| | |
|---|---|
| **Секція Право** | |
| **УДК 351.746.1:351.86:004.738.5** | |
| **Дата першого надходження статті до видання** | 2026-04-30 |
| **Дата прийняття статті до друку після рецензування** | 2026-05-30 |
| **Дата публікації/оприлюднення** | 2026-05-30 |

# Рада національної безпеки і оборони України як чинник забезпечення інформаційної безпеки

**Мосенко Юлія Олександрівна**
кандидат юридичних наук,
Університет Свансі, Свансі, Об'єднане Королівство
e-mail: yuliamosenko@gmail.com
https://orcid.org/0009-0003-6515-2881

**Анотація.** Рада національної безпеки і оборони України (РНБО) відіграє ключову роль у формуванні та реалізації державної політики у сфері інформаційної безпеки. В умовах сучасних гібридних загроз, зокрема інформаційних війн, кібератак та дезінформаційних кампаній, діяльність РНБО набуває особливого значення як координаційного та стратегічного органу при Президентові України. Основною функцією РНБО є забезпечення узгодженості дій органів виконавчої влади у сфері національної безпеки, що включає й інформаційний компонент.

Метою дослідження є визначення ролі та значення РНБО України у системі забезпечення інформаційної безпеки держави, а також аналіз основних напрямів її діяльності у цій сфері.

Методи дослідження включають аналіз нормативно-правових актів, системний підхід до оцінки функцій РНБО та узагальнення наукових джерел щодо проблематики інформаційної безпеки.

Інформаційна безпека охоплює захист національного інформаційного простору, протидію інформаційним впливам з боку іноземних держав, а також забезпечення доступу громадян до достовірної інформації. У цьому контексті РНБО виступає важливим інституційним механізмом, який визначає пріоритети державної політики, розробляє відповідні стратегії та контролює їх виконання. Значну увагу приділено питанням кібербезпеки, захисту критичної інформаційної інфраструктури та боротьбі з пропагандою. Важливим інструментом діяльності РНБО є застосування санкцій щодо суб'єктів, які створюють загрози інформаційній безпеці.

Основні результати дослідження полягають у визначенні ключових функцій РНБО у сфері інформаційної безпеки, зокрема координації державних органів, стратегічного планування та контролю за виконанням рішень. Встановлено, що ефективність діяльності РНБО значною мірою впливає на рівень стійкості держави до інформаційних загроз. Обґрунтовано важливість інтегрованого підходу до забезпечення інформаційної безпеки. Також виявлено актуальні виклики, що потребують удосконалення механізмів державного управління у цій сфері.

**Ключові слова:** інформаційна безпека, виконавча влада, державна політика, нацiаональна безпека, пропаганда, кібербезпека


e-ISSN: 2786-586X

# The National Security and Defense Council of Ukraine as a factor in ensuring information security

**Mosenko Yuliia**
PhD
PhD, Swansea University, Swansea, United Kingdom
e-mail: yuliamosenko@gmail.com
https://orcid.org/0009-0003-6515-2881

**Abstract.** The National Security and Defense Council of Ukraine (NSDC) plays a key role in the formation and implementation of state policy in the field of information security. In the context of modern hybrid threats, in particular information wars, cyberattacks and disinformation campaigns, the activities of the NSDC are of particular importance as a coordinating and strategic body under the President of Ukraine. The main function of the NSDC is to ensure the coherence of actions of executive bodies in the field of national security, which includes the information component.

The purpose of the study is to determine the role and significance of the NSDC of Ukraine in the system of ensuring the information security of the state, as well as to analyze the main areas of its activity in this area.

The research methods include the analysis of regulatory legal acts, a systematic approach to assessing the functions of the NSDC and the generalization of scientific sources on the issues of information security.

Information security covers the protection of the national information space, counteraction to information influences from foreign states, as well as ensuring citizens' access to reliable information. In this context, the NSDC acts as an important institutional mechanism that determines state policy priorities, develops relevant strategies and monitors their implementation. Considerable attention is paid to issues of cybersecurity, protection of critical information infrastructure and combating propaganda. An important tool of the NSDC's activities is the application of sanctions against entities that pose threats to information security.

The main results of the study are to identify the key functions of the NSDC in the field of information security, in particular, coordination of state bodies, strategic planning and control over the implementation of decisions. It has been established that the effectiveness of the NSDC's activities significantly affects the level of state resilience to information threats. The importance of an integrated approach to ensuring information security is substantiated. Current challenges that require improvement of state governance mechanisms in this area have also been identified.

**Keywords:** information security, executive branch, public policy, national security, propaganda, cybersecurity.

## Вступ

**Актуальність проблеми.** В умовах триваючої збройної агресії проти України та активного використання інформаційних операцій як інструменту гібридної війни питання забезпечення інформаційної безпеки набуває критичного значення. Зокрема, поширення дезінформації, кібератаки на об’єкти критичної інфраструктури, а також маніпулятивний вплив через цифрові платформи створюють реальні загрози національній безпеці. За даними міжнародних досліджень у сфері кібербезпеки, кількість кібератак на державні інформаційні системи України зросла у декілька разів протягом останніх років, що потребує ефективної координації з боку державних


e-ISSN: 2786-586X

інституцій. У цьому контексті особливого значення набуває діяльність Ради національної безпеки і оборони України як ключового органу стратегічного управління у сфері інформаційної безпеки.

**Аналіз останніх досліджень і публікацій.**

Проблематика забезпечення інформаційної безпеки держави в сучасних умовах є предметом активних наукових досліджень представників юридичної, політичної та безпекової науки. Особливої актуальності вона набула в умовах російської збройної агресії проти України, коли інформаційний простір перетворився на один із ключових театрів протиборства. У науковій літературі досліджуються як теоретико-правові засади інформаційної безпеки, так і інституційні механізми її забезпечення, роль державних органів, питання кібербезпеки, стратегічних комунікацій та міжвідомчої взаємодії.

Значна група науковців зосереджує увагу на інституційному забезпеченні державної політики інформаційної безпеки. Так, В. Крушеніцький наголошує на ключовій ролі Ради національної безпеки і оборони України у координації діяльності суб'єктів сектору безпеки та оборони, обґрунтовуючи необхідність посилення міжвідомчої взаємодії та зміцнення потенціалу Національного координаційного центру кібербезпеки. Розвиваючи цей підхід, автор також акцентує увагу на потребі формування єдиної державної стратегії інформаційної безпеки, чіткому розмежуванні повноважень органів публічної влади та запровадженні ефективних механізмів стратегічних комунікацій.

Окремий напрям досліджень стосується впливу інституційних чинників на формування інформаційно-безпекової політики держави. В. Галіпчак та Н. Ротар доводять, що в умовах воєнного стану ефективність інформаційної безпеки визначається не лише нормативно-правовими або технологічними інструментами, а й рівнем суспільної довіри до державних інститутів, якістю комунікації між владою та громадянами, а також здатністю держави формувати стійкі національні наративи. У цьому контексті інформаційна безпека розглядається як важливий елемент забезпечення інформаційного суверенітету та суспільної стійкості.

Помітне місце у сучасних наукових дослідженнях займають питання теоретичного осмислення сутності інформаційної безпеки. М. Гончаров та А. Гончаров розглядають її як складне багатовимірне явище, що охоплює різні сфери суспільного життя та забезпечує правомірне володіння, використання і поширення інформації. На думку авторів, ефективна реалізація державної політики у цій сфері потребує вдосконалення організаційно-правових механізмів, кадрового забезпечення та подолання суперечностей між суб'єктами інформаційних відносин. Водночас дослідники підкреслюють важливість формування єдиного понятійного апарату та розвитку теоретичних засад інформаційної безпеки як самостійного напряму наукових досліджень.

Вагомий внесок у розвиток правового забезпечення інформаційної безпеки здійснили О. Довгань та Т. Ткачук. Науковці обґрунтовують необхідність систематизації законодавства у цій сфері шляхом прийняття базового Закону України «Про інформаційну безпеку України», який має закріпити основні принципи, єдину термінологію та структуру нормативно-правового регулювання. Автори звертають увагу на фрагментарність чинного законодавства та необхідність його подальшої кодифікації в межах формування цілісної системи інформаційного права.

У сучасних дослідженнях значна увага приділяється також практичним аспектам забезпечення інформаційної безпеки, насамперед питанням кібербезпеки та діяльності правоохоронних органів. Д. Селіхов наголошує на існуванні системних проблем правового регулювання кібербезпеки, серед яких фрагментарність нормативної бази, дублювання повноважень суб'єктів забезпечення кіберзахисту та недостатній рівень координації між ними. Подібної позиції дотримуються А. Гарбінська-Руденко та М.


e-ISSN: 2786-586X

Кучко, які розглядають забезпечення інформаційної безпеки правоохоронними органами як один із ключових напрямів захисту національної безпеки в умовах зростання зовнішніх та внутрішніх загроз. Водночас Ю. Тимошенко та Д. Кисленко акцентують увагу на ролі поліції охорони як складової системи суб'єктів забезпечення інформаційної безпеки держави.

Проблематика інформаційної безпеки в умовах воєнного стану розкрита у працях Я. Лелет та О. Селецького. Дослідники підкреслюють, що сучасні інформаційні загрози виходять далеко за межі технічних аспектів захисту інформації та безпосередньо впливають на національну єдність, суспільну стійкість і здатність держави протидіяти гібридним загрозам. У їхніх роботах інформаційна безпека розглядається як невід'ємна складова національної безпеки, яка потребує комплексного поєднання правових, організаційних, технологічних та комунікаційних механізмів захисту.

Водночас у зарубіжних дослідженнях переважає підхід, за якого інформаційна безпека розглядається переважно через призму кібербезпеки та цифрової стійкості держави. Хоча такі підходи є важливими, вони не повною мірою враховують специфіку функціонування РНБО України як координаційного органу з особливим конституційним статусом. Таким чином, попри значний науковий доробок, питання ролі РНБО у забезпеченні інформаційної безпеки потребує подальшого комплексного дослідження.

Попри значну кількість наукових праць, присвячених окремим аспектам інформаційної безпеки, питання ролі Ради національної безпеки і оборони України як центрального координаційного суб'єкта формування та реалізації державної політики у цій сфері потребує подальшого комплексного дослідження. Недостатньо висвітленими залишаються проблеми взаємодії РНБО України з іншими суб'єктами сектору безпеки і оборони, механізми координації діяльності у сфері протидії інформаційним загрозам та напрями удосконалення інституційного забезпечення інформаційної безпеки держави в умовах воєнного стану.

**Виділення невирішеної частини проблеми.** Попри значний науковий доробок, невирішеним залишається питання комплексного визначення ролі Ради національної безпеки і оборони України як інституційного чинника забезпечення інформаційної безпеки в умовах сучасних гібридних загроз.

**Мета статті.** Метою статті є обґрунтування ролі Ради національної безпеки і оборони України як ключового інституційного суб'єкта забезпечення інформаційної безпеки держави.

**Наукова новизна.** Наукова новизна полягає у комплексному визначенні функцій РНБО України у сфері інформаційної безпеки, яке, на відміну від існуючих підходів, враховує сучасні гібридні загрози та міжвідомчу координацію як ключовий елемент ефективності.

**Практичне значення.** Практичне значення результатів полягає у можливості їх використання органами державної влади для вдосконалення механізмів забезпечення інформаційної безпеки, а також у науково-освітній діяльності при підготовці фахівців у сфері національної безпеки.

## Методологія

**Методи дослідження.** Методологічну основу дослідження становить сукупність загальнонаукових і спеціальних методів пізнання, що забезпечують комплексний аналіз ролі Ради національної безпеки і оборони України у сфері інформаційної безпеки. Застосовано системний метод для розгляду інформаційної безпеки як складної багаторівневої системи, а також структурно-функціональний підхід для визначення місця та повноважень РНБО у механізмі державного управління. Формально-юридичний метод використано для аналізу нормативно-правових актів, що регулюють діяльність


e-ISSN: 2786-586X

РНБО та сферу інформаційної безпеки. Крім того, застосовано метод узагальнення для формулювання теоретичних висновків.

**Джерела даних.** Інформаційну базу дослідження становлять нормативно-правові акти України, зокрема Конституція України, Закон України «Про національну безпеку України», укази Президента України та рішення РНБО. Використано також наукові праці вітчизняних дослідників у сфері національної та інформаційної безпеки, аналітичні матеріали, а також офіційні публікації державних органів.

**Інструменти аналізу.** У процесі дослідження використано інструменти контент-аналізу, логіко-аналітичного та структурно-функціонального аналізу. Контент-аналіз застосовано для опрацювання нормативно-правових актів, стратегічних документів, офіційних матеріалів Ради національної безпеки і оборони України та наукових публікацій з питань інформаційної безпеки. Логіко-аналітичні інструменти використано для виявлення закономірностей функціонування механізмів забезпечення інформаційної безпеки, встановлення взаємозв'язків між суб'єктами сектору безпеки і оборони та формування обґрунтованих висновків щодо ролі РНБО України у відповідній сфері. Структурно-функціональний аналіз дав можливість дослідити інституційну побудову системи забезпечення інформаційної безпеки та визначити функціональне призначення окремих її елементів. Крім того, застосовано інструменти порівняльного аналізу для зіставлення наукових підходів до розуміння інформаційної безпеки та оцінювання сучасних тенденцій розвитку державної політики у цій сфері.

**Обмеження дослідження.** Обмеження дослідження пов'язані з відсутністю у відкритому доступі частини статистичної та аналітичної інформації щодо діяльності РНБО у сфері інформаційної безпеки, а також обмеженим доступом до окремих рішень і документів, що мають гриф обмеження доступу. Крім того, дослідження ґрунтується на аналізі обмеженої кількості наукових джерел, що може впливати на повноту висновків.

## Результати

Національна безпека України розглядається як стан захищеності її суверенітету, територіальної цілісності, конституційного ладу та інших життєво важливих національних інтересів від наявних і потенційних загроз. Відповідно до положень Закону України «Про національну безпеку України», до ключових національних інтересів належать: збереження державного суверенітету та територіальної цілісності, недопущення втручання у внутрішні справи держави, забезпечення сталого соціально-економічного розвитку, а також інтеграція України до європейського та євроатлантичного простору з перспективою набуття членства в Європейському Союзі та НАТО.

Базові засади функціонування системи національної безпеки закріплені в Конституції України, яка визначає фундаментальні принципи державного устрою та передбачає можливість запровадження надзвичайного чи воєнного стану у разі виникнення загроз. Конституційно-правові механізми формують цілісну систему, що поєднує нормативні акти та діяльність уповноважених інституцій, спрямованих на захист національних інтересів. При цьому забезпечення суверенітету, територіальної цілісності, а також економічної та інформаційної безпеки визнається одним із пріоритетних завдань держави та всього суспільства.

Важливу роль у системі забезпечення національної безпеки відіграє Рада національної безпеки і оборони України, яка функціонує як координаційний орган при Президентові України та здійснює контроль за діяльністю органів виконавчої влади у відповідній сфері. Серед ключових інструментів її діяльності варто виділити санкційну політику, що передбачає застосування обмежувальних заходів до осіб, причетних до загроз державній безпеці, зокрема шляхом блокування активів та обмеження в'їзду.


e-ISSN: 2786-586X

У контексті протидії сучасним загрозам, зокрема в умовах гібридної війни, важливим напрямом діяльності РНБО є забезпечення інформаційної безпеки. З цією метою функціонує Центр протидії дезінформації, який здійснює моніторинг інформаційного простору, виявлення деструктивних інформаційних впливів та організацію заходів щодо їх нейтралізації, а також протидію пропаганді та маніпуляціям громадською думкою.

Стратегічні орієнтири державної політики у сфері національної безпеки визначені у Стратегії національної безпеки України, яка враховує сучасні внутрішні та зовнішні виклики, включаючи збройну агресію Російської Федерації. Документ базується на принципах стримування, стійкості та взаємодії, що передбачають розвиток оборонних спроможностей, підвищення адаптивності держави до загроз та поглиблення міжнародного співробітництва.

Сучасні виклики мають комплексний характер і охоплюють не лише військову агресію, а й інформаційні, кібернетичні та економічні загрози. У зв'язку з цим особливого значення набуває розвиток системи стратегічного планування, модернізація сектору безпеки й оборони та посилення ролі інституцій, відповідальних за забезпечення національної стійкості.

Повномасштабне вторгнення російської федерації у 2022 році суттєво трансформувало підходи до розуміння національної безпеки, продемонструвавши обмеженість міжнародних гарантій, зокрема тих, що були закріплені Будапештським меморандумом. Це актуалізувало необхідність формування ефективної внутрішньої системи безпеки, здатної оперативно реагувати на багатовимірні загрози.

У науковому дискурсі національна безпека також розглядається як механізм самозбереження держави та суспільства, що забезпечує стабільність розвитку та захист інтересів громадян. Таким чином, вона виступає не лише інструментом протидії загрозам, а й важливим чинником стратегічного розвитку держави, орієнтованого на європейські та євроатлантичні стандарти.

## Обговорення

Кризи та війни у світі, а особливо війна в Україні, показали критичне зна-чення інформації, насамперед у сфері національного захисту не лише України, а й кожної цивілізованої держави. Кібератаки, злам даних, заволодіння паролями спонукали держави розробляти більш ефективні системи протидії та захисту власного інформаційного простору. Інформація зайняла чи не найважливіше місце у питаннях забезпечення національного суверенітету та безпеки. Військовий досвід України від початку повномасштабного вторгнення демонструє гнучкість підходу до кібербезпеки. Водночас слід зауважити, що цей досвід вивчають міжнародні партнери, щоб ефективніше протидіяти дезінформації ворожих держав. Утім, на нашу думку, питання інформаційного забезпечення національної безпеки потребує, насамперед, покращення міжвідомчої взаємодії, яка покликана пришвидшити обмін даними та якнайкраще їх оброблення, а отже, прийняття найкращого рішення у тій чи іншій ситуації. В умовах сучасного розвитку технологій та поширення гібридних загроз кордони між тилом і фронтом досить часто стираються, тому інформація стає ідеологічним інструментом, а інформаційна безпека є не менш важливою за фізичну оборону. На нашу думку, сучасні війни дуже важко виграти лише військовим шляхом (танками та ракетами), адже вкрай важливу роль відіграє здатність держави та суспільства критично мислити та оцінювати ситуацію, зберігаючи єдність та діючи в національних інтересах, що вкрай важливо в сучасному світі обману та маніпуляцій. Сьогодні Україна формує унікальний кейс інформаційного спротиву, який, без сумніву, може стати і стане орієнтиром та прикладом для інших демократичних та цивілізованих держав [10, с. 198].


e-ISSN: 2786-586X

Погоджуючись із підходом Я. Лелет, слід відзначити, що сучасні механізми забезпечення інформаційної безпеки в умовах кризи виходять за межі суто технічних заходів і набувають комплексного характеру. Важливо, що автор акцентує увагу на ролі держави у формуванні стійкого інформаційного середовища, де інформація виступає не лише об'єктом захисту, але й інструментом впливу на суспільні процеси та забезпечення національної стійкості.

Інформаційна безпека в умовах воєнного стану є не лише реакцією на зовнішні загрози, а й проактивною політикою формування національної ідентичності, довіри до держави та єдності суспільства. Це складова, без якої неможливе повноцінне функціонування державного механізму в умовах гібридної війни. Сильна інформаційна політика – це сильна держава, готова до викликів сучасного світу [13, с.45].

Погоджуючись із автором, слід наголосити, що інформаційна безпека в умовах воєнного стану набуває стратегічного значення та безпосередньо впливає на функціонування державного механізму. Важливою є теза про те, що інформаційна політика держави формує не лише захист від зовнішніх загроз, але й внутрішню суспільну єдність та довіру до інституцій влади.

Встановлено, що інформаційно-безпекова політика в умовах війни виходить за межі суто технічних або нормативно-правових механізмів і дедалі більше спирається на соціально-полі-тичні чинники, зокрема рівень довіри громадян до державних інститутів, ефективність суспільних комунікацій та здатність формувати стійкі національні наративи. Саме ці аспекти визнача-ють довгострокову стійкість інформаційного простору й інформаційного суверенітету держави. Загалом результати дослідження підтверджують, що інституційні чинники є ключо-вою передумовою формування ефективної інформаційно-безпекової політики України в умо-вах воєнного стану. Перспективи подальших наукових розвідок вбачаються в поглибленому аналізі інституційних механізмів стратегічних комунікацій, розвитку міжнародної співпраці у сфері інформаційної безпеки, а також у дослідженні ролі політичної участі та громадян-ського суспільства у зміцненні інформаційної стійкості держави [2, с. 86].

Отже, заслуговує на підтримку підхід авторів щодо визначальної ролі інституційних чинників у забезпеченні інформаційної безпеки держави. На нашу думку, рівень суспільної довіри до державних інституцій, ефективність стратегічних комунікацій та здатність держави формувати стійкі інформаційні наративи є не менш важливими складовими безпеки, ніж технічні або правові механізми захисту.

Досліджено різні наукові визначення терміну «інформаційна безпека». Враховуючи обмежений обсяг дослідження, нами не ставилося за мету дослідження і пропозиції щодо власного розуміння інформаційної безпеки. Вод-ночас, нами доводиться, що правоохоронні органи, зокрема, поліція охорони, є складовою частиною системи органів забезпечення інформаційної безпеки держави, які мають специфічні особливості функціонування в інформаційному середовищі [15, с. 57].

Підтримується наукова позиція авторів щодо того, що суб'єкти забезпечення інформаційної безпеки мають різну функціональну специфіку, однак діють у межах єдиної системи національної безпеки. Особливо важливим є виокремлення ролі правоохоронних органів як складової цієї системи, що забезпечує практичну реалізацію державної політики у сфері інформаційної безпеки.

С. Онопрієнко вважає що методологічні засади дослідження інформаційної безпеки у науці права національної безпеки та військового права базуються перш за все на міждисциплінарному характері цієї категорії. Використання для вивчення інформаційної безпеки приватно-правових і публічно-правових методів дозволяє досягти комплексності і системності нового наукового знання [11, С. 187-188].

Гріщенко А. О. підкреслює, що багатьма дослідниками спростовується ототожнення "інформаційної безпеки" з "безпекою інформації та інформаційних


e-ISSN: 2786-586X

систем", "кібербезпекою" , "комп'ютерною безпекою" та "захистом інформації" тощо, та підкреслюється її суттєве значення у забезпеченні національної безпеки України та у визначеності стану захищеності громадян, суспільства і держави. Для формування єдиного загального поняття "інформаційної безпеки", що дозволить об'єднати у собі три її складові: інформаційну безпеку людини, інформаційну безпеку суспільства та інформаційну безпеку держави, та підкреслить її значення в контексті забезпечення безпеки держави, пропонується розглянути закріплення на законодавчому рівні поняття "національна інформаційна безпека" [6, с. 131].

Досліджено різні наукові визначення терміну «інформаційна безпека». Враховуючи обмежений обсяг дослідження, нами не ставилося за мету дослідження і пропозиції щодо власного розуміння інформаційної безпеки. Водночас, авторами доводиться, що правоохоронні органи, зокрема, поліція охорони, є складовою частиною системи органів забезпечення інформаційної безпеки держави, які мають специфічні особливості функціонування в інформаційному середовищі [15, с. 57].

Підтримується наукова позиція авторів щодо того, що суб'єкти забезпечення інформаційної безпеки мають різну функціональну специфіку, однак діють у межах єдиної системи національної безпеки. Особливо важливим є виокремлення ролі правоохоронних органів як складової цієї системи, що забезпечує практичну реалізацію державної політики у сфері інформаційної безпеки.

Як видно здосліджень, інформація не існує ізольовано від людського середовища і має конкретну мету впливу на суспільство. На думку дослідників, фундаментальними принципами виникнення в зародковому стані понять, які сьогодні визначаються як інформаційна безпека, є звичаєве право, елементи якого в процесах розвитку цивілізації стали універсально обов'язковими для своїх учасників на основі впровадження регуляторного та правового регулювання цієї сфери [5, с. 35].

Підтримується позиція авторів щодо необхідності розглядати інформаційну безпеку як багатовимірну правову категорію, що охоплює як захист інформаційних ресурсів, так і регулювання суспільних відносин у інформаційній сфері. Важливим є акцент на тому, що інформаційна безпека має системний характер і потребує комплексного підходу до її нормативного та теоретичного осмислення.

Ґрунтуючись на наукових матеріалах, наводиться авторське визначення по-няття «інформаційна безпека», яку розумють як діалектичну єдність всіх складових суспільного життя, якими забезпечується правомірне володіння, користування і поширення відомостей з різним рівнем доступу. Ефективна реалізація стратегічних пріоритетів, основних засад і за-вдань з боку держави у галузі інформаційної безпеки вимагає оновлення нормативно-правових механізмів, удосконалення організаційних підходів до управління сферою інформаційної без-пеки, її належного кадрового забезпечення на умовах залучення до роботи високоінтелекту-альних, патріотично налаштованих спеціалістів. Таке завдання уможливлюється виконанням комплексу законодавчих і практичних заходів, спрямованих на усунення суперечностей, невре-гульованості, конфлікту інтересів між суб'єктами-учасниками сфери передавання і володіння інформаційними ресурсами, а також за умови подолання корупційних проявів на всіх рівнях державного управління [4, с. 57].

Заслуговує на підтримку наукова позиція щодо необхідності подальшого розвитку понятійного апарату інформаційної безпеки та вдосконалення її теоретико-правових засад. Автори обґрунтовано наголошують, що ефективність державної політики у цій сфері значною мірою залежить від узгодженості термінології та чіткого визначення функцій суб'єктів інформаційної безпеки.

Сучасний стан правового регулювання кібербезпеки в Україні виявляє низку системних проблем, зокрема фрагментарність законодавства, відсутність цілісної концепції державної політики, дублювання повноважень суб'єктів забезпечення


e-ISSN: 2786-586X

кібербезпеки та недостатню координацію між ними. За умов постійного зростання кількості та складності кібератак, спрямованих, у тому числі, на критичну інфраструктуру та державні інформаційні ресурси, така ситуація істотно знижує ефективність протидії кіберзагрозам [14, с.98].

Погоджуючись із висновками автора, слід зазначити, що фрагментарність законодавства у сфері кібербезпеки дійсно є однією з ключових проблем сучасної системи захисту інформаційного простору України. Особливої уваги потребує питання усунення дублювання повноважень між суб'єктами кібербезпеки та формування цілісної державної політики у цій сфері.

Методика розрахунку рівня інформаційної безпеки з чітким переліком індикаторів та обґрунтованими пороговими значеннями. Проведене оцінювання рівня інформаційної безпеки на основі показників, які лежать в основі світових рейтингів, може стати підґрунтям для вказаної методики. Зокрема, субіндексами інтегрального показника інформаційної безпеки доцільно визначити: розробленість державної політики у сфері інформаційної безпеки; мо-ніторинг та аналіз загроз інформаційному середовищу; освіта та під-вищення кваліфікації у сфері захисту інформаційного, у тому числі кі-берпростору; внесок у глобальну інформаційну безпеку, захист цифрових сервісів та основних послуг у кіберпросторі, послуг елект-ронної ідентифікації, захист персональних даних; боротьба з кіберзло-чинністю та військові кібероперації [1, с. 72].

Заслуговує на увагу підхід автора до оцінювання рівня інформаційної безпеки через систему індикаторів та інтегральних показників. Така методологія дозволяє перейти від загальнотеоретичних міркувань до вимірюваного аналізу стану інформаційної безпеки, що є важливим для формування ефективної державної політики та моніторингу її результативності.

Проблема забезпеченняі нформаційної безпеки правоохоронними органамив Україні вже давно вийшла за межі суто технічної проблеми та стала системнимвикликомнаціональній безпеці. Коливання впоказниках розслідувань у 2020–2024 рр. чітко продемонстрували залежність результативності правоохоронної діяльності від зовнішньополітичних чинників, кадрового потенціалу та можливостей міжнародної співпраці [3, с. 33].

Підтримується позиція авторів щодо того, що забезпечення інформаційної безпеки правоохоронними органами України є не лише технічним, а насамперед системним завданням державної політики. Важливо, що дослідники підкреслюють залежність ефективності правоохоронної діяльності від зовнішніх чинників, кадрового потенціалу та рівня міжнародної взаємодії, що вказує на багаторівневий характер проблематики інформаційної безпеки.

Чітак В. В., Усманов Ю. І. вважають, що задля досягнення кардинальних змін у сфері міжнародно-правового регулювання інформаційних обмінів та комунікацій має враховуватись значна відмінність у правових підходах різних країн до формування національного інформаційного законодавства, забезпечуватись зв'язок між внутрішньодержавною та світовою (глобальною) інформаційною інфраструктурою, задля уникнення конфліктів, та необхідно гармонізувати правове регулювання на різних рівнях [16, С.276].

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 законодавчом у рівні порядок взаємодії між центральними й місцевими органами влади, а також залучити громадянське суспільство до інформаційного спротиву. Важливими є розвиток національної


e-ISSN: 2786-586X

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 [8, с.255].

Отже, погоджуємося з думкою автора про необхідність формування цілісного механізму взаємодії органів публічної влади у сфері інформаційної безпеки. Вважаємо, що чітке розмежування компетенції державних органів та впровадження єдиних стратегічних підходів дозволить підвищити ефективність реалізації державної політики в інформаційному просторі.

Згідно відповідного закону Рада національної безпеки і оборони України «розробляє та розглядає на своїх засіданнях питання, які відповідно до Конституції та законів України, Стратегії національної безпеки України, Воєнної доктрини України належать до сфери національної безпеки і оборони, та подає пропозиції Президентові України, приймає рішення щодо: .. заходів політичного, економічного, соціального, воєнного, науково-технологічного, екологічного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України» [12].

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 [ 9, с.167].

Отже, підтримуючи позицію В. Крушеніцького, слід зазначити, що в сучасних умовах саме Рада національної безпеки і оборони України здатна забезпечити необхідний рівень міжвідомчої координації у сфері інформаційної безпеки. Особливого значення набуває діяльність РНБО як платформи для консолідації зусиль суб'єктів сектору безпеки і оборони у протидії інформаційним та кібернетичним загрозам.

Прийняття базового Закону України "Про інформаційну безпеку України" вбачається необхідним задля консолідації, вдосконалення відповідного законодавства, чіткої структуризації системи нормативно-правових актів у цій галузі, усунення наявних суперечностей, лакун та інших вад. Цей закон має, на наш погляд, закріпити найзагальніші положення, які поширюватимуться на решту нормативно-правових актів у цій галузі, а саме: принципи правового забезпечення, структуру відповідного законодавства, єдині параметри правового забезпечення інформаційної безпеки, єдину термінологію. Крім того, вказаний закон, синтезувавши норми підгалузі правового забезпечення інформаційної безпеки, може стати одним із базових при кодифікації вітчизняного законодавства у сфері інформації та створенні Інформаційного кодексу України [7, с. 98].

Отже, підтримуємо позицію О. Довганя та Т. Ткачука щодо необхідності подальшого вдосконалення законодавчого забезпечення інформаційної безпеки України. В умовах постійного зростання інформаційних загроз особливо актуальним є формування системного та узгодженого нормативно-правового підґрунтя, яке забезпечуватиме ефективне функціонування всіх суб'єктів інформаційної безпеки держави.


e-ISSN: 2786-586X

**Інтерпретація результатів.**

Отримані в процесі аналізу наукових позицій результати свідчать про відсутність єдиного підходу до розуміння інформаційної безпеки та механізмів її забезпечення, однак простежується чітка тенденція до інституціоналізації цієї сфери. Більшість дослідників (зокрема Крушеніцький, Галіпчак, Ротар) сходяться на тому, що ключову роль у системі забезпечення інформаційної безпеки відіграють органи державної влади координаційного типу, насамперед РНБО України, яка виступає центром узгодження діяльності суб'єктів сектору безпеки і оборони. Водночас підкреслюється, що ефективність такої системи значною мірою залежить від якості міжвідомчої взаємодії та рівня стратегічного планування.

Аналіз наукових підходів також дозволяє констатувати поступове розширення змісту поняття «інформаційна безпека», яке виходить за межі суто технічного або правового виміру. У працях Лелет, Селецького та інших авторів інформаційна безпека розглядається як комплексне соціально-правове явище, що включає інформаційно-психологічний, комунікаційний та ціннісний компоненти. Це свідчить про трансформацію наукового дискурсу від вузького розуміння кіберзахисту до ширшої концепції інформаційної стійкості держави та суспільства, що особливо актуально в умовах гібридної війни та інформаційних загроз.

**Порівняння з іншими дослідженнями.**

Порівняльний аналіз розглянутих наукових підходів свідчить, що в українській доктрині інформаційної безпеки сформувалися щонайменше два базові напрями досліджень. Перший зосереджується на інституційно-правовому вимірі, де ключовими є роботи Довганя, Ткачука та Селіхова, які акцентують увагу на необхідності систематизації законодавства, усунення дублювання повноважень та формування цілісної державної політики у сфері кібер- та інформаційної безпеки. Другий напрям має більш широке, соціально-політичне спрямування (Лелет, Селецький, Галіпчак, Ротар), у межах якого інформаційна безпека розглядається як елемент суспільної стійкості, довіри до держави та формування національних наративів.

Порівняння також демонструє відмінності у визначенні ролі РНБО України в системі забезпечення інформаційної безпеки. У працях інституційного спрямування РНБО розглядається як координаційний центр, що забезпечує узгодження дій суб'єктів сектору безпеки і оборони та формування стратегічних рішень. Натомість у роботах, де акцент зроблено на суспільно-комунікаційному вимірі, роль РНБО опосередковано пов'язується з формуванням інформаційної політики держави через стратегічні комунікації та реагування на інформаційні загрози. Таким чином, у науковій літературі простежується поєднання правового, інституційного та соціально-комунікаційного підходів до розуміння інформаційної безпеки як багатовимірного явища.

**Наукова новизна (розгорнуто).**

Наукова новизна дослідження полягає у комплексному переосмисленні ролі Ради національної безпеки і оборони України як ключового координаційного та стратегічного суб'єкта формування і реалізації державної політики інформаційної безпеки в умовах сучасних гібридних загроз. На відміну від наявних у науковій літературі підходів, де РНБО переважно розглядається як загальний елемент системи національної безпеки або як орган стратегічного рівня без детальної конкретизації його функціонального впливу, у даному дослідженні акцентовано її інтеграційну роль як центру міжвідомчої координації у сфері інформаційної безпеки, що забезпечує узгодження діяльності Служби безпеки України, Міністерства оборони України,


e-ISSN: 2786-586X

Державної служби спеціального зв'язку та захисту інформації України, Національної поліції та інших суб'єктів сектору безпеки і оборони.

Новизна також полягає у розширенні розуміння інституційного механізму забезпечення інформаційної безпеки шляхом включення до нього не лише державних органів виконавчої влади, але й аналітичних центрів, наукових установ та інститутів громадянського суспільства як елементів превентивної та експертної підтримки стратегічних рішень. Такий підхід дозволяє розглядати інформаційну безпеку не як суто вертикально організовану систему управління, а як мережеву модель взаємодії, у якій РНБО України виконує функцію координаційного ядра.

Додатковим елементом наукової новизни є уточнення змісту поняття «інституційна спроможність системи інформаційної безпеки», яке пропонується розуміти як здатність державних та недержавних суб'єктів ефективно взаємодіяти в умовах динамічних інформаційних загроз, забезпечуючи оперативний обмін даними, стратегічне прогнозування та вироблення узгоджених управлінських рішень. На цій основі обґрунтовується необхідність посилення ролі Національного координаційного центру кібербезпеки при РНБО України як ключового елемента оперативного реагування на кіберзагрози.

Крім того, у дослідженні розширено підхід до оцінювання ефективності державної політики інформаційної безпеки шляхом поєднання правових, організаційних та комунікаційних критеріїв. Це дозволяє відійти від вузько нормативного розуміння ефективності та сформувати більш комплексну модель, яка враховує рівень міжвідомчої координації, швидкість реагування на інформаційні загрози, а також ступінь залучення громадянського суспільства до процесів інформаційної стійкості держави.

**Практичне значення (розгорнуто).**

Практичне значення результатів дослідження полягає у можливості їх використання для вдосконалення організаційно-правового та інституційного механізму забезпечення інформаційної безпеки України, насамперед у частині підвищення ефективності діяльності Ради національної безпеки і оборони України як координуючого центру у сфері національної безпеки. Запропоновані підходи можуть бути використані при розробленні та уточненні стратегічних документів у сфері інформаційної безпеки, зокрема Стратегії інформаційної безпеки України, а також підзаконних нормативно-правових актів, що регламентують взаємодію суб'єктів сектору безпеки і оборони.

Отримані результати можуть бути застосовані у практичній діяльності органів державної влади з метою вдосконалення міжвідомчої координації, підвищення оперативності обміну інформацією та усунення дублювання функцій між Службою безпеки України, Міністерством оборони України, Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією та іншими суб'єктами, що беруть участь у забезпеченні інформаційної безпеки. Особливого значення набуває можливість використання висновків дослідження для оптимізації роботи Національного координаційного центру кібербезпеки при РНБО України як інструменту оперативного реагування на кіберзагрози.

Практична цінність роботи також полягає у можливості її використання в освітньому процесі при викладанні навчальних дисциплін «Інформаційне право», «Кібербезпека», «Національна безпека», «Адміністративне право» та суміжних курсів у закладах вищої освіти. Матеріали дослідження можуть бути використані при підготовці навчально-методичних комплексів, лекційних курсів, а також при написанні курсових, дипломних і магістерських робіт.

Крім того, результати дослідження мають прикладне значення для подальших наукових розробок у сфері інформаційної безпеки, оскільки формують підґрунтя для


e-ISSN: 2786-586X

поглибленого аналізу інституційної моделі забезпечення інформаційної стійкості держави, розвитку стратегічних комунікацій та вдосконалення механізмів протидії інформаційним і кіберзагрозам в умовах гібридної війни.

**Висновки**

У результаті проведеного дослідження встановлено, що інформаційна безпека в сучасних умовах є ключовим елементом національної безпеки України та визначається як комплексне соціально-правове явище, яке охоплює не лише технічні аспекти захисту інформації, а й інституційні, правові, комунікаційні та ціннісні складові. Її значення істотно зросло в умовах гібридної війни та активного використання інформаційного простору як інструменту впливу на державу та суспільство.

Визначено, що наукові підходи до розуміння інформаційної безпеки характеризуються багатовимірністю та відсутністю єдності у трактуванні її змісту. Водночас простежується загальна тенденція до розширення цієї категорії від вузького техніко-кібернетичного розуміння до більш широкої концепції інформаційної стійкості держави, що включає психологічний, соціальний та політико-комунікаційний виміри.

Встановлено, що у системі забезпечення інформаційної безпеки України важливе місце займає Рада національної безпеки і оборони України, яка виконує функцію координаційного центру між суб'єктами сектору безпеки і оборони. Її роль полягає у забезпеченні узгодженості дій державних органів, стратегічному плануванні та реагуванні на комплексні загрози в інформаційній сфері. Особливе значення має діяльність Національного координаційного центру кібербезпеки як елемента оперативного реагування на кіберінциденти.

Доведено, що ефективність державної політики інформаційної безпеки значною мірою залежить від рівня міжвідомчої координації, чіткого розмежування повноважень суб'єктів забезпечення безпеки, а також від залучення наукових установ, аналітичних центрів та громадянського суспільства до формування стратегічних рішень. Це дозволяє підвищити адаптивність державної системи до сучасних інформаційних загроз.

Підсумовано, що подальший розвиток системи інформаційної безпеки України потребує вдосконалення нормативно-правової бази, посилення інституційної спроможності координаційних органів, розвитку стратегічних комунікацій та формування комплексного підходу до протидії інформаційним і кіберзагрозам. Отримані результати можуть бути використані для вдосконалення державної політики у сфері національної безпеки та підвищення рівня інформаційної стійкості держави.

**Список використаних джерел**

1. Білько С. «Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку» Науковий вісник Полісся, 2022. № 1 (24). С. 58-77
2. Галіпчак В. Ротар Н. Інституційні чинники інформаційно-безпекової політик в умовах воєнного стану: концепт дослідження. Вісник Прикарпатського університету. Серія: Політологія. Випуск 22, 2026. С. 83-87
3. Гарбінська-Руденко А.В., Кучко М.О. «Забезпечення інформаційної безпеки правоохоронними органами України» // Ірпінський юридичний часопис, 2025. Вип. 3 (20). С. 28-36
4. Гончаров М.В., Гончаров А.В. «Деякі аспекти досліджень наукових поглядів щодо поняття інформаційної безпеки» // Науковий вісник УжНУ. Серія Право, 2025. №92. Том 1. С. 53-58
5. Гончаров М.В., Гончаров А.В. «Загальнотеоретичні основи дослідження поняття "інформаційна безпека"». Аналітично-порівняльне правознавство, 2025. №2. С. 32-36


e-ISSN: 2786-586X

6. Гріщенко А. О.Підходи до розуміння категорії «інформаційна безпека» та правові засади її забезпечення. *Інформація і право. 2020. №4 (35). С. 119-133*
7. Довгань О.Д. Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України» // Інформація і право, 2019.
8. Крушеніцький В.С. Органи публічної влади як суб'єкти формування та реалізації політики національної безпеки в інформаційному просторі Наукові записки: Серія Право. 2024. Вип. 17. С. 252-256
9. Крушеніцький В.С. Роль Ради національної безпеки і оборони України у формуванні державної політики інформаційної безпеки Наукові записки: Серія Право. 2025. Вип. 18. С. 164-167
10. Лелет Я. Механізми та форми забезпечення інформаційної безпеки в умовах кризи Вісник Прикарпатського університету. Серія: Політологія. Випуск 21, 2025. С. 193-201
11. Онопрієнко С. Г. Методологічні засади дослідження інформаційної безпеки у науці права національної безпеки та військового права. Аналітично-порівняльне правознавство. 2021. №4. С. 185-188
12. Про Раду національної безпеки і оборони України. Закон України 5 березня 1998 року № 183/98-ВР URL: https://zakon.rada.gov.ua/laws/show/183/98-вр#Text
13. Селецький, О. В. Інформаційна безпека в умовах воєнного стану як складова національної безпеки. Актуальні проблеми політики. - 2025. - Вип. 76. - С. 43-47.
14. Селіхов Д.А. «Кібербезпека як складова інформаційної безпеки: теоретичні та прикладні аспекти» // Аналітично-порівняльне правознавство, 2026. Випуск 1. Частина 1. С.94-99
15. Тимошенко Ю., Кисленко Д. Поліція охорони як суб'єкт забезпечення інформаційної безпеки Наукові праці МАУП. Юридичні науки. 2023. Вип. 1 (64) С. 53-59
16. Чітак В. В., Усманов Ю. І. Міжнародний і національно-правовий аналіз стану інформаційної безпеки України в умовах збройного конфлікту. Науковий вісник Ужгородського Національного Університету. 2023. Серія ПРАВО. Випуск 76: частина 2. С. 271-277

## References

1. Bilko S. "Informatsiina ta ekonomichna bezpeka: otsiniuvannia rivnia ta vzaiemozviazku". Naukovyi visnyk Polissia, 2022, No. 1 (24), pp. 58–77.
2. Halipchak V., Rotar N. "Instytutsiini chynnyky informatsiino-bezpekovoi polityky v umovakh voiennoho stanu: kontsept doslidzhennia". Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia, Issue 22, 2026, pp. 83–87.
3. Harbinska-Rudenko A.V., Kuchko M.O. "Zabezpechennia informatsiinoi bezpeky pravookhoronnymy orhanamy Ukrainy". Irpinskyi yurydychnyi chasopys, 2025, Issue 3 (20), pp. 28–36.
4. Honcharov M.V., Honcharov A.V. "Deyaki aspekty doslidzhen naukovykh pohliadiv shchodo poniattia informatsiinoi bezpeky". Naukovyi visnyk UzhNU. Seriia Pravo, 2025, No. 92, Vol. 1, pp. 53–58.
5. Honcharov M.V., Honcharov A.V. "Zahalnoteoretychni osnovy doslidzhennia poniattia 'informatsiina bezpeka'". Analitychno-porivnialne pravoznavstvo, 2025, No. 2, pp. 32–36.
6. Hryshchenko A.O. "Pidkhody do rozuminnia katehorii 'informatsiina bezpeka' ta pravovi zasady yii zabezpechennia". Informatsiia i pravo, 2020, No. 4 (35), pp. 119–133.


e-ISSN: 2786-586X

7. Dovhan O.D., Tkachuk T.Yu. “Kontseptualni zasady zakonodavchoho zabezpechennia informatsiinoi bezpeky Ukrainy”. Informatsiia i pravo, 2019.
8. Krushenitskyi V.S. “Orhany publichnoi vlady yak subiekty formuvannia ta realizatsii polityky natsionalnoi bezpeky v informatsiinomu prostori”. Naukovi zapysky: Seriia Pravo, 2024, Issue 17, pp. 252–256.
9. Krushenitskyi V.S. “Rol Rady natsionalnoi bezpeky i oborony Ukrainy u formuvanni derzhavnoi polityky informatsiinoi bezpeky”. Naukovi zapysky: Seriia Pravo, 2025, Issue 18, pp. 164–167.
10. Lelet Ya. “Mekhanizmy ta formy zabezpechennia informatsiinoi bezpeky v umovakh kryzy”. Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia, Issue 21, 2025, pp. 193–201.
11. Onopriienko S.H. “Metodolohichni zasady doslidzhennia informatsiinoi bezpeky u nautsi prava natsionalnoi bezpeky ta viiskovoho prava”. Analitychno-porivnialne pravoznavstvo, 2021, No. 4, pp. 185–188.
12. Law of Ukraine “On the National Security and Defence Council of Ukraine” No. 183/98-VR, 05 March 1998. https://zakon.rada.gov.ua/laws/show/183/98-vr
13. Seletskyi O.V. “Informatsiina bezpeka v umovakh voiennoho stanu yak skladova natsionalnoi bezpeky”. Aktualni problemy polityky, 2025, Issue 76, pp. 43–47.
14. Selikhov D.A. “Kiberbezpeka yak skladova informatsiinoi bezpeky: teoretychni ta prykladni aspekty”. Analitychno-porivnialne pravoznavstvo, 2026, Issue 1, Part 1, pp. 94–99.
15. Tymoshenko Yu., Kislenko D. “Politsiia okhorony yak subiekt zabezpechennia informatsiinoi bezpeky”. Naukovi pratsi MAUP. Yurydychni nauky, 2023, Issue 1 (64), pp. 53–59.
16. Chitak V.V., Usmanov Yu.I. “Mizhnarodnyi i natsionalno-pravovyi analiz stanu informatsiinoi bezpeky Ukrainy v umovakh zbroinoho konfliktu”. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia Pravo, 2023, Issue 76 (Part 2), pp. 271–277.


e-ISSN: 2786-586X