11. Pro utvorennia terytorialnykh orhaniv Derzhavnoi sluzhby z pytan bezpechnosti kharchovykh produktiv ta zakhystu spozhyvachiv. (2015, December 16). *Postanova Kabinetu Ministriv Ukrainy* № 1092. Retrieved from: https://zakon.rada.gov.ua/laws/show/1092-2015-%D0%BF#Text [in Ukrainian].

12. Svitlychnyi, O.P. (2017). Sluzhbove pravo: vytoky, suchasnist ta perspektyvy rozvytku. kolektyvna monohrafiia / za zah. red. T.O. Kolomoiets, V.K. Kolpakova. Zaporizhzhia: Vydavnychyi dim «Helvetyka». 205–217. [in Ukrainian].

13. Sukmanova O.V. (2018). Poniattia ta systema subiektiv publichnoho administruvannia okhorony prava vlasnosti v Ukraini. [Concept and system of subjects of public administration of property rights protection in Ukraine]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu.* Seriia: Yurysprudentsiia. *№ 33.* 64-67. [in Ukrainian].

14. Shestak V.S. (2015). Rol administratyvnoho prava u pravovomu zabezpechenni realizatsii okremykh funktsii derzhavy subiektamy publichnoho upravlinnia (na prykladi kulturnoi funktsii). [The role of administrative law in legal provision of some state functions realization by subjects of public management (based on the cultural function example)]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. № 34(2).* 151–154. [in Ukrainian].

Стаття надійшла до редакції 9.06.2025

УДК 351.862:004.738.5
DOI: 10.36550/2522-9230-2025-18-164-167

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

РОЛЬ РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ У ФОРМУВАННІ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті здійснено комплексний аналіз інституційної ролі Ради національної безпеки і оборони України (РНБО) у формуванні та реалізації державної політики у сфері інформаційної безпеки в умовах зростаючих викликів гібридної війни, інформаційно-психологічного впливу та кіберзагроз. Автором розкрито правову основу функціонування РНБО як координаційного центру з питань національної безпеки, зокрема в інформаційній сфері, з урахуванням норм Конституції України та профільного законодавства. Визначено основні функції РНБО у зазначеній сфері, серед яких: стратегічне планування, міжвідомча координація, аналітичне забезпечення, ініціювання нормативно-правових змін та оперативне реагування на загрози в інформаційному просторі.

Особливу увагу приділено діяльності Національного координаційного центру кібербезпеки як робочого органу РНБО, що відіграє ключову роль у моніторингу, оцінці та нейтралізації кіберінцидентів. Розглянуто функціональні завдання НКЦК, включно з управлінням національною системою кіберзахисту, координацією міждержавної інформаційної взаємодії, обміном даними між суб'єктами кібербезпеки та приватним сектором. Проаналізовано інституційні механізми взаємодії РНБО з основними суб'єктами сектору безпеки і оборони України, такими як Служба безпеки України, Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації України, Міністерство цифрової трансформації тощо.

Окремо висвітлено питання удосконалення інституційної діяльності РНБО в умовах інформаційної агресії з боку російської федерації, що проявляється у системному поширенні фейкових наративів та маніпулятивної інформації. Автор підкреслює, що вказані загрози зумовлюють необхідність поглиблення стратегічного підходу до інформаційної безпеки на державному рівні. У цьому контексті обґрунтовано доцільність оновлення нормативно-правової бази, впровадження нових стандартів інформаційної безпеки, активізації аналітичної діяльності РНБО, створення національних технологічних рішень для захисту інформаційної інфраструктури. Зроблено висновок про те, що лише за умов комплексного, міжвідомчо скоординованого підходу РНБО може ефективно виконувати свою роль у забезпеченні інформаційної безпеки, зокрема шляхом аналітичного прогнозування загроз, нормативного регулювання та інституційної інтеграції вітчизняної системи кіберзахисту в міжнародні безпекові формати.

Ключові слова: Рада національної безпеки і оборони України, інформаційна безпека, кібербезпека, стратегія національної безпеки, інформаційна політика, гібридна війна, Національний координаційний центр кібербезпеки, державне управління.

Krushenitskyi V. THE ROLE OF THE NATIONAL SECURITY AND DEFENSE COUNCIL OF UKRAINE IN FORMING STATE INFORMATION SECURITY POLICY

The article provides a comprehensive analysis of the institutional role of the National Security and Defense Council of Ukraine (NSDC) in the formation and implementation of state policy in the field of information security in the context of the growing challenges of hybrid warfare, information and psychological influence and cyber threats. The author reveals the legal

basis for the functioning of the NSDC as a coordination center for national security issues, in particular in the information sphere, taking into account the norms of the Constitution of Ukraine and relevant legislation. The main functions of the NSDC in this area are identified, including: strategic planning, interagency coordination, analytical support, initiation of regulatory and legal changes and prompt response to threats in the information space.

Particular attention is paid to the activities of the National Cybersecurity Coordination Center as a working body of the National Security and Defense Council, which plays a key role in monitoring, assessing and neutralizing cyber incidents. The functional tasks of the NCSC are considered, including managing the national cyber defense system, coordinating interstate information interaction, and exchanging data between cybersecurity entities and the private sector. The institutional mechanisms of interaction of the NSDC with the main entities of the security and defense sector of Ukraine, such as the Security Service of Ukraine, the Ministry of Defense, the State Service for Special Communications and Information Protection of Ukraine, the Ministry of Digital Transformation, etc. are analyzed.

The issue of improving the institutional activities of the NSDC in the context of information aggression from the Russian Federation, which is manifested in the systematic spread of fake narratives and manipulative information, is separately highlighted. The author emphasizes that these threats necessitate a deepening of the strategic approach to information security at the state level. In this context, the feasibility of updating the regulatory framework, implementing new information security standards, intensifying the analytical activities of the NSDC, and creating national technological solutions for protecting information infrastructure is substantiated. The conclusion is made that only under the conditions of a comprehensive, interdepartmental coordinated approach can the NSDC effectively fulfill its role in ensuring information security, in particular through analytical threat forecasting, regulatory regulation, and institutional integration of the domestic cyber defense system into international security formats.

Keywords: National Security and Defense Council of Ukraine, information security, cybersecurity, national security strategy, information policy, hybrid warfare, National Cybersecurity Coordination Center, public administration.

Постановка проблеми. У сучасних умовах повномасштабної агресії російської федерації проти України, а також глобального поширення гібридних загроз, питання забезпечення інформаційної безпеки набуло першочергового значення в системі національної безпеки держави. Інформаційний простір перетворився на один із ключових театрів бойових дій, де ворог активно застосовує інструменти дезінформації, інформаційно-психологічного впливу, кібератак та пропаганди з метою дестабілізації суспільства, підриву довіри до державних інституцій та дискредитації української державності на міжнародній арені.

У цьому контексті особливої ваги набуває діяльність Ради національної безпеки і оборони України (РНБО) як координаційного органу, що визначає стратегічні пріоритети, ініціює ключові політичні рішення у сфері національної безпеки, а також впливає на формування інформаційної політики держави. Водночас, попри активізацію РНБО у питаннях інформаційної та кібербезпеки в останні роки, все ще залишається низка невирішених проблем, зокрема: відсутність сталої концепції інформаційної безпеки, недостатня міжвідомча координація, фрагментарність законодавчої бази та обмежена прозорість ухвалених рішень.

Отже, постає необхідність системного аналізу ролі РНБО у формуванні державної політики інформаційної безпеки, оцінки її ефективності, виявлення наявних викликів і розробки практичних рекомендацій щодо вдосконалення механізмів управління у цій сфері. Дослідження цієї проблематики є актуальним не лише в контексті воєнного часу, а й з огляду на потребу створення довгострокової стратегії інформаційної стійкості України.

Аналіз останніх досліджень та публікацій. Питання інформаційної безпеки привертають значну увагу вітчизняних науковців. Серед вчених слід відзначити дослідження таких вчених, як О. Сосніна, В.Грубова, В. Домарьова, О. Дрозда, В. Ліпкана, В. Косевцова, І. Бінько, В. Мунтіян, Г. Почепцова, О.Литвиненко та інших.

Мета статті полягає в тому, щоб проаналізувати інституційну роль Ради національної безпеки і оборони України у формуванні та реалізації державної політики у сфері інформаційної безпеки, а також обґрунтувати напрями удосконалення її діяльності в умовах сучасних інформаційних і кібернетичних загроз.

Виклад основного матеріалу дослідження. РНБО України виступає центральною ланкою в системі координації заходів із забезпечення національної безпеки в умовах сучасної інформаційної війни. Її функціональний статус визначено у ст. 107 Конституції України [1] та Законі України «Про Раду національної безпеки і оборони України» [2], згідно з якими цей орган забезпечує підготовку рішень щодо всіх ключових напрямів безпеки, включно з інформаційною.

У контексті інформаційної безпеки РНБО виконує стратегічну, координуючу, аналітичну та регуляторну функції. Вона формує концептуальні засади державної інформаційної політики, ініціює розробку програмних документів (зокрема Стратегії інформаційної безпеки) [3], визначає пріоритетні напрямки діяльності у сфері протидії інформаційним загрозам, а також ухвалює рішення, які мають обов’язковий характер після введення їх у дію указом Президента України.

У межах своїх повноважень РНБО здійснює аналіз стану і можливих загроз національній безпеці України в інформаційній сфері; аналіз здійснення галузевих програм і виконання заходів, пов'язаних із реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в інформаційній сфері; розроблення і внесення Президентові України та Раді національної безпеки і оборони України пропозицій в інформаційній сфері; удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України (в тому числі альтернативною інформацією) у сфері

національної безпеки і оборони та інші функції [4]

Таким чином, РНБО виступає центральним органом стратегічного управління інформаційною безпекою, здатним оперативно реагувати на загрози, координувати зусилля державних інституцій і формувати ефективну політику в умовах сучасної гібридної війни.

Робочим органом Ради національної безпеки і оборони України є Національний координаційний центр кібербезпеки утворений відповідно до рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведений в дію Указом Президента України від 15 березня 2016 року № 96 [5]. Його функції включають: оперативний аналіз кіберзагроз; формування рекомендацій для органів виконавчої влади та приватного сектору; управління загальнодержавною системою кіберзахисту; забезпечення обміну інформацією між ключовими учасниками кіберпростору.

Завдяки цьому інструменту РНБО має змогу оперативно впливати на хід інформаційних операцій, здійснювати превентивні заходи, підтримувати кіберстійкість державної ІТ-інфраструктури.

Також, досліджуючи дане питання, зупинемося на міжвідомчій співпраці РНБО з іншими органами у сфері інформаційної безпеки.

Зокрема, однією з найважливіших інституційних ролей РНБО є забезпечення ефективної міжвідомчої взаємодії, яка координує діяльність таких органів: Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку); Міністерства цифрової трансформації України; Служби безпеки України; Міністерства оборони України та Генерального штабу ЗСУ.

РНБО забезпечує не лише формальну взаємодію між вказаними структурами, а й організацію спільних засідань, узгодження стратегічних документів, інтеграцію інформаційних систем і впровадження єдиних стандартів безпеки. Особливе значення має координація при реагуванні на масштабні кібератаки та під час надзвичайних ситуацій — саме тоді активізуються механізми кризового управління під безпосереднім керівництвом РНБО.

Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки було одноголосно затверджено ще на засіданні Національного координаційного центру кібербезпеки 22 вересня 2022 року [6].

Документ розроблено створеною при ньому робочою групою, до складу якої увійшли представники всіх основних суб'єктів національної системи кібербезпеки, а також Мінцифри, МЗС та Національного інституту стратегічних досліджень [6].

Даним порядком взаємодії, з-поміж іншого, передбачено створити постійну Об'єднану групу реагування на кіберінциденти та кібератаки, та врегульовано питання інформаційного обміну, координації та спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки [6].

У світлі загострення інформаційної агресії з боку російської федерації, Рада національної безпеки і оборони України посилює свою стратегічну та координаційну функцію у сфері протидії зовнішнім дестабілізуючим впливам. РНБО фіксує систематичне поширення росією викривленої, неповної та маніпулятивної інформації щодо України як на внутрішньому, так і на міжнародному рівнях.

У відповідь на такі виклики РНБО ініціює масштабний перегляд та оновлення нормативно-правової бази у сфері інформаційної безпеки, зокрема шляхом доручень Кабінету Міністрів України щодо розробки нових стратегій, законодавчих ініціатив та організаційних заходів. Йдеться, зокрема, про формування комплексної стратегії інформаційної політики [7, с. 572]. РНБО також ініціює створення умов для появи національних технологічних рішень, таких як безпечна операційна система, вітчизняне антивірусне програмне забезпечення тощо.

Таким чином, у сучасних умовах трансформації безпекового середовища та зростання кількості інформаційних і кібернетичних загроз актуалізується необхідність удосконалення інституційної діяльності Ради національної безпеки і оборони України (РНБО) у сфері забезпечення інформаційної безпеки. Як координуючий орган у системі національної безпеки, РНБО має відігравати провідну роль у формуванні стратегічних підходів до протидії дезінформації, інформаційно-психологічному впливу, кібератакам та іншим формам інформаційного тиску. Одним із ключових напрямів вдосконалення діяльності РНБО є посилення її аналітичної спроможності. З метою своєчасного виявлення, моніторингу та прогнозування загроз інформаційного характеру доцільним є створення спеціалізованих структурних підрозділів в Апараті РНБО, що здійснюватимуть комплексний аналіз інформаційної ситуації в державі. Важливим компонентом цього процесу є впровадження системи постійного моніторингу національного інформаційного простору, зокрема традиційних ЗМІ, соціальних мереж, цифрових платформ тощо, а також інтеграція інформації з різних джерел — державних, неурядових та міжнародних — задля формування достовірної інформаційно-аналітичної бази.

Наступним напрямом удосконалення діяльності РНБО виступає оновлення нормативно-правової бази, що регламентує її повноваження у сфері інформаційної безпеки. Зокрема, потребує законодавчого уточнення компетенція РНБО щодо координації дій органів виконавчої влади у випадках інформаційних атак чи кризових ситуацій в інформаційній сфері. Необхідно розробити чіткі механізми виявлення та нейтралізації дезінформації, а також механізми відповідальності за участь у її поширенні. Важливим кроком є також гармонізація національного законодавства з міжнародними стандартами та практиками держав-членів ЄС і НАТО, що сприятиме підвищенню ефективності державної інформаційної політики.

Окрему увагу слід приділити удосконаленню міжвідомчої координації, яка має здійснюватися під егідою РНБО. У цьому контексті важливою є ефективна взаємодія з іншими суб'єктами сектору безпеки і оборони — Службою безпеки України, Міністерством оборони, Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією та іншими структурами. Важливим інституційним елементом у цій системі виступає Національний координаційний центр кібербезпеки при РНБО, який потребує подальшого зміцнення як основний орган оперативного реагування на кіберзагрози. Також доцільною є активізація співпраці РНБО з науковими установами, аналітичними центрами, експертним середовищем та громадськими організаціями, що дозволить не лише розширити інформаційно-аналітичну базу, але й сприяти розробці превентивних стратегій у сфері інформаційної безпеки.

Висновок. Отже, вдосконалення інституційної діяльності РНБО у сфері інформаційної безпеки має відбуватися шляхом комплексного підходу, що охоплює аналітичний, нормативно-правовий та координаційний виміри. Такий підхід дозволить не лише ефективно протидіяти сучасним інформаційним загрозам, а й забезпечити стратегічну стійкість держави в умовах гібридної війни та постійного інформаційного тиску.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80

2. Про Раду національної безпеки і оборони України: Закон України від 5 березня 1998 р. № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

3. Стратегія інформаційної безпеки від 28 грудня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7

4. 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

5. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Diialnist/3303.html

6. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки одноголосно затверджено на засіданні НКЦК. URL: https://www.rnbo.gov.ua/ua/Diialnist/5765.html

7. Дрозд О.Ю. Розвиток інформаційного суспільства: виклики державної інформаційної політики. *Юридичний науковий електронний журнал.* 2025. №1. С. 570-572.

REFERENCES:

1. Konstytutsiia Ukrainy. (1996, June 28). [Constitution of Ukraine]. *Zakon №254k/96-VR.* Retrieved from: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 [in Ukrainian].

2. Pro Radu natsionalnoi bezpeky i oborony Ukrainy. (1998, March 5). [On the National Security and Defense Council of Ukraine]. Zakon Ukrainy №183/98-VR. Retrieved from:https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text [in Ukrainian].

3. Stratehiia informatsiinoi bezpeky. (2021, December 28). [Information security strategy]. *Ukaz Prezydenta Ukrainy №685/2021.* Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#n7 [in Ukrainian].

4. 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].

5. Rada natsionalnoi bezpeky i oborony Ukrainy. (2019) [National Security and Defense Council of Ukraine]. Retrieved from: https://www.rnbo.gov.ua/ua/Diialnist/3303.html [in Ukrainian].

6. Poriadok vzaiemodii subiektiv zabezpechennia kiberbezpeky pid chas reahuvannia na kiberintsydenty/kiberataky odnoholosno zatverdzheno na zasidanni NKTsK. (2022, September 28). [The procedure for interaction between cybersecurity entities when responding to cyber incidents/cyber attacks was unanimously approved at a meeting of the NCCC]. Retrieved from: https://www.rnbo.gov.ua/ua/Diialnist/5765.html [in Ukrainian].

7. Drozd, O.Iu. (2025). Rozvytok informatsiinoho suspilstva: vyklyky derzhavnoi informatsiinoi polityky. [Development of the information society: challenges of state information policy]. *Yurydychnyi naukovyi elektronnyi zhurnal. №1.* 570-572. [in Ukrainian].

Стаття надійшла до редакції 3.06.2025