



DOI: 10.21564/2786-7811.1.290476

ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ ТА ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ВИКЛИКИ ТА РЕАЛІЇ ВІЙНИ

Куцепал Світлана Вікторівна,
професор кафедри теоретико-правових дисциплін
Полтавський юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

ORCID: 0000-0003- 3804-6031
e-mail: svetlanakutsepal@gmail.com

Анотація. Стаття присвячена дослідженню феноменів інформаційного суверенітету та інформаційної безпеки України в умовах російської військової агресії. В умовах повномасштабної війни національна безпека нерозривно пов'язана з інформаційним суверенітетом держави і перетворюється на своєрідний «інформаційний фронт», де держава має використати усі наявні можливості для руйнування інформаційно-маніпулятивних вкидів та маніпуляцій, забезпечення доступу населення до перевіреної достовірної інформації. Аргументовано тезу, що інформаційна безпека займає ключове місце в системі національної безпеки держави, особливо важливим це стає в умовах повномасштабної військової агресії, коли актуалізується необхідність захисту суб'єктів інформаційних відносин від негативного інформаційного впливу ворога. Доведено, що національні інтереси України в умовах повномасштабної війни, яку розв'язала країна-агресор, вимагають захисту інформаційного суверенітету та створення сприятливих умов для забезпечення інформаційної безпеки країни, протидії спеціальним інформаційним операціям, що мають за мету підлив державного суверенітету та територіальної цілісності України. Проаналізовано зв'язок між феноменами інформаційної безпеки та інформаційного суверенітету, встановлено, що в умовах повномасштабної війни суттєво збільшується роль органів державної влади у контексті захисту



державних та національних інтересів, мінімізації руйнівних наслідків інформаційної агресії. Обґрунтовано, що важливою умовою перемоги України є забезпечення її інформаційної безпеки та інформаційного суверенітету. Інформаційна безпека є важливою складовою національної безпеки держави, тому увага до питань інформаційної безпеки, забезпечення ефективних механізмів та моделей її захисту є одним з пріоритетних завдань держави. Це потребує вдосконалення координації діяльності владних органів стосовно запобігання, виявлення та знешкодження інформаційних операцій ворога, оцінки та прогнозування загроз інформаційної безпеки, оперативного забезпечення ліквідації їх наслідків.

Ключові слова: війна, інформаційна війна, суверенітет, інформація, інформаційний суверенітет, інформаційна безпека, засоби масової інформації, комунікативний простір.

INFORMATION SOVEREIGNTY AND INFORMATION SECURITY IN UKRAINE: CHALLENGES AND REALITIES OF WAR

Svitlana V. Kutsepal,

Professor at the Department of Theoretical Legal Subjects
Poltava Law Institute of the Yaroslav Mudryi National Law University

ORCID: 0000-0003-3804-6031

e-mail: svetlanakutsepal@gmail.com

Summary. The article is devoted to the study of the phenomena of information sovereignty and information security of Ukraine under the conditions of Russian military aggression. The thesis is argued that information security occupies a key place in the state national security system; it becomes especially important in the conditions of full-scale military aggression, when the need to protect the subjects of information relations from the negative informational influence of the enemy is actualized. It has been proven that the national interests of Ukraine in the conditions of a full-scale war, which was unleashed by the aggressor country, require the protection of information



sovereignty and the creation of favorable conditions for ensuring the country's information security, countering special information operations aimed at undermining the state sovereignty and territorial integrity of Ukraine. The relationship between the phenomena of information security and information sovereignty was analyzed, and it was established that in the conditions of a full-scale war, the role of state authorities in the context of protecting state and national interests and minimizing the destructive consequences of information aggression significantly increases. It is substantiated that an important condition for the victory of Ukraine is to ensure its information security and information sovereignty. Information security is an important component of the state's national security; therefore, attention to information security issues, provision of effective mechanisms and models for its protection is one of the priority tasks of the state. This requires improving the coordination of the activities of the authorities in relation to the prevention, detection and neutralization of information operations of the enemy, assessment and forecasting of threats to information security, prompt provision of liquidation of their consequences.

Key words: war, information war, sovereignty, information, information sovereignty, information security, mass media, communication space.

Постановка проблеми. 24 лютого 2022 року життя населення України кардинально змінилося, відбувся розрив сталих соціальних зв'язків, мільйони українських громадян перетворилися на вимушених мігрантів. У перші тижні війни виникла ситуація «інформаційного вакууму», мільйони людей вчилися жити(виживати) в умовах, які важко було навіть уявити в ХХІ столітті. Потрібно було також адекватно реагувати на шквал інформації, яка далеко не завжди відповідала дійсності, відокремлювати істину від інформаційних вкидів та маніпуляцій, протистояти інформаційній агресії.

Вже півтора року триває повномасштабна російська агресія і Україна виборює свою свободу не лише безпосередньо на полі бою, а й відстоює національні інтереси в ідеологічній, політичній, енергетичній, гуманітарній



сферах, де також здійснюється агресія. Все вище зазначене актуалізує проблеми інформаційної безпеки, що характеризується «як стан захищеного інформаційного простору, що здатен забезпечити реалізацію загальнонаціональних інтересів, збереження стійкості держави до екзогенних і ендогенних чинників, що становлять загрозу та пов'язані із активним розвитком цифровізації»[1, с.95].

Інформаційна війна/Інформаційна агресія – суттєвий фактор сьогодення, має свою архітектоніку та відповідний інструментарій, внаслідок чого інформаційна сфера перетворюється на поле бою, де використовуються різноманітні інформаційні технології впливу на свідомість громадян,

Інформаційна агресія побудована на засадах тоталітаризму, масової пропаганди, відсутності політичного плюралізму, коли довіра до інформації зазвичай втрачає свою аксіологічну природу, базується на неякісному та клікбейтному опрацюванні інформації в ЗМІ, а не тлумачиться як «суттєва рушійна сила переконань громадян й еліти щодо легітимності глобального управління» [2].

Арсенал засобів інформаційної агресії вражає розмаїттям і постійно поповнюється новітніми «розробками» - технології знецінення і висміювання, хайп на страшних новинах, інформаційна вакханалія, «зливи» неправдивої інформації, блогери та «експерти» з «необмеженим» доступом до «секретної» інформації, поширення дестабілізуючої інформації, стрімке просування «твіттер-медіа», провокування на потрібну емоцію, просування концептів та наративів, що привабливі у короткостроковій перспективі, проте насправді здійснюють руйнівний вплив на споживачів медіапродукту.

Стан опрацювання обраної проблематики, аналіз останніх публікацій та досліджень. Ґрунтовні та комплексні розвідки з проблематики феномену суверенітету загалом та інформаційного суверенітету зокрема, інформаційної безпеки наявні у вітчизняному та зарубіжному політико-правовому та соціально-філософському дискурсах. Проблематика інформаційного суверенітету та



інформаційної безпеки України висвітлюється у розвідках Бондаренка Р., Михальчука В., Залевської І., Удренас Г., Котерліна І., Солодкої О., Панченка О., Данильяна О., Дзьобаня О., Панфілова О. та ін. Проте дослідження інформаційного суверенітету та інформаційної безпеки України в контексті викликів війни проти країни-агресора у XXI столітті варте ґрунтовної соціально-філософської рефлексії з метою обґрунтуванням прикладних висновків і рекомендацій.

Мета статті – соціально-філософський аналіз специфіки феномену інформаційного суверенітету та інформаційної безпеки України в контексті реалій та викликів повномасштабної війни.

Реалізація зазначеної мети забезпечується використанням відповідного методологічного інструментарію, що поєднує як загальнонаукові методи (аналіз, синтез, узагальнення, порівняння, абстрагування), так і методи контент-аналізу, політико-правові та соціально-правові, діалектичний, аксіологічний та інші методи наукового дослідження.

Виклад основного матеріалу. XXI століття називають інформаційним століттям, тому будь-який сучасний збройний конфлікт неможливий без інформаційного супроводу, де активно задіяний увесь арсенал інформаційних можливостей як країни-агресора, так і країни, що протистоїть агресії. «Володіння інформаційними ресурсами та його захист у військовій сфері стали таким самим неодмінним атрибутом, як озброєння, боєприпаси, транспорт тощо»[3, с.25]. Інформація перетворюється на зброю, яка здатна ефективно впливати не лише на психіку та свідомість людей, а й на інформаційно-технічну інфраструктуру суспільства. Про ефективність та небезпечність такої зброї зауважує І.Котерлін: «Наявність зброї масового знищення не гарантує державі можливість перемоги, якщо вона не забезпечена перевагою в інформаційній сфері»[4, с.151]

Саме тому в інформаційній війні використовується практично вся інформаційна інфраструктура держави та суспільства, актуалізується необхідність захисту національного інформаційного простору, під яким



розуміється сукупність інформаційних ресурсів та інформаційної інфраструктури, актуалізуються проблеми інформаційної безпеки держави, що визначається як «стан збереження інформаційних ресурсів держави і захищеності законних прав особистості і суспільства в інформаційній сфері; стан держави, при якому не може бути завдано шкоди її інформаційному середовищу за допомогою використання інформаційних ресурсів і систем» [5, с.150].

Інформаційна безпека є важливою складовою національної безпеки держави, тому увага до питань інформаційної безпеки, забезпечення ефективних механізмів та моделей її захисту є одним з пріоритетних завдань держави.

Інформаційний вплив та інформаційні технології розраховані на масового споживача, мають на меті формування і розпалювання внутрішніх протиріч, при цьому обов'язково враховуються політичні, ментальні, екзистенційні особливості представників того чи іншого суспільства. Як писав С.Московічі, достатньо декілька яскравих образів, кількох формул, які «чіпляють» серце та проникають в душу, нагадування про велику колективну віру, і люди вже відчують себе колективом, певною зцементованою цілісністю [див.:6].

Інформаційне протистояння почалося задовго до повномасштабної агресії, як зауважує О.Панфілов, «суть стратегії інформаційного протиборства, що реалізується в сучасних війнах, полягає в тому, що цілі війни багато в чому досягаються не за рахунок захоплення та утримання чужих територій, а за рахунок підризу ще в мирний час оборонного та економічного потенціалу держави-противника» [7, с.190]. Найбільш дієвим інструментом інформаційного протиборства виступають ЗМІ. На думку О.Данильяна та О.Дзьобаня, ЗМІ «як найпоширеніший компонент медіапростору, мають величезні можливості у сфері політичних маніпуляцій та впливу на масову свідомість через формування в населення певної суспільної думки про ті чи інші події, людей, явища. ЗМІ і далі залишаються одним із найбільш потужних «каналів» трансляції настроїв та упереджень громадськості, її реакції на ті події, які відбуваються в країні та світі,



вони відіграють важливу роль у формуванні та висвітленні громадської думки, поєднуючи світ з особистістю та відтворюючи самооцінку суспільства» [8, с.12].

Український соціум, пересічні громадяни України вже декілька десятиліть є основним об'єктом впливу та маніпуляцій, адже «проросійські сили впродовж понад 30 років незалежності України мали неконкурентну перевагу над демократичними силами у фінансовому, медійному, політичному, ресурсному забезпеченні та проводили підривну роботу з метою висвітлення недієспроможності інституційного розвитку України»[9, с.121]. Така підривна робота проводилася з використанням найрізноманітніших можливостей – політичних та соціальних ток-шоу, кінофільмів та телесеріалів, телеграм-каналів, соціальних мереж.

Наявність різноманітних гаджетів та цифрових технологій, інтернет та мережових комунікацій актуалізувала проблему свідомого ставлення населення України до комунікації в умовах військової агресії, тому що в умовах війни на зброю перетворюється усе, що пов'язано з техніко-технологічними засобами і способами забезпечення телефонних розмов, електронних повідомлень, чатів у соцмережах, телеграм-каналів, особистого поштового листування та інших видів інформаційно-комунікаційних зв'язків, тобто гаджети перетворюються на джерело для несанкціонованого збирання та отримання інформації, яка може суттєво зашкодити національним та державним інтересам.

На жаль, неодноразово публікації у соціальних мережах фото та відео наслідків ворожих обстрілів, роботи засобів ППО, пересування української військової техніки тощо створювали загрозу для військових та цивільного населення, спричиняли значні руйнації інфраструктури. Таким чином в умовах війни інформаційні та цифрові технології мають використовуватися свідомо та обережно, щоб унеможливити витік інформації, тому «формування інформаційної безпеки в умовах війни є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У воєнний час захист інформаційної безпеки держави є



пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини» [4, с.154].

«В умовах повномасштабної агресії ворог використовує будь-які засоби для того, щоб залякати населення, «зломати» спротив, породити відчай та недовіру до держави, уряду, армії, тобто «чужоземна влада не тільки захоплює територію, матеріальні блага, руйнує культурні архетипи мислення та «калічить» мову, а й становить загрозу існуванню автохтонного населення території, спонукає до розділу країни та забуття окупованих»[Цюрупа, с.52]. Це надзвичайно небезпечна стратегія, яка може призвести до негативних наслідків, розповсюдження сепаратистських настроїв, зневіри та відчаю серед частини населення захоплених територій.

В умовах повномасштабної інформаційної війни актуалізуються питання захисту інформаційного суверенітету України. Інформаційний суверенітет тлумачиться як «здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави» [11]. Закон України «Про Національну програму інформатизації» визначає також і основні напрями державної політики у сфері інформатизації, до яких належать: створення та розвиток державних і регіональних систем та мереж інформатизації та проектів інформатизації, що передбачають можливість сумісності та взаємодії в єдиному інформаційному просторі України, захист як національного надбання інформаційних ресурсів держави, забезпечення єдності державних стандартів у даній сфері та відповідність міжнародним стандартам, забезпечення національної безпеки, здійснення єдиної державної науково-технічної та промислової політики, забезпечення залучення іноземних інвестицій, створення механізму стимулювання участі недержавних структур у реалізації проектів у сфері інформатизації [11].

Окрім дефініції поняття «інформаційний суверенітет», репрезентованої Законом України «Про Національну програму інформатизації», наведемо ще дві



дефініції. Так, інформаційний суверенітет визначається як «здатність і намір суб'єкта політики виробляти, розподіляти та споживати інформацію залежно від власних інтересів та використовувати інформацію як ресурс політичного впливу в тих масштабах і обсягах, які відповідають за поточний та довгостроковий політичний інтерес» [12, с.191]. У даній дефініції акцент робиться на політичну природу інформаційного суверенітету.

О.Солодка пропонує таку дефініцію: «інформаційний суверенітет – це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України та рівноправності і незалежності у відносинах з іншими державами у глобальному інформаційному просторі»[13, с.83]. На основі наведених дефініцій можна виділити основні компоненти інформаційного суверенітету, якими є інформація, інформаційний простір, що включає інформаційну інфраструктуру і інформаційні технології.

Інформаційний суверенітет базується на національних інформаційних ресурсах, забезпечується контролем держави за станом та наповнюванням інформаційних потоків. Видом інформаційного суверенітету вважається цифровий суверенітет, пов'язаний з «забезпеченням пріоритетних завдань щодо забезпечення ІКТ-незалежності держави» [13, с.82]. Забезпечення інформаційної безпеки та інформаційного суверенітету мають визначальне значення в успішному протистоянні російській агресії.

Висновки та пропозиції. Таким чином, проведене дослідження дає підставу для наступних висновків:

В умовах повномасштабної війни національна безпека нерозривно пов'язана з інформаційним суверенітетом держави і перетворюється на своєрідний «інформаційний фронт», де держава має використати усі наявні можливості для руйнування інформаційно-маніпулятивних вкидів та маніпуляцій, забезпечення доступу населення до перевіреної достовірної інформації.



Для мінімізації наслідків інформаційної агресії актуальним є вдосконалення координації діяльності владних органів стосовно запобігання, виявлення та знешкодження інформаційних операцій ворога, оцінки та прогнозування загроз інформаційної безпеки, оперативного забезпечення ліквідації їх наслідків.

Війна залишить кривавий відбиток не лише на економіці, демографічній та соціальній структурах українського суспільства, але й в свідомості та світогляді кожного небайдужого українця, підніме хвилю рефлексії з приводу інформаційних кампаній та вкидів, які роками здійснювали медіа та мас-медіа країни-агресорки, актуалізує пошуки винних в інформаційних програшах та провалах. Це деструктивний шлях, на який і розраховують політтехнологи країни-агресорки, натомість необхідна консолідація, об'єднання зусиль, що забезпечить непохитність інформаційного фронту, де протистояння спробам дестабілізувати ситуацію гібридними методами буде лише посилюватися, тому політико-медійне має бути переведене не в емоційне, а в «правове поле».

ЛІТЕРАТУРА

- 1.Бондаренко Р. В., Михальчук В. М. Інформаційна безпека держави. *Інвестиції: практика та досвід*. 2021. № 5. С. 95–101.
- 2.Dellmuth, L., Aart Scholte, J., Tallberg, J., & Verhaegen, S. (2022). Legitimacy in Global Governance. Chapter 1. Citizens, Elites, and the Legitimacy of Global Governance. Oxford: Oxford University Press. 289 p.
3. Залевська І.І., Удренас Г.І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. С.20-26.
- 4.Котерлін І.Б. Інформаційна безпека в умовах воєнного стану в аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. №1. С.150-155.



- 5.Панченко О.А. Суспільний запит на інформаційну безпеку. *Публічне урядування*. 2020. № 2 (22). С. 141-149.
- 6.Moscovici S. L'age des Foules. Un traité historique de psychologie des masses. Editions Complexe, 1985. 503 s.
- 7.Панфілов О.Ю. Інформаційне насильство як соціальний феномен. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2023. № 1 (56).С.188-200.
- 8.Данильян О.Г., Дзьобань О.П. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2022. № 3 (54).С.11-29.
- 9.Дурдинець М., Драп'ятий Б. Філософський вимір легітимності влади в період екзистенційної війни: досвід України ХХ–ХХІ століть. *Філософські та методологічні проблеми права*. 2023. № 1 (25). С. 120–129.
- 10.Цюрупа М. Соціально-філософський аналіз політико-правового статусу режиму окупації в контексті боротьби України за територіальну цілісність. *Українознавчий альманах*. 2017. Вип.20. С.52-55
- 11.Про Національну програму інформатизації: Закон України від 04.02.98 р. *Відомості Верховної Ради України*. 1998. № 27-28. Ст.181.
- 12.Ярема О.Г. Зміст інформаційного суверенітету в контексті державного суверенітету. *Юридичний науковий електронний журнал*. 2022. №3. С.191-194.
- 13.Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. №1(32).С.80-87.