроводжується системною політикою обмеження доступу до інформації, яка висвітлює військові злочини, та наявність жертв серед цивільних [8]. Отже, інституційний вимір інформаційної політики рф як країни-агресора, базується на поєднанні правових заборон, адміністративного тиску та маніпулятивних практик, що робить формування ефективних механізмів протидії інформаційним війнам критично необхідним завданням для демократичних держав.

Нажаль сьогодні в академічних колах і досі триває дискусія щодо концептуалізації поняття інформаційної політики. У реальному світі також політика, що проголошується як інформаційна, часто немає узгодженості, водночас багато політичних практик, які (можливо) є інформаційною політикою, продовжують представлятися під альтернативними заголовками. Все це відображає хронічну аморфність центрального поняття – інформації – та, як наслідок, плутанину щодо цілей інформаційного суспільства.

Сандра Браман у праці «Визначення інформаційної політики», опублікованій у першому випуску Journal of Information Policy, зазначає, що інформаційна політика охоплює закони, нормативні акти, доктрини та управлінські практики, які мають конститутивні наслідки для суспільства та стосуються створення, обробки, поширення, доступу й використання інформації [7, с. 3]. Це визначення підкреслює, що інформаційна політика є не просто сукупністю технічних рішень, а системним відображенням суспільних цінностей та управлінських стратегій. У сучасних умовах воєнних криз особливого значення набуває питання розширення цього визначення на сферу даних, адже саме великі масиви даних («big data») дедалі частіше визначають зміст інформаційних потоків, механізми прийняття політичних рішень та інституційні практики держав. Отже, формування ефективної інформаційної політики потребує врахування не лише технічних і правових аспектів, але й інформаційної етики – традиції обміну, відкритості та доступу, які в умовах глобальних інформаційних протистоянь можуть по-різному інтерпретуватися й набувати різної ваги, у залежності від політичних контекстів.

У грудні 2023 року Європейський Союз ухвалив Regulation (EU, Euratom) 2023/2841, що закріплює спільні стандарти забезпечення високого рівня кібербезпеки в інституціях, органах, офісах та агентствах ЄС. Цей документ є важливою віхою у формуванні сучасної інформаційної політики Союзу в умовах зростання кіберзагроз,

оскільки встановлює обов'язки щодо впровадження комплексних систем управління ризиками, регулярного моніторингу та звітності про кіберінциденти, застосування принципів «безпека за замовчуванням» і «безпека в процесі проєктування». Регламент передбачає створення міжінституційного органу – *Interinstitutional Cybersecurity Board*, який координує політику кіберзахисту та контролює її виконання, а також розширення мандату *CERT-EU* (тепер – *Cybersecurity Service for the Union institutions, bodies, offices and agencies*), що функціонує як центр реагування на інциденти, обміну інформацією та кризового управління. Такий підхід засвідчує перехід від фрагментарних заходів до єдиної нормативно-правової рамки, що зміцнює стійкість інституцій ЄС до інформаційних та кібернетичних загроз і водночас слугує прикладом для національних держав у сфері розбудови власної інформаційної безпеки [9].

Інформаційна політика України у 2022–2025 роках формувалася під вирішальним впливом повномасштабної війни та стала фактично інструментом національної безпеки. Її сутність полягає у протидії російським інформаційно-психологічним операціям, консолідації суспільства навколо державних рішень, забезпеченні єдиного голосу держави переважно через активні зовнішні комунікації для мобілізації міжнародної підтримки, стратегічні комунікації ключових інститутів, а також розвиток цифрових сервісів як елементів довіри до держави. Водночас слабкими сторонами цієї політики стали надмірна централізація та уніфікація інформаційного простору, що призвело до зниження довіри до офіційних каналів через відсутність плюралізму; провальні кампанії, пов'язані з недооцінкою роботи з внутрішньою аудиторією (зокрема у темах мобілізації, воєнних втрат чи соціально-економічних проблем); недостатня координація між державними інституціями та незалежними медіа; а також слабкий розвиток довгострокових наративів, здатних формувати візію майбутнього після війни. Це робить українську інформаційну політику ефективною у кризовому режимі «тут і зараз», але вразливою до стратегічних викликів та зростання суспільної втоми.

Висновки. У підсумку хочемо зазначити, що інформаційна політика при воєнних кризах – це не лише про державні канали й медіа; це *«whole-of-society»* підхід, який поєднує оперативну протидію дезінформації, посилення фактчекінгу, підвищення медіаграмотності й співпрацю з міжнародними партнерами. Практика останніх років показує: поєднання державної координації із залученням неурядових ініціатив, експертних центрів і платформ дозволяє значно швидше нейтралізувати інформаційні загрози та зберегти стратегічні комунікаційні переваги.

Література:

1. Біденко А., Золотухін Д., Тарабукін О. Біла книга протидії дезінформації. Київ : ГО «Інститут інформаційної безпеки», 2022. 62 с.

2. Гудмен М. Злочини майбутнього. Харків : Фабула, 2019. 592 с.

3. Кастельс М. Інтернет-ґалактика. Міркування щодо Інтернету, бізнесу і суспільства. Київ : Ваклер, 2007. 304 с.

4. Келлі К. Невідворотне: 12 технологій, що формують наше майбутнє. Київ : Наш формат, 2018. 340 с.

5. Свідерська О. І. Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. *Політикус*. 2022. Вип. 2. С. 60–65.

6. Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. Special Anniversary Edition, with a new foreword by the author. New York : Basic Books, 1999. 507 p.

7. Braman S. Defining information policy. *Journal of Information Policy*. 2011. № 1. P. 1–5.

8. Governments' content removal requests to Google. URL: http://surl.li/nvzfu (дата звернення: 06.10.2025).

9. Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. URL: https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng (дата звернення: 06.10.2025).

10. Wodak R. On far-right populism and shame. URL: https://bit.ly/3VX2gs2 (дата звернення: 06.10.2025).