УДК 351:004.738.5:327.5
DOI: 10.36550/2522-9230-2024-17-252-256

Крушеніцький Владислав Сергійович,
аспірант кафедри права та правоохоронної діяльності
Центральноукраїнського державного університету
імені Володимира Винниченка
v.s.krushenickiy@cuspu.edu.ua
ORCID ID: 0000-0001-9194-7897

ОРГАНИ ПУБЛІЧНОЇ ВЛАДИ ЯК СУБ'ЄКТИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ПОЛІТИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

У статті досліджено сучасні виклики у сфері національної безпеки України, які обумовлені масштабною гібридною агресією, масовим поширенням дезінформації, кіберзлочинністю, інформаційно-психологічним впливом та маніпуляціями у цифровому середовищі. В цих умовах пріоритетного значення набуває інформаційна безпека як складова системи національної безпеки. Метою дослідження є виявлення ролі органів публічної влади у формуванні та реалізації державної політики інформаційної безпеки, аналіз їхніх функцій, повноважень і взаємодії, а також формулювання практичних рекомендацій для підвищення ефективності інституційної діяльності в цій сфері.

Визначено, що законодавче забезпечення політики інформаційної безпеки здійснює Верховна Рада України через діяльність відповідних комітетів. Президент України реалізує стратегічне керівництво у цій сфері, зокрема через Раду національної безпеки і оборони України, яка координує дії органів виконавчої влади. Кабінет Міністрів України відповідає за формування та реалізацію державної інформаційної політики, розробку програм захисту інформаційного простору та цифрової трансформації. Важливими виконавчими структурами у сфері інформаційної безпеки є Служба безпеки України, Міністерство оборони України, Міністерство цифрової трансформації, Національний інститут стратегічних досліджень та інші органи, кожен з яких виконує специфічні завдання у межах національної системи безпеки.

У роботі окреслено проблеми у сфері міжвідомчої взаємодії, зокрема фрагментарність функцій, дублювання повноважень, недостатню координацію, слабку участь органів місцевого самоврядування, кадрову недостатність і нормативні прогалини. Автори підкреслюють, що в умовах сучасної інформаційної війни ефективне управління інформаційною безпекою потребує єдиного стратегічного бачення, скоординованих дій усіх державних суб'єктів та широкого залучення громадянського суспільства.

Запропоновано комплекс практичних заходів щодо удосконалення інституційної взаємодії у сфері інформаційної безпеки: розробка єдиної державної стратегії з чітким розподілом повноважень, створення спільних центрів аналізу й оперативного реагування, посилення стратегічних комунікацій, розвиток цифрової інфраструктури безпеки, підготовка кадрів та підвищення публічної прозорості. Усе це має сприяти формуванню ефективної, узгодженої, стійкої системи захисту інформаційного простору України.

Ключові слова: національна безпека, інформаційна безпека, органи публічної влади, інформаційний простір, державна політика, міжвідомча взаємодія, кіберзагрози, дезінформація, стратегічні комунікації.

Krushenitskyi V. PUBLIC AUTHORITY BODIES AS ENTITIES OF FORMING AND IMPLEMENTING NATIONAL SECURITY POLICY IN THE INFORMATION SPACE

The article examines the current challenges in the field of national security of Ukraine, which are caused by large-scale hybrid aggression, mass dissemination of disinformation, cybercrime, information and psychological influence and manipulation in the digital environment. In these conditions, information security as a component of the national security system acquires priority importance. The purpose of the study is to identify the role of public authorities in the formation and implementation of state information security policy, analyze their functions, powers and interaction, as well as formulate practical recommendations for increasing the effectiveness of institutional activities in this area.

It is determined that the legislative support of information security policy is carried out by the Verkhovna Rada of Ukraine through the activities of relevant committees. The President of Ukraine implements strategic leadership in this area, in particular through the National Security and Defense Council of Ukraine, which coordinates the actions of executive bodies. The Cabinet of Ministers of Ukraine is responsible for the formation and implementation of state information policy, the development of programs for the protection of the information space and digital transformation. Important executive structures in the field of information security are the Security Service of Ukraine, the Ministry of Defense of Ukraine, the Ministry of Digital Transformation, the National Institute for Strategic Studies and other bodies, each of which performs specific tasks within the framework of the national security system.

The paper outlines problems in the area of interagency cooperation, including fragmentation of functions, duplication of powers, insufficient coordination, weak participation of local governments, staff shortages, and regulatory gaps. The authors emphasize that in the context of modern information warfare, effective information security management requires a unified strategic vision, coordinated actions of all state actors, and broad involvement of civil society.

A set of practical measures to improve institutional interaction in the field of information security is proposed: development of a single state strategy with a clear division of powers, creation of joint analysis and operational response centers, strengthening strategic communications, development of digital security infrastructure, training of personnel and increasing

public transparency. All this should contribute to the formation of an effective, coordinated, sustainable system for protecting the information space of Ukraine.

Key words: national security, information security, public authorities, information space, state policy, interagency interaction, cyber threats, disinformation, strategic communications.

Постановка проблеми. В умовах інформаційного суспільства та цифровізації всієї сфери суспільного життя інформаційний простір набуває стратегічного значення для забезпечення національної безпеки. Україна, яка перебуває в стані гібридної війни, зіштовхується з безпрецедентними загрозами у сфері інформаційної безпеки, серед яких — кібератаки, дезінформація, інформаційно-психологічний вплив з боку ворожих держав, маніпуляції громадською думкою через цифрові платформи.

Попри існування нормативно-правової бази, питання ефективної участі органів публічної влади у формуванні та реалізації державної політики в інформаційному просторі залишається відкритим. Спостерігається недостатній рівень координації між державними структурами, фрагментарність управлінських рішень, обмежена кадрова та технологічна спроможність, а також недосконаліть стратегічного планування у сфері інформаційної безпеки.

Особливої уваги потребує інституційна взаємодія між ключовими суб'єктами публічної влади — Кабінетом Міністрів України, Міністерством цифрової трансформації, Службою безпеки України, Радою національної безпеки і оборони, а також органами місцевого самоврядування — з метою формування єдиного державного підходу до захисту інформаційного простору. Водночас важливою залишається проблема формування інформаційної культури серед громадян та забезпечення прозорої комунікації з суспільством.

Таким чином, актуальність дослідження полягає у необхідності наукового обґрунтування ролі органів публічної влади в реалізації політики національної безпеки в інформаційному просторі, виявлення існуючих прогалин та розробки ефективних управлінських і правових механізмів для протидії сучасним загрозам.

Аналіз останніх досліджень та публікацій. Питанням формування та реалізації політики національної безпеки в інформаційному просторі присвячено праці науковців, таких як: В. Антонюк, І. Березовська, О. Дзьобань, І. Кушнір, А. Марущак, О. Довгань, В. Негодченко, О. Олійник, В. Пилипчук, Д. Русак, Д. Федченко, В. Фурашев, В. Шеломенцев та ін.

Метою статті є визначення ролі органів публічної влади у формуванні та реалізації політики національної безпеки України в інформаційному просторі, аналіз сучасних викликів і проблем у сфері міжвідомчої взаємодії, а також обґрунтування напрямів удосконалення інституційного механізму забезпечення інформаційної безпеки держави в умовах гібридної війни та цифрових трансформацій.

Виклад основного матеріалу дослідження. Сучасні виклики у сфері національної безпеки України характеризуються значною активізацією загроз, пов'язаних з інформаційним впливом, кібератаками та масовим поширенням дезінформації, що робить питання інформаційної безпеки надзвичайно актуальним у політичному дискурсі. У цьому контексті особливої ваги набуває роль органів публічної влади як ключових суб'єктів формування та реалізації політики національної безпеки в інформаційному просторі.

Органи публічної влади в Україні діють відповідно до конституційно визначених повноважень і компетенцій, які дозволяють їм здійснювати нормативне регулювання, стратегічне планування, оперативне реагування на загрози та контроль за станом інформаційної безпеки. Зокрема, державну інформаційну політику та політику національної безпеки визначає Верховна Рада України, у складі якої діють такі профільні комітети: з питань свободи слова та інформаційної політики; з питань інформатизації та зв'язку; з питань національної безпеки і оборони [1; 2, с. 25]. Верховна Рада України виконує функцію законодавчого забезпечення політики національної безпеки, приймаючи нормативно-правові акти, що регулюють діяльність суб'єктів інформаційної сфери, визначають стандарти інформаційного захисту та відповідальність за порушення інформаційної безпеки.

Президент України, як гарант державного суверенітету та територіальної цілісності, визначає засади внутрішньої і зовнішньої політики держави у сфері національної безпеки, у тому числі в інформаційному просторі. Через видання указів, затвердження стратегічних документів, призначення керівників органів безпеки та ініціювання рішень Ради національної безпеки і оборони України, Президент реалізує політичне керівництво у цій сфері. Президенту України також підпорядковуються: Національний інститут стратегічних досліджень. Апарат РНБО України координує діяльність Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при РНБО України та зазначених науково-дослідних установ стратегічного рівня [3].

Кабінет Міністрів України (уповноважено на забезпечення формування та реалізацію інформаційної політики держави, забезпечення інформаційного суверенітету, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує і координує роботу міністерств, інших органів виконавчої влади у цій сфері) [4, с. 610].

Центральне місце у системі координації дій з протидії загрозам в інформаційному просторі посідає Рада національної безпеки і оборони України. Вона первинно, координує діяльність органів виконавчої влади з метою реалізації та гарантування інформаційної безпеки, шляхом застосування можливостей Центру протидії дезінформації [4; 5], що є його робочим органом, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії

дезінформації» [4; 6]. До основних завдань вказаного спеціального органу віднесено: аналіз та моніторинг подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі; виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, чинників, які впливають на їх формування, прогнозування та оцінка наслідків для безпеки національних інтересів України; виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою; участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку; участь у створенні інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них тощо [4; 7].

Окрему роль у формуванні та реалізації політики відіграють спеціалізовані органи. Зокрема, Служба безпеки України здійснює моніторинг спеціальними методами й способами вітчизняних та іноземних засобів масової інформації та мережі інтернет із метою виявлення загроз національній безпеці України в інформаціцйній сфері; пртидіє проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності в України, загострення суспільно-політичної та соціально-економічної ситуацій; здійснює попередження, виявлення, припинення та розкриття злочинів проти миру й безпеки людства, які вчиняються в кіберпросторі, контррозвідувальні й оперативно- розшукові заходи, спрямовані на боротьбу з кібертероризмом і кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцедентів; притидіє кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтереспм України; здійснює розслідуввання кіберінцедентів і кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на комп'ютерні інцеденти у сфері державної безпеки [8, с. 44; 9].

Міністерство оборони України та Генеральний штаб Збройних Сил України здійснюють інформаційно-психологічні операції, спрямовані на протидію інформаційній агресії та забезпечення морально-психологічної стійкості населення і військовослужбовців.

Вагомим інструментом реалізації політики у сфері безпеки є Міністерство цифрової трансформації України, яке забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії [10, с. 97].

Короткий аналіз повноважень і функцій органів публічної влади у сфері формування та реалізації політики національної безпеки в інформаційному просторі засвідчує наявність розгалуженої системи управління, що охоплює як органи законодавчої, виконавчої влади, так і спеціалізовані структури безпекового призначення. Кожен із цих органів виконує важливу роль у забезпеченні інформаційного суверенітету держави, протидії інформаційним загрозам та формуванні сучасної цифрової держави.

Водночас, на нашу думку є низка проблем у взаємодії між цими органами, які стримують ефективність державної політики у сфері інформаційної безпеки:

- фрагментарність та дублювання функцій — частина повноважень різних органів перетинається, що створює конкуренцію замість координації (особливо між СБУ, РНБО, Міністерством цифрової трансформації та іншими виконавчими структурами).

- недостатня міжвідомча координація — незважаючи на координаційну роль РНБО та створення Центру протидії дезінформації, досі спостерігається відсутність ефективного механізму оперативного обміну інформацією та узгоджених дій між відомствами.

- слабка інституційна спроможність на місцевому рівні — органи місцевого самоврядування практично не залучені до реалізації заходів інформаційної безпеки, попри їхню потенційну важливість у протидії деструктивному впливу в регіонах.

- нестача висококваліфікованих кадрів у сфері кібербезпеки та цифрової політики — кадрова проблема залишається критичною для швидкої адаптації до новітніх інформаційних загроз.

- обмежена нормативна база у сфері стратегічних комунікацій — не забезпечено чіткого розмежування функцій з комунікації між державою та суспільством у кризових інформаційних ситуаціях.

- відсутність єдиної державної стратегії інформаційної безпеки з чіткими індикаторами ефективності — існують концептуальні документи, проте їх реалізація не має належної узгодженості між усіма суб’єктами безпекового сектору.

Таким чином, удосконалення взаємодії між органами публічної влади, створення ефективного інституційного механізму управління в інформаційному просторі мають стати пріоритетом для державної політики національної безпеки України.

Для удосконалення взаємодії органів публічної влади у сфері формування та реалізації політики

національної безпеки в інформаційному просторі доцільно розробити єдину державну стратегію інформаційної безпеки з чітким розмежуванням повноважень і відповідальності, посилити міжвідомчу координацію через створення спільних аналітичних центрів, запровадити інституційний механізм стратегічних комунікацій, врегулювати на законодавчому рівні порядок взаємодії між центральними й місцевими органами влади, а також залучити громадянське суспільство до інформаційного спротиву. Важливими є розвиток національної цифрової інфраструктури безпеки, підготовка кадрів у сфері кіберзахисту, підвищення прозорості та публічності дій державних структур, що в комплексі забезпечить ефективне управління загрозами в інформаційному середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Прав Р.Ю. Діяльність суб'єктів формування і реалізації політики державної безпеки в інформаційній сфері України. *Електронний журнал «Державне управління: удосконалення та розвиток».* 2018. №9. URL: http://www.dy.nayka.com.ua/?n=9&y=2018

2. Пилипчук В. Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти матеріали наук.-практ. конф.* / 06 жовт. 2016 р. / Упоряд. : В. М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка». 2016. С. 24-28.

3. Антонюк В.В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. *Електронний журнал «Державне управління: удосконалення та розвиток».* 2014. №8. URL: http://www.dy.nayka.com.ua/?op=1&z=747

4. Цибульник Н.Ю. Інформаційно-правова характеристика основних складових сектору безпеки держави. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2023. Випуск 80: частина 1. С. 607-612.

5. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

6. Офіційний сайт Центру протидії дезінформації при Раді національної безпеки та оборони України. URL: https://cpd.gov.ua/category/documents/

7. Питання Центру протидії дезінформації: Указ Президента України від 07.05.2021 р. № 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text

8. Ткачук Т. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Національний юридичний журнал: теорія і практика.* 2017. №6. Ч.2 С. 42-46

9. Про Службу безпеки України: Закон України від 25 березня 1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

10. Троянський О.А. Інформаційна безпека в Україні: сучасний стан та перспективи розвитку. *Науковий вісник Льотної академії. Серія: Економіка, менеджмент та право.* 2021. Випуск 5. С. 185-194.

REFERENCES:

1. Prav, R.Iu. (2018). Diialnist subiektiv formuvannia i realizatsii polityky derzhavnoi bezpeky v informatsiinii sferi Ukrainy. [Activities of entities involved in the formation and implementation of state security policy in the information sphere of Ukraine]. *Elektronnyi zhurnal «Derzhavne upravlinnia: udoskonalennia ta rozvytok». №9.* Retrieved from: http://www.dy.nayka.com.ua/?n=9&y=2018 [in Ukrainian].

2. Pylypchuk, V.H. (2016, October 6). Zabezpechennia informatsiinoi bezpeky Ukrainy: suchasni tendentsii ta problemy. [Ensuring information security in Ukraine: current trends and problems]. *Zapobihannia novym vyklykam ta zahrozam informatsiinii bezpetsi Ukrainy: pravovi aspekty: materialy nauk.-prakt. konf.* Kyiv. NTUU «KPI imeni Ihoria Sikorskoho», Vyd-vo «Politekhnika». 24-28. [in Ukrainian].

3. Antoniuk, V.V. (2014). Mekhanizmy derzhavnoho reahuvannia na suchasni vyklyky ta zahrozy informatsiinii bezpetsi. [Mechanisms of state response to modern challenges and threats to information security]. *Elektronnyi zhurnal «Derzhavne upravlinnia: udoskonalennia ta rozvytok». №8.* Retrieved from: http://www.dy.nayka.com.ua/?op=1&z=747 [in Ukrainian].

4. Tsybulnyk, N.Iu. (2023). Informatsiino-pravova kharakterystyka osnovnykh skladovykh sektoru bezpeky derzhavy. [Information and legal characteristics of the main components of the state security sector]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia PRAVO. Vypusk 80: chastyna 1.* 607-612. [in Ukrainian].

5. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky». (2021, December 28). [On the decision of the National Security and Defense Council of Ukraine of October 15, 2021 "On the Information Security Strategy"]. *Ukaz Prezydenta Ukrainy №685/2021.* Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].

6. Tsentr protydii dezinformatsii pry Radi natsionalnoi bezpeky ta oborony Ukrainy. (2024). [Center for Countering Disinformation at the National Security and Defense Council of Ukraine]. *Ofitsiinyi sait.* Retrieved from: https://cpd.gov.ua/category/documents/ [in Ukrainian].

7. Pytannia Tsentru protydii dezinformatsii. (2021, May 7). [Questions from the Center for Countering Disinformation]. *Ukaz Prezydenta Ukrainy №187/2021.* Retrieved from: https://zakon.rada.gov.ua/laws/show/187/2021#Text [in Ukrainian].

8. Tkachuk, T. (2017). Subiekty zabezpechennia informatsiinoi bezpeky derzhavy: funktsionalnyi analiz. [Subjects of ensuring state information security: functional analysis]. *Natsionalnyi yurydychnyi zhurnal: teoriia i praktyka. №6. Ch.2* 42-46. [in Ukrainian].

9. Pro Sluzhbu bezpeky Ukrainy. (1992, March 25). [On the Security Service of Ukraine]. *Zakon Ukrainy №2229-XII.* Retrieved from: https://zakon.rada.gov.ua/laws/show/2229-12#Text [in Ukrainian].

10. Troianskyi, O.A. (2021). Informatsiina bezpeka v Ukraini: suchasnyi stan ta perspektyvy rozvytku. [Information security in Ukraine: current state and development prospects]. *Naukovyi visnyk Lotnoi akademii. Seriia: Ekonomika, menedzhment ta pravo. Vypusk 5.* 185-194. [in Ukrainian].

Стаття надійшла до редакції 1.12.2024