Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

Кваліфікаційна наукова
праця на правах рукопису

Пупяліс Єгор Вікторович

УДК 351.861:352/354:614.8

ДИСЕРТАЦІЯ
ІНСТИТУЦІАЛІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ В УМОВАХ ГІБРИДНОЇ ВІЙНИ В УКРАЇНІ

Спеціальність 281-Публічне управління та адміністрування
Галузь знань 28-Публічне управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ Є.В. Пупяліс

Науковий керівник:
Величко Лариса Юріївна, доктор юридичних наук, професор

Харків-2026

АНОТАЦІЯ

Пупяліс Є.В. Інституціалізація публічного управління національною безпекою в умовах гібридної війни в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування. – Харківський національний університет імені В.Н. Каразіна, Міністерство освіти та освіти України, Харків, 2026.

В умовах глибоких трансформацій глобального безпекового середовища проблематика публічного управління національною безпекою набуває особливої актуальності та нагальності. Сучасний світ характеризується якісно новими формами загроз, що не вписуються в традиційну дихотомію війни та миру, поєднують воєнні та невоєнні засоби впливу, розмивають межі між внутрішніми та зовнішніми викликами безпеці. Феномен гібридної війни як комплексного багатовимірного конфлікту став домінуючою характеристикою сучасних міжнародних конфліктів та потужним каталізатором інституційних трансформацій у сфері національної безпеки. Особливої гостроти ця проблема набуває для України, яка з 2014 року перебуває в стані масштабної гібридної агресії з боку Російської Федерації, що з лютого 2022 року переросла у повномасштабну воєнну агресію з потужними гібридними компонентами.

У дисертаційному дослідженні здійснено системний аналіз теоретико-методологічних засад інституціалізації публічного управління національною безпекою в умовах гібридної війни. Встановлено, що інституціалізація виступає фундаментальним процесом трансформації спонтанних та ситуативних управлінських практик у стійкі організаційні форми, здатні забезпечувати ефективне функціонування системи національної безпеки в умовах високої невизначеності та багатовекторних загроз. Сутність інституціалізації в безпековій сфері полягає не лише у формальному створенні

організаційних структур та нормативно-правової бази, а й у глибинній трансформації управлінської культури, формуванні нових ціннісних орієнтирів та поведінкових моделей, які визначають характер взаємодії між різними суб'єктами забезпечення національної безпеки.

Доведено, що концептуалізація національної безпеки як об'єкта публічного управління в сучасних умовах вимагає переходу від традиційного державоцентричного та мілітаристського розуміння до комплексного багатовимірного підходу, що охоплює військові, політичні, економічні, соціальні, інформаційні, кібернетичні та інші виміри безпеки. Взаємозв'язок між інституціалізацією та ефективністю управління національною безпекою має діалектичний характер: з одного боку, розвинене інституційне середовище створює передумови для ефективного безпекового управління через забезпечення координації, легітимності та ресурсної бази; з іншого боку, ефективність управління стимулює подальший інституційний розвиток через накопичення досвіду та вдосконалення організаційних форм.

З'ясовано, що феномен гібридної війни фундаментально трансформує парадигму публічного управління національною безпекою, розмиваючи традиційні межі між війною та миром, внутрішніми та зовнішніми загрозами, державними та недержавними акторами, створюючи якісно нове безпекове середовище, що характеризується високим рівнем невизначеності, амбівалентності та взаємопов'язаності різнорідних загроз. Гібридні загрози відрізняються комплексністю, адаптивністю, використанням легальних інструментів для досягнення нелегітимних цілей, експлуатацією когнітивних вразливостей, довготривалим характером та мережевою організацією, що вимагає від системи публічного управління розвитку принципово нових компетенцій та механізмів реагування.

Розроблено багатовимірну систему критеріїв оцінювання інституційної зрілості системи публічного управління національною безпекою, яка інтегрує сім взаємопов'язаних вимірів: структурної, функціональної, нормативної, координаційної, адаптивної, культурної та інтеграційної зрілості, що

комплексно відображають здатність безпекових інститутів ефективно функціонувати в умовах гібридної війни. На відміну від існуючих методик, які акцентують переважно на статичних формальних показниках, розроблена система критеріїв враховує динамічні характеристики інституційного розвитку, зокрема адаптивність до швидкозмінного характеру гібридних загроз, здатність до міжвідомчої інтеграції та стійкість до багатовекторних деструктивних впливів.

Дослідження нормативно-правової бази функціонування системи національної безпеки України виявило її фундаментальну трансформацію під впливом гібридної агресії, що виявилося у прийнятті нового базового законодавства, оновленні стратегічних документів та запровадженні нових правових інструментів протидії гібридним загрозам. Аналіз організаційної структури суб'єктів забезпечення національної безпеки продемонстрував еволюцію від пострадянської моделі до більш інтегрованої системи, адаптованої до викликів гібридної війни, з створенням нових інституцій та трансформацією існуючих структур. Водночас виявлено проблеми дублювання функцій, недостатньої горизонтальної координації, існування «сірих зон» компетенції, що вимагає подальшої оптимізації організаційної архітектури.

Оцінювання ефективності механізмів публічного управління національною безпекою в умовах гібридної агресії продемонструвало значну позитивну динаміку порівняно з початковим етапом 2014 року. Десятирічний період протистояння став безпрецедентним випробуванням, що стимулювало інституційну адаптацію – від початкового колапсу та хаотичного реагування до формування більш структурованої системи з елементами превентивного планування, розвиненою координацією та міжнародною інтеграцією. Еволюція реагування включала чотири основні етапи з різним рівнем готовності та ефективності протидії загрозам.

На основі порівняльного аналізу зарубіжного досвіду інституціалізації управління національною безпекою в умовах гібридних загроз виявлено

спільні тенденції та кращі практики, релевантні для України. Особливо цінним визначено досвід країн Балтії, що першими зіткнулися з російською гібридною агресією та розробили ефективні механізми протидії: концепцію комплексної оборони, світове лідерство в кібербезпеці, активну протидію інформаційній агресії, програми соціальної інтеграції. Виявлено спільні елементи успішних моделей: створення координаційних центрів протидії гібридним загрозам, розбудова спроможностей кіберзахисту, системи стратегічних комунікацій, механізми залучення громадянського суспільства, міжнародна кооперація.

Ключовим результатом дослідження стала розробка концептуальної моделі інституціалізації публічного управління національною безпекою в умовах гібридної війни, яка вперше об'єднує в органічну систему принципи функціонування, архітектурні елементи, механізми координації та адаптаційні спроможності. Модель ґрунтується на чотирнадцяти взаємопов'язаних базових принципах та передбачає багаторівневу архітектуру з інноваційними елементами: функціональні кластери замість традиційних відомчих структур, Національний центр стійкості для забезпечення безперебійного функціонування критичної інфраструктури, Регіональні центри безпеки та стійкості як інтегровані міжвідомчі структури, мережева компонента з горизонтальними зв'язками, інформаційна підсистема на базі єдиного інформаційного простору, вбудовані механізми адаптації до еволюції гібридних загроз. На відміну від існуючих підходів, запропонована модель забезпечує системний підхід до формування стійкої та адаптивної системи реагування на комплексні гібридні загрози.

Обґрунтовано систему механізмів координації, яка поєднує вертикальну координацію через каскадну систему узгодженого цілепокладання з використанням «стратегічних контрактів» та горизонтальну координацію через систему спеціалізованих міжвідомчих комітетів, спільні ситуаційні центри, інтегровані інформаційні системи, уніфіковані стандарти та перехід до програмно-цільового фінансування. Розроблено комплексну систему правових механізмів удосконалення публічного управління національною

безпекою, концептуальною основою якої є парадигмальний перехід від фрагментарного до інтегрованого системного підходу через масштабну кодифікацію законодавства, введення нових правових концепцій, створення ефективного правового забезпечення координації, гармонізацію з міжнародними стандартами.

Розроблено систему організаційних механізмів трансформації сектору безпеки на засадах переходу від функціонально-галузевого до процесно-орієнтованого принципу побудови структур. Ключовими елементами є створення Інтегрованого командування сил безпеки та оборони, реорганізація розвідувальної спільноти через Національне розвідувальне агентство, структурна інтеграція кіберсил через об'єднане Кіберкомандування, трансформація територіальної організації до гнучкої мережевої моделі, консолідація забезпечувальних функцій у формі спільних міжвідомчих сервісів.

Практичне значення одержаних результатів визначається можливістю їх використання органами державної влади при розробці стратегій, програм та планів у сфері національної безпеки, проведенні інституційного аудиту, впровадженні механізмів міжвідомчої координації, вдосконаленні системи реагування на гібридні загрози. Запропонована концептуальна модель може використовуватись як методологічна основа для організації діяльності безпекових структур, планування заходів з підвищення інституційної спроможності та адаптивності системи національної безпеки до динамічних змін безпекового середовища.

Ключові слова: публічне управління, національна безпека, інституціалізація, гібридна війна, гібридні загрози, інституційна зрілість, міжвідомча координація, адаптивна архітектура, функціональні кластери, безпекові інститути, правові механізми, організаційні механізми.

ABSTRACT

Pupalis E.V. Institutionalization of public management of national security in the conditions of hybrid war in Ukraine. – Qualifying scientific work on the rights of the manuscript.

The dissertation on competition of a scientific degree of the doctor of philosophy on a specialty 281 – Public Management and Administration. – V.N. Karazin Kharkiv National University, Kharkiv, 2025.

In the context of profound transformations of the global security environment, the issues of public management of national security are gaining particular relevance and urgency. The modern world is characterized by qualitatively new forms of threats that do not fit into the traditional dichotomy of war and peace, combine military and non-military means of influence, blur the boundaries between internal and external security challenges. The phenomenon of hybrid warfare as a complex multidimensional conflict has become the dominant characteristic of contemporary international conflicts and a powerful catalyst for institutional transformations in the sphere of national security. This problem acquires particular acuteness for Ukraine, which since 2014 has been in a state of large-scale hybrid aggression by the Russian Federation, which since February 2022 has escalated into full-scale military aggression with powerful hybrid components.

The dissertation research provides a systematic analysis of theoretical and methodological foundations of institutionalization of public management of national security in the context of hybrid warfare. It has been established that institutionalization acts as a fundamental process of transforming spontaneous and situational management practices into stable organizational forms capable of ensuring effective functioning of the national security system in conditions of high uncertainty and multivector threats. The essence of institutionalization in the security sphere lies not only in the formal creation of organizational structures and normative-legal framework, but also in the profound transformation of management

culture, formation of new value orientations and behavioral models that determine the nature of interaction between different subjects of national security provision.

The conceptualization of national security as an object of public management in modern conditions requires a transition from the traditional state-centric and militaristic understanding to a comprehensive multidimensional approach covering military, political, economic, social, informational, cyber and other dimensions of security. The relationship between institutionalization and effectiveness of national security management has a dialectical character: on the one hand, a developed institutional environment creates prerequisites for effective security management through ensuring coordination, legitimacy and resource base; on the other hand, management effectiveness stimulates further institutional development through accumulation of experience and improvement of organizational forms.

The phenomenon of hybrid warfare fundamentally transforms the paradigm of public management of national security, blurring traditional boundaries between war and peace, internal and external threats, state and non-state actors, creating a qualitatively new security environment characterized by a high level of uncertainty, ambivalence and interconnectedness of heterogeneous threats. Hybrid threats are distinguished by complexity, adaptability, use of legal instruments to achieve illegitimate goals, exploitation of cognitive vulnerabilities, long-term character and network organization, which requires the public management system to develop fundamentally new competencies and response mechanisms.

A multidimensional system of criteria for assessing the institutional maturity of the public management system of national security has been developed, which integrates seven interconnected dimensions: structural, functional, normative, coordinational, adaptive, cultural and integrational maturity, comprehensively reflecting the ability of security institutions to function effectively in conditions of hybrid warfare. Unlike existing methodologies that emphasize predominantly static formal indicators, the developed system of criteria takes into account dynamic characteristics of institutional development, particularly adaptability to the rapidly changing nature of hybrid threats, capacity for interagency integration and resilience

to multivector destructive influences.

The study of the normative-legal framework for the functioning of Ukraine's national security system revealed its fundamental transformation under the influence of hybrid aggression, manifested in the adoption of new basic legislation, updating of strategic documents and introduction of new legal instruments for countering hybrid threats. Analysis of the organizational structure of national security providers demonstrated evolution from the post-Soviet model to a more integrated system adapted to the challenges of hybrid warfare, with the creation of new institutions and transformation of existing structures. At the same time, problems of duplication of functions, insufficient horizontal coordination, and existence of «gray zones» of competence were identified, requiring further optimization of organizational architecture.

The assessment of effectiveness of public management mechanisms of national security in conditions of hybrid aggression demonstrated significant positive dynamics compared to the initial stage of 2014. The ten-year period of confrontation became an unprecedented test that stimulated institutional adaptation – from initial collapse and chaotic response to formation of a more structured system with elements of preventive planning, developed coordination and international integration. The evolution of response included four main stages with different levels of readiness and effectiveness in countering threats.

Based on comparative analysis of foreign experience in institutionalization of national security management in conditions of hybrid threats, common trends and best practices relevant for Ukraine were identified. The experience of the Baltic countries, which were the first to face Russian hybrid aggression and developed effective countermeasures, was determined to be particularly valuable: the concept of comprehensive defense, world leadership in cybersecurity, active counteraction to information aggression, social integration programs. Common elements of successful models were identified: creation of coordination centers for countering hybrid threats, development of cyber defense capabilities, strategic communication systems, mechanisms for civil society engagement, international cooperation.

The key result of the research was the development of a conceptual model of institutionalization of public management of national security in conditions of hybrid warfare, which for the first time combines into an organic system the principles of functioning, architectural elements, coordination mechanisms and adaptive capabilities. The model is based on fourteen interconnected basic principles and provides for a multilevel architecture with innovative elements: functional clusters instead of traditional departmental structures, National Resilience Center to ensure uninterrupted functioning of critical infrastructure, Regional Security and Resilience Centers as integrated interagency structures, network component with horizontal connections, information subsystem based on a unified information space, built-in mechanisms for adaptation to the evolution of hybrid threats. Unlike existing approaches, the proposed model provides a systematic approach to forming a resilient and adaptive system for responding to complex hybrid threats.

A system of coordination mechanisms has been substantiated, which combines vertical coordination through a cascade system of coordinated goal-setting using «strategic contracts» and horizontal coordination through a system of specialized interagency committees, joint situational centers, integrated information systems, unified standards and transition to program-targeted financing. A comprehensive system of legal mechanisms for improving public management of national security has been developed, the conceptual basis of which is a paradigmatic transition from fragmented to integrated systemic approach through large-scale codification of legislation, introduction of new legal concepts, creation of effective legal support for coordination, harmonization with international standards.

A system of organizational mechanisms for transforming the security sector has been developed based on the transition from functional-sectoral to process-oriented principle of building structures. Key elements include the creation of Integrated Command of Security and Defense Forces, reorganization of the intelligence community through the National Intelligence Agency, structural integration of cyber forces through a unified Cyber Command, transformation of territorial organization to a flexible network model, consolidation of support

functions in the form of joint interagency services.

The practical significance of the obtained results is determined by the possibility of their use by state authorities in developing strategies, programs and plans in the field of national security, conducting institutional audits, implementing interagency coordination mechanisms, improving the system of response to hybrid threats. The proposed conceptual model can be used as a methodological basis for organizing the activities of security structures, planning measures to increase institutional capacity and adaptability of the national security system to dynamic changes in the security environment.

Keywords: public management, national security, institutionalization, hybrid warfare, hybrid threats, institutional maturity, interagency coordination, adaptive architecture, functional clusters, security institutions, legal mechanisms, organizational mechanisms.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Публікації у фахових виданнях:

1. Величко Л. Ю., Пупяліс Є.В. Особливості публічного управління в умовах гібридних війн. *Суспільство та національні інтереси*. 2025. № 6(14). С. 634-647. DOI: https://doi.org/10.52058/3041-1572-2025-6(14)-634-647

Особистий внесок автора: визначення ключових аспектів впливу гібридних війн на публічне управління.

2. Пупяліс Є.В. Розвиток інституційної спроможності публічного управління у протидії гібридним загрозам національній безпеці. Наукові інновації та передові технології. 2025. № 6(46). С. 253-264. DOI: https://doi.org/10.52058/2786-5274-2025-6(46)-253-264

3. Пупяліс Є.В. Зарубіжний досвід інституціалізації управління національною безпекою в умовах гібридних загроз: можливості для України. *Національні інтереси України*. № 11(16), 2025. С. 1317-1328. DOI: https://doi.org/10.52058/3041-1793-2025-11(16)-1317-1328

4. Пупяліс Є.В. Концептуальна модель інституціалізації публічного управління національною безпекою в умовах гібридної війни. *Актуальні проблеми державного управління*. 2025. № 2 (67). С. 285-302. DOI: https://doi.org/10.26565/1684-8489-2025-2-14

Публікації, що засвідчують апробацію результатів дослідження:

5. Величко Л. Ю., Пупяліс Є.В. Стратегічна культура як чинник публічного управління національною безпекою в умовах гібридної війни. *Матеріали VIII Міжнародної науково-практичної конференції «Міжнародна та національна безпека: теоретичні і прикладні аспекти»*. С. 397-400. https://er.dduvs.edu.ua/bitstream/123456789/14155/1/183.pdf

Особистий внесок автора: визначення каталізаторів змін стратегічної культури у контексті безпекової політики.

6. Пупяліс Є.В. Адаптація системи національної безпеки до викликів гібридної агресії. *Матеріали XXV Міжнародного наукового конгресу «Публічне управління XXI століття: основні виклики післявоєнної відбудови»*. С. 218-222. https://ekhnuir.karazin.ua/handle/123456789/22470

7. Пупяліс Є.В. Інституалізація публічного управління національною безпекою в умовах гібридної агресії. *Матеріали Наукового – практичної коференції « Потенціал молоді у розвитку публічного управління в Україні».*

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. В умовах глибоких трансформацій глобального безпекового середовища проблематика публічного управління національною безпекою набуває особливої актуальності та нагальності. Сучасний світ характеризується якісно новими формами загроз, що не вписуються в традиційну дихотомію війни та миру, поєднують воєнні та невоєнні засоби впливу, розмивають межі між внутрішніми та зовнішніми викликами безпеці. Феномен гібридної війни як комплексного багатовимірного конфлікту, що одночасно охоплює воєнну, інформаційну, економічну, кібернетичну, дипломатичну та інші сфери, став домінуючою характеристикою сучасних міжнародних конфліктів та потужним каталізатором інституційних трансформацій у сфері національної безпеки.

Ефективність публічного управління національною безпекою в умовах гібридної війни визначає спроможність держави та суспільства протидіяти багатовекторним асиметричним загрозам, зберігати державний суверенітет та територіальну цілісність, забезпечувати безпеку громадян та критичної інфраструктури в умовах високої невизначеності та обмеженості ресурсів. Вона безпосередньо впливає на рівень національної стійкості, соціальної згуртованості та міжнародної підтримки в протистоянні агресору. При цьому традиційні підходи до організації публічного управління національною безпекою, сформовані для епохи конвенційних загроз та побудовані на принципах чіткого відомчого розмежування, ієрархічної централізації та секторальної спеціалізації, виявляються недостатньо ефективними для протидії комплексним гібридним загрозам, що експлуатують міжвідомчі розриви, використовують уразливості демократичних інститутів та діють у сірих зонах міжнародного права.

Особливої гостроти та практичної актуальності ця проблема набуває для України, яка з 2014 року перебуває в стані масштабної гібридної агресії з боку

Російської Федерації, що з лютого 2022 року переросла у повномасштабну воєнну агресію з потужними гібридними компонентами. Український досвід став унікальною лабораторією протидії гібридним загрозам та інституційної адаптації системи національної безпеки в екстремальних умовах. Водночас цей досвід виявив критичні системні проблеми чинної моделі публічного управління національною безпекою: відомчу фрагментацію та роз'єднаність зусиль, слабкість механізмів міжвідомчої координації, інформаційну несумісність та ізольованість відомчих баз даних, дублювання функцій та непродуктивну конкуренцію за ресурси, реактивний характер реагування замість проактивного прогнозування, низьку адаптивність організаційних структур до швидкої еволюції загроз, недостатність правового забезпечення міжвідомчої взаємодії в кризових ситуаціях.

В епоху глобальної нестабільності та поширення гібридних конфліктів традиційна модель публічного управління національною безпекою потребує фундаментального переосмислення та системної трансформації. Гібридна війна як якісно новий феномен вимагає не косметичних покращень існуючої системи, а її глибокої інституційної перебудови на нових концептуальних засадах. Ключовими напрямами такої трансформації є перехід від секторального до інтегрованого підходу через створення функціональних кластерів замість традиційних відомчих бар'єрів, від реактивного до проактивного управління через розвиток систем раннього виявлення загроз та сценарного прогнозування, від жорсткої ієрархії до гнучких мережевих структур з потужними горизонтальними зв'язками, від інформаційної роз'єднаності до єдиного інформаційного простору з можливістю крос-відомчого доступу, від статичної організації до адаптивної архітектури зі вбудованими механізмами еволюції разом із загрозами.

Актуальність дослідження обумовлена також практичними потребами удосконалення системи публічного управління національною безпекою в Україні на основі узагальнення унікального вітчизняного досвіду протидії гібридній агресії та критичного осмислення релевантних міжнародних

практик. Попри безпрецедентну мобілізацію державних інститутів та суспільства перед обличчям екзистенційної загрози, попри значні досягнення в окремих напрямах безпекової політики, залишаються невирішеними фундаментальні проблеми інституційної архітектури сектору безпеки. Особливо гостро проявляються системні вади в ситуаціях, що вимагають швидкої синхронізованої відповіді різних відомств на комплексні багатовимірні загрози – від масованих кібератак на критичну інфраструктуру до координованих інформаційних кампаній, від диверсійних актів до економічного тиску. Це вимагає розробки нових концептуальних підходів до інституціалізації публічного управління національною безпекою, що органічно поєднують стратегічну стабільність з операційною гнучкістю, забезпечують синергію зусиль різних суб'єктів безпеки при збереженні їх функціональної спеціалізації, створюють умови для випереджувальної адаптації до майбутніх невідомих форм агресії.

Проблематика публічного управління національною безпекою та його інституційного розвитку досліджується у працях таких вітчизняних науковців, як Г. Ситник, В. Богданович, С. Пирожков, О. Резнікова, В. Абрамов, С. Кондратов, Л. Шипілова, О. Суходоля, І. Тодоров, В. Ліпкан, О. Данильян, В. Цюкало, М. Рижков та ін.

Теоретичні та прикладні аспекти формування та реалізації державної політики у сфері національної безпеки, трансформації безпекових інститутів розглядаються у роботах таких дослідників, як М. Требін, Є. Березняк, С. Телешун, О. Валевський, І. Арістова, Ю. Барабаш, О. Джафарова, Л. Герасіна, О. Литвиненко, Г. Перепелиця, В. Смолянюк, М. Пашков, О. Кириченко, Т. Стародубцева та ін.

Феномен гібридної війни та її вплив на національну безпеку досліджують такі українські науковці, як В. Горбулін, Л. Величко, О. Власюк, В. Дзюндзюк, Б. Парахонський, Є. Камінський, М. Дорошко, Д. Дубов, Л. Компанцева, І. Рущенко, О. Литвиненко, Є. Лисицин, Я. Жарков та ін.

Значний внесок у дослідження гібридних загроз та інституційної

трансформації систем національної безпеки зробили такі зарубіжні науковці, як Ф. Хоффман, Дж. Маттіс, М. Галеотті, Т. Рід, Л. Фрідман, П. Мансур, Р. Гленн, Дж. Най, Б. Нільсен, К. Герасимов, І. Суворов та ін.

Проблематику інституціалізації та інституційного розвитку в публічному управлінні розробляють такі дослідники, як Д. Норт, Е. Остром, О. Вільямсон, Т. Веблен, Дж. Марч, Й. Олсен, П. Холл, а в українському науковому дискурсі – М. Білинська, О. Амосов, Н. Гавкалова, В. Мартиненко, А. Колодій, В. Бакуменко та ін.

Водночас, незважаючи на значний інтерес науковців до проблематики національної безпеки та гібридних загроз, питання інституціалізації публічного управління національною безпекою саме в умовах гібридної війни залишаються недостатньо дослідженими з точки зору цілісного системного підходу.

Зокрема, потребують подальшого вивчення теоретико-методологічні засади інституціалізації публічного управління національною безпекою в специфічних умовах гібридної війни, механізми оцінки інституційної зрілості безпекових структур, принципи побудови адаптивної архітектури системи безпеки, механізми координації між різнорідними суб'єктами безпеки в кризових ситуаціях, шляхи адаптації зарубіжного досвіду з урахуванням унікальності українського контексту, розробка концептуальної моделі та практичних механізмів інституційної трансформації сектору безпеки для ефективної протидії комплексним гібридним загрозам. Саме це зумовило вибір мети і завдань дисертаційного дослідження, його об'єкта та предмета.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційної роботи пов'язана з науково-дослідною роботою «Організаційно-правовий механізм модернізації публічного управління відповідно до стандартів "Good Governance"» (номер державної реєстрації 0120U105739), що виконувалась кафедрою права, національної безпеки та європейської інтеграції навчально-наукового інституту «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна. У

межах цієї роботи автором досліджено особливості інституціалізації публічного управління національною безпекою в умовах гібридної війни та розроблено рекомендації щодо її вдосконалення.

Метою роботи є теоретичне обґрунтування та розробка практичних рекомендацій щодо вдосконалення інституціалізації публічного управління національною безпекою в умовах гібридної війни в Україні.

Досягнення поставленої мети зумовило необхідність вирішення таких завдань:

– розкрити зміст і сутність публічного управління національною безпекою в умовах гібридної війни;

– визначити особливості гібридної війни як детермінанти трансформації системи публічного управління національною безпекою з урахуванням багатовимірного впливу гібридних загроз на інституційне середовище;

– обґрунтувати систему критеріїв оцінювання інституційної зрілості безпекових інститутів в умовах гібридної війни;

– проаналізувати нормативно-правове та організаційне забезпечення системи управління національною безпекою України з метою виявлення його відповідності викликам гібридної війни;

– дослідити та узагальнити зарубіжний досвід інституціалізації управління національною безпекою в умовах гібридних загроз для виявлення кращих практик, релевантних для України.

– розробити концептуальну модель інституціалізації публічного управління національною безпекою в умовах гібридної війни;

– обґрунтувати пріоритетні напрями вдосконалення інституційного забезпечення публічного управління національною безпекою України на основі аналізу вітчизняного та зарубіжного досвіду протидії гібридним загрозам.

Об’єктом дослідження є публічне управління національною безпекою.

Предметом дослідження є інституціалізація публічного управління

національною безпекою в умовах гібридної війни в Україні.

Методи дослідження. Теоретичною основою дослідження є фундаментальні положення теорії публічного управління, інституціональної теорії, теорії національної безпеки, теорії систем, кризового менеджменту, а також дослідження вітчизняних і зарубіжних учених з проблем управління національною безпекою в умовах гібридних загроз та інституційного розвитку безпекових структур.

Для досягнення поставленої мети та вирішення завдань дисертаційного дослідження автором було використано низку загальнонаукових та спеціальних методів:

– абстрагування, узагальнення, порівняння, логіко-семантичний аналіз – для з'ясування сутності інституціалізації публічного управління національною безпекою в умовах гібридної війни, виокремлення її специфічних характеристик та відмінностей від управління в конвенційних конфліктах, уточнення понятійно-категоріального апарату дослідження, зокрема таких ключових концептів як «інституціалізація», «інституційна зрілість», «гібридна війна», «адаптивна архітектура», «функціональні кластери»;

– системний аналіз та синтез – для розробки концептуальної моделі інституціалізації публічного управління національною безпекою як цілісної багаторівневої системи, що органічно інтегрує принципи функціонування, архітектурні елементи, механізми координації та адаптаційні спроможності; для виявлення системних взаємозв'язків між різними компонентами моделі та механізмів їх синергетичної взаємодії; для аналізу емерджентних властивостей системи національної безпеки, що виникають внаслідок інтеграції окремих елементів;

– класифікація та типологізація – для систематизації гібридних загроз за різними критеріями (за сферами прояву, рівнем інтенсивності, динамікою розвитку, ступенем прихованості), визначення типології організаційних структур у секторі безпеки, класифікації механізмів координації за характером

зв’язків (вертикальні/горизонтальні) та рівнями управління (стратегічний/оперативний/тактичний);

– інституційний аналіз – для дослідження формальних та неформальних інститутів у сфері національної безпеки, механізмів їх формування, трансформації та взаємодії; для виявлення інституційних обмежень та стимулів, що визначають поведінку акторів у безпековій сфері; для аналізу інституційних пасток та шляхозалежності в розвитку безпекових структур; для обґрунтування необхідності та напрямів інституційних реформ у секторі безпеки;

– структурно-функціональний аналіз – для дослідження організаційно-правових засад функціонування системи національної безпеки, аналізу функцій різних безпекових інститутів, механізмів їх взаємодії та координації, виявлення функціональних дублювань та лакун у розподілі відповідальності між суб’єктами безпеки, обґрунтування оптимальної функціональної архітектури системи;

– компаративний аналіз – для вивчення зарубіжного досвіду інституціалізації публічного управління національною безпекою в країнах НАТО та ЄС (зокрема США, Великобританії, Франції, Німеччини, Польщі, країн Балтії), виокремлення кращих практик організації міжвідомчої координації, побудови інтегрованих систем управління кризовими ситуаціями, розвитку адаптивних організаційних структур; для оцінювання релевантності міжнародних практик для українського контексту з урахуванням контекстуальних чинників (масштабу загроз, ресурсної забезпеченості, інституційної культури, геополітичного становища);

– SWOT-аналіз – для комплексної діагностики поточного стану системи публічного управління національною безпекою в Україні через виявлення сильних сторін (досвід протидії реальній гібридній агресії, високий рівень суспільної мобілізації, міжнародна підтримка), слабких сторін (відомча роз’єднаність, застарілі організаційні структури, недостатня правова база), можливостей (залучення міжнародної технічної допомоги, впровадження

інновацій, навчання на власному досвіді) та загроз (ескалація конфлікту, ресурсне виснаження, гібридні впливи), що дозволило обґрунтувати пріоритетні напрями модернізації системи;

– моделювання – для розробки концептуальної моделі інституціалізації публічного управління національною безпекою з визначенням базових принципів (системної цілісності, адаптивної архітектури, мережецентричності, інформаційної інтеграції, проактивності, розподіленої стійкості), архітектурних елементів (функціональні кластери, Національний центр стійкості, Регіональні центри безпеки), механізмів координації (вертикальної та горизонтальної) та адаптаційних спроможностей;

– прогнозування та сценарний аналіз – для обґрунтування перспективних напрямів еволюції гібридних загроз, передбачення можливих майбутніх форм агресії, розробки альтернативних сценаріїв розвитку безпекового середовища (оптимістичного, песимістичного, реалістичного) та відповідних траєкторій інституційної адаптації системи національної безпеки, що забезпечує стратегічну обґрунтованість запропонованих інституційних рішень.

Наукова новизна одержаних результатів полягає у вирішенні важливого науково-прикладного завдання – теоретичного обґрунтування та розробки практичних рекомендацій щодо вдосконалення інституціалізації публічного управління національною безпекою в умовах гібридної війни в Україні.

Новизна наукових результатів конкретизується в таких положеннях:

уперше:

– розроблено концептуальну модель інституціалізації публічного управління національною безпекою в умовах гібридної війни, яка на відміну від існуючих ґрунтується на принципах системної інтеграції та передбачає багаторівневу архітектуру з інноваційними елементами у вигляді функціональних кластерів замість традиційних відомчих структур,

Національного центру стійкості для забезпечення безперебійного функціонування критичної інфраструктури, Регіональних центрів безпеки та стійкості як інтегрованих міжвідомчих структур на обласному рівні, мережевої компоненти з горизонтальними зв'язками, інформаційної підсистеми на базі концепції єдиного інформаційного простору та вбудованих механізмів адаптації до еволюції гібридних загроз через раннє виявлення слабких сигналів, сценарне прогнозування, організаційну і технологічну гнучкість та когнітивну адаптивність, що забезпечує не лише протидію існуючим гібридним загрозам, а й випереджувальне пристосування до їх можливих майбутніх форм;

удосконалено:

– систему критеріїв та індикаторів оцінювання інституційної зрілості системи публічного управління національною безпекою шляхом інтеграції семи взаємопов'язаних вимірів: структурної, функціональної, нормативної, координаційної, адаптивної, культурної та інтеграційної зрілості, що комплексно відображають здатність безпекових інститутів ефективно функціонувати в умовах гібридної війни; на відміну від існуючих методик, які акцентують переважно на статичних формальних показниках, розроблена система критеріїв враховує динамічні характеристики інституційного розвитку, зокрема адаптивність до швидкозмінного характеру гібридних загроз, здатність до міжвідомчої інтеграції та стійкість до багатовекторних деструктивних впливів, що забезпечує можливість багатоаспектної діагностики інституційної спроможності та виявлення пріоритетних напрямів інституційного вдосконалення;

– структурно-функціональну модель публічного управління національною безпекою в умовах гібридної війни, яка базується на принципах багатовимірності, адаптивності та інтегрованості, що відрізняє її від традиційних моделей, орієнтованих на ієрархічність, сталість та секторальність; модель включає три взаємопов'язані компоненти: структурно-організаційний (створення гнучких мережевих форм координації замість

жорстких ієрархічних структур, формування міжвідомчих платформ взаємодії, розвиток механізмів публічно-приватного партнерства), процесуально-функціональний (стандартизація процедур ситуаційного аналізу та швидкого реагування, впровадження систем раннього попередження, автоматизація обміну інформацією між суб'єктами безпеки) та ціннісно-культурний (формування культури міжвідомчої співпраці, розвиток професійних компетенцій для роботи в умовах невизначеності, виховання стратегічного мислення у керівників безпекових структур);

– організаційну архітектуру сектору безпеки через обґрунтування переходу від функціонально-галузевого до процесно-орієнтованого принципу побудови структур, створення Інтегрованого командування сил безпеки та оборони з реальними повноваженнями оперативного управління всіма силовими компонентами незалежно від відомчої підпорядкованості, реорганізації розвідувальної спільноти через Національне розвідувальне агентство як єдиний аналітично-координаційний центр при збереженні функціональної спеціалізації служб на рівні первинного збору інформації, структурної інтеграції кіберсил через об'єднане Кіберкомандування з чітким функціональним розподілом між військовими, правоохоронними та захисними функціями;

дістали подальшого розвитку:

– теоретичне осмислення гібридної війни як детермінанти інституційної трансформації системи публічного управління національною безпекою через обґрунтування концепції множинної детермінації, що розкриває механізми одночасного впливу гібридних загроз на всі рівні інституційної організації безпекової сфери; при цьому конкретизовано каскадний ефект гібридної агресії, який проявляється у послідовному порушенні стабільності нормативного, організаційного, функціонального та культурного рівнів інституційної системи, створюючи необхідність комплексної інституційної відповіді, що виходить за межі традиційних секторальних підходів;

– механізми координації в системі управління національною безпекою, що передбачають поєднання вертикальної координації на основі каскадної системи узгодженого цілепокладання з використанням інструменту «стратегічних контрактів» та горизонтальної координації через систему спеціалізованих міжвідомчих комітетів при РНБО, спільні ситуаційні центри, інтегровані інформаційні системи з можливістю крос-відомчого доступу, уніфіковані стандарти та протоколи, а також перехід від відомчого до програмно-цільового фінансування через консолідований бюджет сектору безпеки і оборони.

– методичні підходи до компаративного аналізу зарубіжного досвіду інституціалізації управління національною безпекою в умовах гібридних загроз через розробку системи критеріїв оцінювання релевантності міжнародних практик для українського контексту; на відміну від існуючих підходів, що зосереджуються на формальному порівнянні організаційних структур або правових норм, запропонований підхід враховує контекстуальні чинники: масштаб і характер загроз, ресурсну забезпеченість, особливості інституційної культури, ступінь суспільної мобілізації, геополітичне становище країни.

Практичне значення одержаних результатів визначається можливістю використання її положень та рекомендацій для вдосконалення державної політики у сфері національної безпеки та механізмів її реалізації в Україні.

Запропонований комплекс взаємопов’язаних заходів для підвищення координаційної та адаптивної зрілості системи цивільного захисту в умовах гібридної війни прийнято для впровадження у Головному управлінні Державної служби України з надзвичайних ситуацій у Харківській області.

Вставити дані з довідок про впровадження якщо такі є.

Результати дослідження можуть бути корисними для Ради національної безпеки і оборони України, Офісу Президента України, Кабінету Міністрів України, Міністерства оборони України, Служби безпеки України, Служби зовнішньої розвідки України, розвідувального управління Генерального штабу Збройних Сил України, Національної поліції України, Державної прикордонної служби України, центральних та місцевих органів виконавчої влади, органів місцевого самоврядування при розробці та реалізації програм і планів у сфері національної безпеки, впровадженні механізмів міжвідомчої координації, вдосконаленні системи реагування на гібридні загрози.

Запропонована концептуальна модель інституціалізації публічного управління національною безпекою в умовах гібридної війни може використовуватись органами державної влади як методологічна основа для організації діяльності у сфері національної безпеки, розробки та впровадження відповідних стратегій, програм та планів, проведення інституційного аудиту безпекових структур, планування заходів з підвищення інституційної спроможності та адаптивності системи національної безпеки. Розроблена система критеріїв оцінювання інституційної зрілості може бути використана для проведення регулярної діагностики стану безпекових інститутів, виявлення проблемних аспектів їх функціонування, визначення пріоритетних напрямів інституційного вдосконалення, моніторингу ефективності впроваджених реформ.

Запропоновані організаційні механізми трансформації сектору безпеки можуть бути використані для практичної модернізації організаційної архітектури системи національної безпеки, подолання відомчої фрагментації, підвищення ефективності міжвідомчої координації та оперативності реагування на комплексні гібридні загрози. Також отримані результати і рекомендації можуть бути використані для вдосконалення нормативно-правової бази у сфері національної безпеки, створення сучасної правової

інфраструктури для ефективної протидії гібридним загрозам.

Особистий внесок здобувача. Дисертаційне дослідження є самостійною науковою працею автора. Всі наукові результати, висновки і практичні рекомендації, що наведені в дисертації, отримані автором особисто. З наукових праць, опублікованих у співавторстві, в дисертаційній роботі використані лише ті ідеї та положення, які є результатом особистої роботи здобувача.

Апробація результатів дисертації. Основні результати дисертаційного дослідження обговорювались на міжнародних науково-практичних конференціях, VIII Міжнародній науково-практичній конференції «Міжнародна та національна безпека: теоретичні і прикладні аспекти» (м. Дніпро, 2024), XXV Міжнародному науковому конгресі «Публічне управління XXI століття: основні виклики післявоєнної відбудови» (м. Харків, 2025), засіданнях кафедри права, національної безпеки та європейської інтеграції.

Публікації. Основні положення дисертаційного дослідження висвітлено у 6 публікаціях, зокрема, в 4 публікаціях у наукових фахових виданнях.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків та списку використаних джерел. Її повний обсяг становить 256 сторінок. Список використаних джерел налічує 224 найменування (на 20 сторінках), у тому числі іноземною мовою – 133.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНСТИТУЦІАЛІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

1.1. Сутність та зміст інституціалізації публічного управління національною безпекою

Інституціалізація в системі публічного управління представляє собою фундаментальний процес формування, закріплення та розвитку формальних і неформальних правил, норм, процедур та організаційних структур, які регулюють взаємодію між різними суб'єктами управлінської діяльності та забезпечують стабільність і передбачуваність функціонування державних і суспільних механізмів. Цей процес охоплює не лише створення нових інституцій або реформування існуючих, а й глибинну трансформацію управлінської культури, цінностей та поведінкових моделей, які визначають характер взаємовідносин між владою та суспільством.

Сутність інституціалізації полягає у перетворенні спонтанних, ситуативних або хаотичних соціальних практик на впорядковані, регламентовані та відтворювані форми діяльності, які набувають характеру стійких інституційних утворень. У контексті публічного управління це означає формування цілісної системи взаємопов'язаних елементів, що включає правові норми, організаційні структури, управлінські процедури, механізми контролю та відповідальності, а також неформальні практики взаємодії, які в сукупності забезпечують ефективне виконання державою її функцій [181]. При цьому природа інституціалізації в публічному управлінні має дуалістичний характер, оскільки вона одночасно виступає як процес і як результат. Як процес, інституціалізація являє собою динамічну послідовність етапів формування інституційного середовища, починаючи від виникнення потреби в упорядкуванні певної сфери суспільних відносин і завершуючи

створенням стійких інституційних форм. Як результат, вона постає у вигляді сформованої системи інститутів, які забезпечують стабільність та ефективність публічного управління. Ця подвійність природи інституціалізації обумовлює складність її дослідження та необхідність застосування комплексного методологічного підходу.

Теоретичне осмислення інституціалізації в публічному управлінні базується на синтезі різних наукових підходів. Соціологічний підхід акцентує увагу на соціальних практиках та нормах, які формуються в процесі взаємодії різних суспільних груп та поступово набувають інституційного характеру. Правовий підхід зосереджується на формально-юридичних аспектах створення та функціонування інститутів публічного управління, розглядаючи інституціалізацію передусім як процес правового оформлення управлінських відносин [185]. Організаційний підхід трактує інституціалізацію як формування організаційних структур та механізмів, які забезпечують реалізацію управлінських функцій. Системний підхід дозволяє розглядати інституціалізацію як комплексний процес формування цілісної системи взаємопов'язаних інститутів, які функціонують у динамічному середовищі та постійно адаптуються до змін зовнішніх і внутрішніх умов.

Важливим аспектом розуміння природи інституціалізації є її зв'язок із легітимністю публічної влади. Інституціалізація виступає механізмом легітимації управлінських рішень та дій через їх вписування в усталені інституційні рамки, які сприймаються суспільством як правильні та справедливі. Водночас легітимність самих інститутів публічного управління залежить від того, наскільки вони відповідають суспільним очікуванням та ефективно виконують покладені на них функції. Таким чином, між інституціалізацією та легітимністю існує діалектичний взаємозв'язок, який забезпечує стійкість системи публічного управління.

Процес інституціалізації в публічному управлінні характеризується певними закономірностями та особливостями. По-перше, він має інерційний характер, оскільки сформовані інститути прагнуть до самозбереження та

опираються змінам. По-друге, інституціалізація відбувається нерівномірно в різних сферах публічного управління, що може призводити до інституційних розривів та дисбалансів. По-третє, на процес інституціалізації впливають як об'єктивні фактори (економічні умови, технологічний розвиток, геополітична ситуація), так і суб'єктивні чинники (політична воля, управлінська культура, суспільні настрої).

Сучасне розуміння інституціалізації в публічному управлінні неможливе без урахування концепції інституційних змін. На відміну від традиційного підходу, який розглядав інститути як статичні утворення, сучасна теорія визнає їх динамічну природу та здатність до трансформації. Інституційні зміни можуть відбуватися як еволюційним шляхом через поступове накопичення малих змін, так і революційним шляхом через радикальну трансформацію або заміну існуючих інститутів новими [122]. При цьому успішність інституційних змін значною мірою залежить від їх узгодженості з існуючим інституційним середовищем та готовності суспільства до сприйняття нових інституційних форм. Особливого значення набуває питання інституційної спроможності, яка визначається як здатність інститутів публічного управління ефективно виконувати покладені на них функції та адаптуватися до змін середовища. Інституційна спроможність включає такі компоненти: ресурсне забезпечення (фінансові, кадрові, інформаційні ресурси), організаційну структуру (чіткий розподіл повноважень та відповідальності), управлінські процедури (стандартизовані процеси прийняття та реалізації рішень), а також інституційну культуру (цінності, норми поведінки, неформальні правила взаємодії).

Концептуалізація інституціалізації в публічному управлінні потребує також урахування феномену інституційних пасток – неефективних стійких інститутів, які виникають внаслідок короткострокової раціональності акторів або помилкових управлінських рішень. Інституційні пастки можуть проявлятися у вигляді корупційних практик, бюрократичної тяганини, дублювання функцій різними органами влади, неефективного розподілу

ресурсів. Подолання інституційних пасток вимагає цілеспрямованих зусиль з реформування системи публічного управління та створення стимулів для переходу до більш ефективних інституційних форм.

Важливим виміром інституціалізації є її культурно-ціннісний аспект. Формальні інститути публічного управління можуть ефективно функціонувати лише за умови їх відповідності неформальним нормам та цінностям, які поділяються суспільством. Невідповідність між формальними та неформальними інститутами призводить до виникнення інституційного дуалізму, коли офіційні правила та процедури існують паралельно з неофіційними практиками, які часто мають більший вплив на реальну поведінку акторів [182]. Подолання інституційного дуалізму вимагає не лише зміни формальних правил, а й трансформації управлінської культури та суспільних цінностей.

Сучасні тенденції розвитку публічного управління висувають нові вимоги до процесів інституціалізації. Глобалізація, цифровізація, зростання складності та невизначеності управлінського середовища вимагають формування більш гнучких та адаптивних інституційних форм. Традиційна модель ієрархічних бюрократичних інститутів поступово доповнюється або заміщується мережевими формами організації, які передбачають горизонтальну координацію та партнерство між різними акторами. Це призводить до виникнення нових форм інституціалізації, таких як публічно-приватне партнерство, участь громадськості в управлінні, міжвідомча координація, транскордонне співробітництво. Особливої уваги заслуговує проблема вимірювання та оцінювання рівня інституціалізації в публічному управлінні. Складність та багатоаспектність цього феномену ускладнюють розробку універсальних критеріїв та показників. Водночас існують певні індикатори, які дозволяють оцінити ступінь інституціалізації: стабільність та передбачуваність функціонування інститутів, чіткість розподілу повноважень та відповідальності, наявність формалізованих процедур та правил, рівень дотримання цих правил на практиці, ефективність виконання інститутами

покладених на них функцій, здатність до адаптації та інновацій.

Інституціалізація в публічному управлінні тісно пов'язана з концепцією good governance (належне врядування), яка передбачає формування таких інституційних умов, які забезпечують ефективне, прозоре, підзвітне та інклюзивне управління. Принципи good governance – верховенство права, участь громадськості, прозорість, відповідальність, консенсус, справедливість та інклюзивність, ефективність та результативність – виступають орієнтирами для інституційного розвитку системи публічного управління [203]. Реалізація цих принципів вимагає комплексної інституційної трансформації, яка охоплює правову систему, організаційні структури, управлінські процеси та культуру.

Аналіз сучасних тенденцій свідчить про зростання ролі наднаціональних та транснаціональних інститутів у системі публічного управління. Європейська інтеграція, членство в міжнародних організаціях, участь у глобальних регуляторних режимах створюють нові виміри інституціалізації, які виходять за межі національної держави. Це призводить до формування багаторівневої системи управління, де національні інститути взаємодіють з наднаціональними та субнаціональними інститутами. Така багаторівневість створює додаткові виклики для забезпечення узгодженості та ефективності інституційної системи. Тобто національна безпека як об'єкт публічного управління являє собою складну багатовимірну систему, що охоплює сукупність умов, факторів та механізмів, які забезпечують захищеність життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз. Концептуалізація національної безпеки в контексті публічного управління передбачає розуміння її не лише як стану захищеності, а й як динамічного процесу, що потребує постійного управлінського впливу, координації зусиль різних суб'єктів та адаптації до змін безпекового середовища.

При цьому еволюція концептуальних підходів до розуміння національної безпеки демонструє поступовий перехід від вузького мілітаристського трактування до широкого інтегрального підходу. Традиційна

парадигма національної безпеки, що домінувала протягом холодної війни, зводила її переважно до військово-політичних аспектів та зосереджувалася на захисті територіальної цілісності та суверенітету держави від зовнішньої агресії [110]. Однак трансформація глобального безпекового середовища, поява нових типів загроз та усвідомлення взаємозалежності різних вимірів безпеки призвели до формування більш комплексного розуміння цього феномену. Через це сучасний підхід до національної безпеки як об'єкта публічного управління базується на секторальній концепції, яка виокремлює кілька взаємопов'язаних вимірів: військовий, політичний, економічний, соціальний, екологічний, інформаційний, кібернетичний. Кожен із цих секторів має власну специфіку загроз, суб'єктів забезпечення безпеки та інструментів управлінського впливу, водночас усі вони перебувають у тісному взаємозв'язку та взаємозалежності. Така багатовимірність національної безпеки вимагає застосування міжсекторального підходу в публічному управлінні, який передбачає координацію діяльності різних відомств та інституцій.

Концептуальне осмислення національної безпеки неможливе без урахування її суб'єктно-об'єктної структури. З одного боку, держава виступає основним суб'єктом забезпечення національної безпеки, формуючи відповідну політику, створюючи спеціалізовані інституції та виділяючи необхідні ресурси. З іншого боку, в сучасних умовах зростає роль недержавних акторів – громадянського суспільства, бізнесу, міжнародних організацій – у забезпеченні різних аспектів національної безпеки [101]. Це призводить до трансформації традиційної державоцентричної моделі управління національною безпекою в бік більш інклюзивної моделі, яка передбачає залучення широкого кола стейкхолдерів.

Важливим концептуальним підходом є розуміння національної безпеки через призму теорії систем. Системний підхід дозволяє розглядати національну безпеку як цілісну систему, що складається з взаємопов'язаних елементів (суб'єктів, об'єктів, загроз, механізмів забезпечення), функціонує в

певному середовищі та характеризується емерджентними властивостями. Ключовими характеристиками системи національної безпеки є її відкритість (взаємодія із зовнішнім середовищем), динамічність (постійні зміни та адаптація), ієрархічність (наявність різних рівнів організації), нелінійність (непропорційність між впливами та результатами).

Концепція людської безпеки, що набула поширення з 1990-х років, також суттєво розширила традиційне розуміння національної безпеки, поставивши в центр уваги не державу, а людину. Цей підхід акцентує увагу на забезпеченні базових потреб людини – свободи від страху, свободи від нужди, свободи жити в гідності. Інтеграція концепції людської безпеки в систему публічного управління вимагає переорієнтації безпекової політики з виключно державних інтересів на потреби та права громадян, що передбачає розвиток соціальних програм, забезпечення доступу до базових послуг, захист прав людини [138].

Критично важливим для розуміння національної безпеки як об’єкта публічного управління є концепція безпекового середовища. Безпекове середовище являє собою сукупність внутрішніх та зовнішніх умов, факторів та процесів, які впливають на стан національної безпеки. Сучасне безпекове середовище характеризується високим рівнем турбулентності, невизначеності, комплексності та амбівалентності (відомий акронім VUCA – volatility, uncertainty, complexity, ambiguity). Управління національною безпекою в таких умовах вимагає розвитку адаптивних механізмів, здатності до швидкого реагування на зміни та проактивного підходу до виявлення потенційних загроз.

Концептуалізація загроз національній безпеці також зазнала суттєвої трансформації. Традиційний поділ на внутрішні та зовнішні загрози стає дедалі більш умовним в епоху глобалізації та взаємозалежності. Сучасні загрози часто мають транскордонний, гібридний та асиметричний характер, що ускладнює їх ідентифікацію та протидію. Крім того, спостерігається зростання ролі нетрадиційних загроз – тероризму, організованої злочинності,

кіберзагроз, пандемій, кліматичних змін, міграційних криз. Така трансформація природи загроз вимагає відповідної адаптації концептуальних підходів та управлінських механізмів у сфері національної безпеки.

Як зазначають багато сучасних дослідників, важливе місце в концептуалізації національної безпеки займає проблема балансу між безпекою та свободою. Забезпечення національної безпеки часто вимагає певних обмежень громадянських свобод, посилення контролю з боку держави, розширення повноважень силових структур. Водночас надмірна секюритизація може призвести до згортання демократичних інститутів та порушення прав людини. Тому пошук оптимального балансу між безпековими імперативами та демократичними цінностями становить одне з ключових завдань публічного управління у сфері національної безпеки.

Дедалі більшого значення в сучасному розумінні національної безпеки набуває концепція стійкості (resilience). На відміну від традиційного підходу, орієнтованого на запобігання загрозам, концепція стійкості акцентує увагу на здатності системи абсорбувати шоки, адаптуватися до змін та відновлюватися після криз. Формування національної стійкості передбачає розвиток не лише державних інституцій, а й суспільства в цілому – підвищення його згуртованості, розвиток горизонтальних зв'язків, формування культури безпеки [180]. Інтеграція концепції стійкості в систему публічного управління національною безпекою вимагає переходу від реактивної до проактивної моделі, від жорсткого планування до адаптивного управління, від централізованого контролю до розподіленої відповідальності.

Через зазначені особливості взаємозв'язок між інституціалізацією та ефективністю управління національною безпекою являє собою складну діалектичну залежність, де рівень розвитку інституційного середовища безпосередньо впливає на здатність держави забезпечувати захист національних інтересів, а ефективність безпекового управління, у свою чергу, створює передумови для подальшого інституційного розвитку. Цей взаємозв'язок проявляється через множину механізмів та каналів впливу, які

формують цілісну систему взаємодетермінації інституційних та управлінських процесів у безпековій сфері. При цьому інституціалізація створює структурні передумови для ефективного управління національною безпекою через формування стійких організаційних форм, чіткий розподіл повноважень та відповідальності, стандартизацію процедур прийняття та реалізації рішень. Наявність розвинених інститутів дозволяє подолати фрагментарність та ситуативність управлінських дій, забезпечити наступність безпекової політики незалежно від зміни політичного керівництва, створити умови для накопичення інституційної пам'яті та досвіду [139]. Водночас слабка інституціалізація призводить до хаотичності управління, дублювання функцій, конфліктів компетенцій, неефективного використання ресурсів та, як наслідок, нездатності адекватно реагувати на безпекові виклики.

Ефективність управління національною безпекою значною мірою залежить і від якості інституційного дизайну – того, наскільки структура та функції безпекових інститутів відповідають характеру загроз та особливостям безпекового середовища. Оптимальний інституційний дизайн передбачає досягнення балансу між спеціалізацією та інтеграцією, централізацією та децентралізацією, ієрархічністю та мережевістю, формальністю та гнучкістю. Невідповідність інституційного дизайну реальним потребам безпекового управління призводить до зниження його ефективності навіть за наявності достатніх ресурсів та політичної волі.

Критично важливим аспектом взаємозв'язку інституціалізації та ефективності є проблема координації між різними суб'єктами забезпечення національної безпеки. Високий рівень інституціалізації передбачає наявність формалізованих механізмів міжвідомчої взаємодії, чітких протоколів обміну інформацією, узгоджених процедур спільного планування та проведення операцій [188]. Ефективна координація дозволяє досягти синергетичного ефекту від діяльності різних безпекових структур, уникнути дублювання зусиль та забезпечити комплексний підхід до вирішення безпекових проблем. Натомість слабка координація, зумовлена недостатньою інституціалізацією,

призводить до фрагментації безпекової системи, міжвідомчих конфліктів та зниження загальної ефективності.

Інституціалізація впливає на ефективність управління національною безпекою не в останню чергу через механізм легітимації. Легітимні інститути користуються довірою суспільства, що забезпечує підтримку безпекової політики, готовність громадян співпрацювати з безпековими структурами, соціальну мобілізацію в умовах кризи. Високий рівень легітимності безпекових інститутів дозволяє знизити трансакційні витрати на примусове забезпечення виконання рішень, підвищити ефективність використання обмежених ресурсів, створити сприятливе середовище для реалізації довгострокових безпекових стратегій. І навпаки, нелегітимні або слабко легітимовані інститути стикаються з опором суспільства, що суттєво знижує ефективність їхньої діяльності.

Безумовно, важливим виміром взаємозв'язку інституціалізації та ефективності є здатність до адаптації та інновацій. Парадоксальність цього взаємозв'язку полягає в тому, що, з одного боку, інституціалізація передбачає стабільність та передбачуваність, а з іншого – сучасне безпекове середовище вимагає гнучкості та інноваційності [199]. Вирішення цього парадоксу лежить у площині формування адаптивних інститутів, які поєднують стабільність базових принципів та процедур із здатністю до модифікації операційних практик відповідно до змін середовища, тому ефективність управління національною безпекою в умовах високої невизначеності прямо залежить від того, наскільки інституційна система здатна генерувати та впроваджувати інновації без втрати своєї цілісності та функціональності.

Ще один важливий вимір, ресурсний, взаємозв'язку інституціалізації та ефективності проявляється через вплив інституційного середовища на алокацію та використання ресурсів у безпековій сфері. Розвинені інститути забезпечують прозорість бюджетного процесу, обґрунтованість розподілу коштів між різними напрямами безпекової діяльності, ефективний контроль за цільовим використанням ресурсів. Інституціалізовані механізми планування

та програмування дозволяють оптимізувати співвідношення між поточними та капітальними витратами, забезпечити збалансований розвиток різних компонентів безпекової системи. Слабка інституціалізація, навпаки, створює умови для неефективного використання ресурсів, корупції, недофінансування критично важливих напрямів.

У свою чергу, кадровий аспект взаємозв'язку інституціалізації та ефективності відіграє ключову роль у забезпеченні якості управління національною безпекою. Інституціалізація кадрової політики передбачає формування прозорих механізмів відбору, підготовки, просування та ротації кадрів, систему безперервного професійного розвитку, об'єктивні критерії оцінювання результатів діяльності. Наявність таких механізмів дозволяє формувати професійний кадровий корпус, здатний ефективно вирішувати складні безпекові завдання. Водночас інституційні патології – кумівство, політизація призначень, відсутність кар'єрних ліфтів – призводять до деградації кадрового потенціалу та зниження ефективності управління.

Інформаційно-аналітичний вимір взаємозв'язку проявляється через вплив інституціалізації на якість інформаційного забезпечення процесів прийняття рішень у сфері національної безпеки. Розвинені інституційні механізми збору, обробки, аналізу та поширення інформації створюють основу для обґрунтованих управлінських рішень, своєчасного виявлення загроз, адекватної оцінки ситуації. Інституціалізація інформаційно-аналітичної діяльності передбачає не лише створення відповідних структур, а й формування культури розробки політики, основаної на доказах, яка базується на об'єктивних даних та науковому аналізі. Недостатня інституціалізація цієї сфери призводить до прийняття рішень на основі неповної або викривленої інформації, що критично знижує їх ефективність.

Темпоральний аспект взаємозв'язку інституціалізації та ефективності виявляється в різних часових горизонтах їхнього взаємовпливу. У короткостроковій перспективі інституціалізація може навіть знижувати оперативну ефективність через необхідність дотримання формальних

процедур, бюрократичні затримки, опір змінам. Однак у середньо- та довгостроковій перспективі інституціалізація створює передумови для сталого підвищення ефективності через накопичення досвіду, вдосконалення процедур, формування організаційної культури. Розуміння цієї темпоральної динаміки критично важливе для вироблення збалансованого підходу до інституційного розвитку безпекової сфери.

Міжнародний вимір взаємозв'язку інституціалізації та ефективності набуває особливого значення в умовах глобалізації безпекових викликів. Інтеграція національної системи управління безпекою в міжнародні безпекові структури вимагає досягнення певного рівня інституційної сумісності – гармонізації стандартів, процедур, організаційних форм [153]. Ефективність участі в міжнародному безпековому співробітництві прямо залежить від того, наскільки національні інститути здатні взаємодіяти з відповідними міжнародними інституціями. Водночас міжнародна співпраця може виступати драйвером інституційного розвитку через трансфер кращих практик та технічну допомогу.

Діалектична природа взаємозв'язку інституціалізації та ефективності проявляється також у тому, що надмірна інституціалізація може призводити до зниження ефективності через бюрократизацію, ригідність, втрату здатності до швидкого реагування. Феномен «інституційного склерозу» виникає, коли інститути стають самоціллю, а не засобом забезпечення національної безпеки, коли дотримання процедур стає важливішим за досягнення результатів. Тому критично важливим є пошук оптимального рівня інституціалізації, який забезпечує необхідну стабільність та передбачуваність без втрати гнучкості та адаптивності. Для цього структурно-функціональні компоненти інституціалізації безпекового управління формують комплексну архітектуру, що забезпечує системність, цілісність та ефективність функціонування національної безпеки як об'єкта публічного управління. Ці компоненти охоплюють організаційні структури, функціональні підсистеми, управлінські механізми та процедури, які у своїй сукупності створюють інституційний

каркас системи забезпечення національної безпеки. Розуміння природи та особливостей функціонування кожного з цих компонентів є критично важливим для забезпечення ефективної інституціалізації безпекового управління.

Організаційно-структурний компонент представлений системою державних органів та інституцій, що здійснюють функції у сфері національної безпеки. Центральне місце в цій системі займають вищі органи державної влади – глава держави, парламент, уряд, які визначають основні напрями безпекової політики та здійснюють стратегічне керівництво. Спеціалізовані безпекові структури – міністерства оборони, внутрішніх справ, спеціальні служби, правоохоронні органи – реалізують оперативне управління в межах своїх компетенцій. Координаційні органи, такі як ради національної безпеки, забезпечують узгодження діяльності різних відомств та вироблення комплексних рішень [164]. Ефективність організаційно-структурного компонента залежить від чіткості розподілу повноважень, відсутності дублювання функцій, оптимальності управлінських ланцюгів.

Нормативно-правовий компонент інституціалізації охоплює систему законодавчих та підзаконних актів, що регулюють відносини у сфері національної безпеки. Конституційні норми визначають основи безпекової політики та розподіл повноважень між гілками влади. Базові закони про національну безпеку встановлюють концептуальні засади, принципи, механізми забезпечення безпеки. Галузеве законодавство регламентує діяльність окремих безпекових структур та специфічні аспекти безпекової діяльності. Підзаконні акти деталізують процедури та механізми реалізації законодавчих норм. Якість нормативно-правового компонента визначається його повнотою, несуперечливістю, адекватністю реальним потребам безпекового управління.

Функціональний компонент структурується через основні функції безпекового управління: аналітично-прогностичну, планувальну, організаційну, координаційну, контрольну. Аналітично-прогностична функція

забезпечує виявлення та оцінювання загроз, моніторинг безпекового середовища, розробку сценаріїв розвитку ситуації. Планувальна функція передбачає формування стратегій, програм, планів у сфері національної безпеки. Організаційна функція спрямована на мобілізацію ресурсів та забезпечення виконання планів. Координаційна функція забезпечує узгодження дій різних суб'єктів безпекової діяльності. Контрольна функція передбачає моніторинг виконання рішень та оцінювання їх ефективності [222].

Процедурно-технологічний компонент включає стандартизовані процедури та алгоритми діяльності в різних режимах функціонування системи національної безпеки. Процедури повсякденної діяльності регламентують рутинні операції з моніторингу, аналізу, планування. Процедури кризового реагування визначають порядок дій в умовах загострення безпекової ситуації. Процедури надзвичайного стану встановлюють особливий режим функціонування в умовах найвищих загроз. Технологічний аспект охоплює методи та інструменти реалізації безпекових функцій, включаючи інформаційні технології, системи зв'язку, аналітичні методики.

Ресурсний компонент інституціалізації формується через механізми акумуляції, розподілу та використання різних видів ресурсів для забезпечення національної безпеки. Фінансові ресурси включають бюджетні асигнування, позабюджетні кошти, міжнародну допомогу. Людські ресурси охоплюють кадровий склад безпекових структур, резерви, мобілізаційний потенціал. Матеріально-технічні ресурси представлені озброєнням, технікою, інфраструктурою. Інформаційні ресурси включають бази даних, аналітичні системи, розвідувальну інформацію [131]. Ефективність ресурсного компонента визначається не лише обсягом наявних ресурсів, а й механізмами їх раціонального використання.

Комунікаційний компонент забезпечує взаємодію між різними елементами системи безпекового управління та зв'язок із зовнішнім середовищем. Внутрішні комунікації охоплюють канали обміну інформацією між безпековими структурами, механізми координації, системи оперативного

управління. Зовнішні комунікації включають взаємодію з громадськістю, міжнародними партнерами, засобами масової інформації. Особливе значення має стратегічна комунікація як інструмент формування сприятливого інформаційного середовища для реалізації безпекової політики. Розвиненість комунікаційного компонента визначає швидкість реагування системи на виклики та здатність до скоординованих дій.

Культурно-ціннісний компонент інституціалізації представлений системою норм, цінностей, традицій, що формують організаційну культуру безпекових структур та культуру безпеки суспільства в цілому. Професійна етика визначає стандарти поведінки представників безпекових структур, їх відданість національним інтересам, готовність до самопожертви. Корпоративна культура формує внутрішню згуртованість безпекових інституцій, механізми передачі досвіду, традиції служби. Суспільна культура безпеки визначає ставлення громадян до питань національної безпеки, готовність до співпраці з безпековими структурами, рівень безпекової свідомості.

Інноваційно-адаптивний компонент відображає здатність системи безпекового управління до розвитку та адаптації в умовах змін середовища. Інноваційна складова включає механізми генерування нових ідей, технологій, організаційних рішень у безпековій сфері. Дослідницькі центри, аналітичні структури, експериментальні підрозділи створюють інтелектуальну основу для інновацій. Адаптивна складова забезпечує гнучкість системи, здатність до модифікації структур та процедур відповідно до нових викликів. Механізми зворотного зв’язку, оцінювання ефективності, організаційного навчання формують адаптивний потенціал системи.

Контрольно-наглядовий компонент забезпечує підзвітність та відповідальність у системі безпекового управління. Парламентський контроль реалізується через спеціалізовані комітети, бюджетні процедури, парламентські розслідування. Судовий контроль забезпечує законність діяльності безпекових структур. Громадський контроль здійснюється через

інститути громадянського суспільства, незалежні ЗМІ, громадські ради [105]. Внутрішній контроль включає системи інспектування, внутрішнього аудиту, службових розслідувань. Ефективність контрольно-наглядового компонента є запорукою демократичного характеру системи національної безпеки.

Міжнародно-інтеграційний компонент відображає включеність національної системи безпекового управління в міжнародні безпекові структури та механізми. Двосторонні безпекові угоди формують мережу партнерських відносин. Участь у міжнародних безпекових організаціях забезпечує колективний вимір безпеки. Імплементація міжнародних стандартів та практик сприяє підвищенню ефективності національної системи. Механізми обміну інформацією, спільних навчань, операцій формують практичний вимір міжнародної співпраці (рис. 1.1).

Все зазначене свідчить про комплексність феномену національної безпеки, що, у свою чергу, вимагає застосування багатовимірної системи критеріїв та показників, які охоплюють різні аспекти інституційного розвитку та дозволяють здійснювати як якісну, так і кількісну оцінку.

Так, структурна зрілість як базовий критерій відображає ступінь сформованості організаційної архітектури системи управління національною безпекою. Цей критерій включає оцінку повноти охоплення всіх сфер національної безпеки відповідними інституціями, раціональності розподілу функцій та повноважень, оптимальності організаційної структури з точки зору управлінської ефективності. Показниками структурної зрілості виступають: наявність всіх необхідних інституційних ланок для забезпечення національної безпеки; чіткість вертикальних та горизонтальних зв’язків між інституціями; відсутність дублювання функцій та інституційних лакун; збалансованість централізації та децентралізації управлінських повноважень; гнучкість організаційної структури та її здатність до реконфігурації відповідно до змін безпекового середовища.

Функціональна зрілість характеризує здатність системи управління національною безпекою ефективно виконувати весь спектр необхідних

функцій – від стратегічного планування до оперативного реагування на загрози.

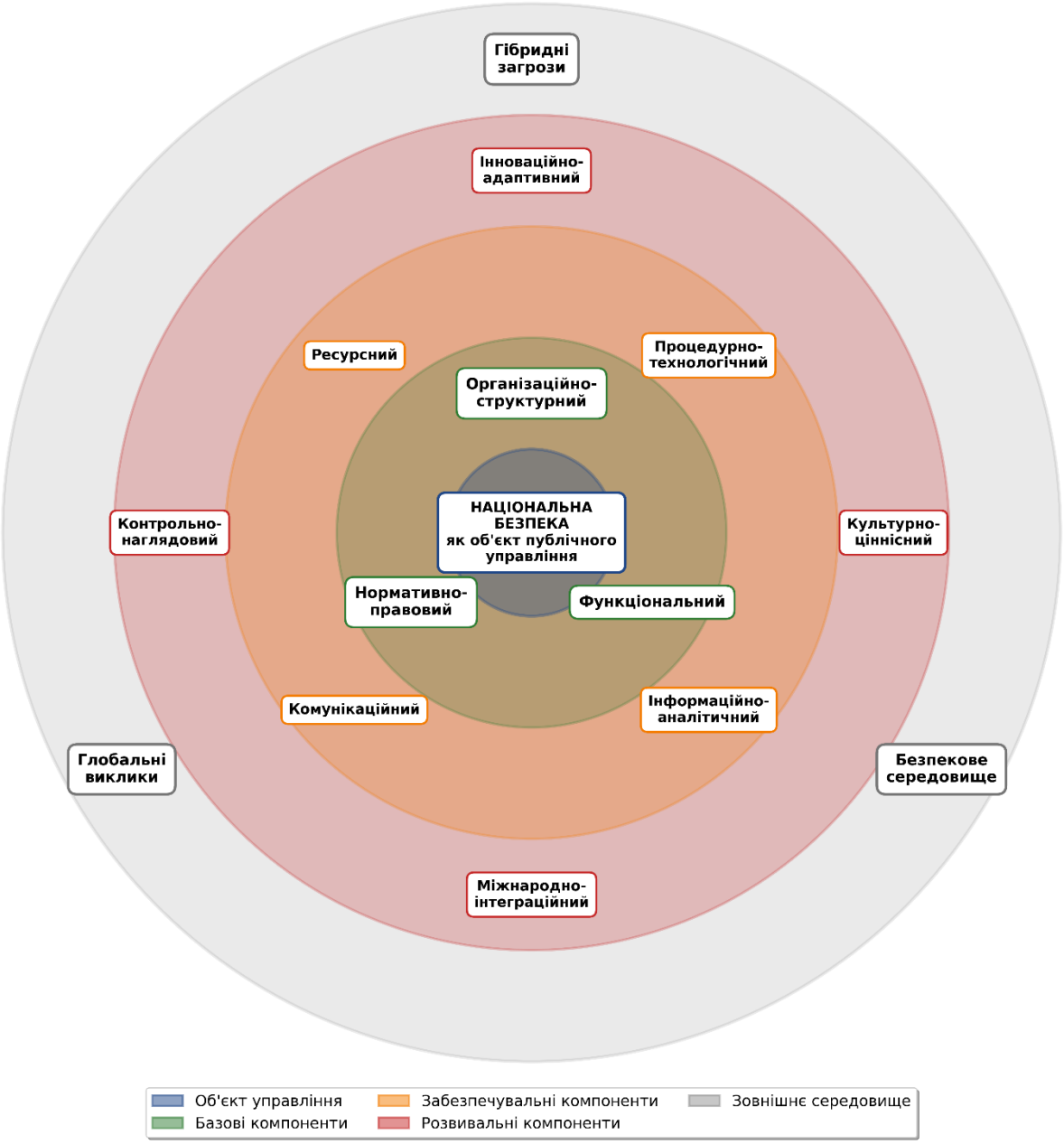

Рис. 1.1. Структурно-функціональна модель публічного управління національною безпекою з урахуванням гібридних загроз

Оцінка функціональної зрілості передбачає аналіз того, наскільки повно та якісно реалізуються основні функції безпекового управління, чи існують

механізми їх постійного вдосконалення. Ключовими показниками є: ефективність системи раннього попередження та виявлення загроз; якість стратегічного планування та його зв'язок з оперативною діяльністю; швидкість та адекватність реагування на кризові ситуації; здатність до міжвідомчої координації при вирішенні комплексних безпекових завдань; результативність превентивних заходів щодо запобігання загрозам.

Нормативно-правова зрілість відображає ступінь розвитку правової бази, що регулює функціонування системи національної безпеки. Цей критерій охоплює не лише наявність необхідних законодавчих та нормативних актів, а й їх якість, узгодженість, відповідність сучасним викликам та міжнародним стандартам. Показники нормативно-правової зрілості включають: повноту правового регулювання всіх аспектів забезпечення національної безпеки; відсутність правових колізій та прогалин; чіткість правових механізмів розподілу повноважень та відповідальності; наявність ефективних правових процедур для різних режимів функціонування системи безпеки; регулярність оновлення нормативно-правової бази відповідно до еволюції безпекового середовища.

Ресурсна зрілість характеризує спроможність системи управління національною безпекою акумулювати, розподіляти та ефективно використовувати необхідні ресурси. Цей критерій передбачає оцінку не лише обсягів наявних ресурсів, а й механізмів управління ними, їх відповідності реальним потребам та пріоритетам. Індикаторами ресурсної зрілості є: достатність фінансового забезпечення для виконання завдань національної безпеки; ефективність механізмів бюджетного планування та контролю; оптимальність структури видатків на різні компоненти безпекової системи; якість кадрового забезпечення та системи професійного розвитку персоналу; рівень технологічного оснащення безпекових структур; розвиненість резервних потужностей для реагування на кризові ситуації.

Процесна зрілість відображає ступінь формалізації, стандартизації та оптимізації управлінських процесів у системі національної безпеки. Високий

рівень процесної зрілості означає, що ключові процеси чітко визначені, документовані, регулярно аналізуються та вдосконалюються. Показниками процесної зрілості виступають: наявність формалізованих процедур для всіх критичних процесів; ступінь автоматизації рутинних операцій; швидкість проходження управлінських циклів; ефективність механізмів моніторингу та контролю процесів; регулярність аудиту та оптимізації процесів; інтегрованість процесів різних відомств та рівнів управління.

Інформаційно-аналітична зрілість характеризує розвиненість системи інформаційного забезпечення прийняття рішень у сфері національної безпеки. Цей критерій відображає здатність системи збирати, обробляти, аналізувати та використовувати інформацію для ефективного управління. Ключові показники включають: повноту та достовірність інформаційних потоків; швидкість обробки та передачі критичної інформації; якість аналітичних продуктів та їх релевантність для прийняття рішень; рівень інтеграції інформаційних систем різних відомств; захищеність інформаційної інфраструктури від несанкціонованого доступу; розвиненість систем підтримки прийняття рішень.

Адаптивна зрілість відображає здатність системи управління національною безпекою еволюціонувати відповідно до змін внутрішнього та зовнішнього середовища. Цей критерій особливо важливий в умовах високої динамічності та непередбачуваності сучасних безпекових викликів. Показниками адаптивної зрілості є: швидкість реагування на нові типи загроз; гнучкість організаційних структур та їх здатність до реконфігурації; наявність механізмів організаційного навчання та акумуляції досвіду; інноваційність у розробці нових підходів та інструментів; здатність до проактивної адаптації на основі прогнозування майбутніх викликів; ефективність механізмів зворотного зв’язку.

Культурна зрілість характеризує ступінь розвитку організаційної культури безпекових інституцій та культури безпеки в суспільстві загалом. Цей критерій відображає глибинні аспекти інституціалізації, пов’язані з

цінностями, нормами поведінки, неформальними практиками. Індикатори культурної зрілості включають: рівень професійної етики та доброчесності в безпекових структурах; ступінь довіри між різними інституціями та готовність до співпраці; розвиненість традицій служби та корпоративної ідентичності; рівень безпекової свідомості громадян; готовність суспільства підтримувати заходи із забезпечення національної безпеки; ефективність механізмів передачі організаційного досвіду та знань.

Інтеграційна зрілість відображає ступінь включеності національної системи управління безпекою в міжнародні безпекові структури та механізми співпраці. В умовах глобалізації безпекових викликів здатність до ефективної міжнародної взаємодії стає критичним фактором забезпечення національної безпеки. Показники інтеграційної зрілості охоплюють: рівень гармонізації національних стандартів та процедур з міжнародними; ефективність участі в міжнародних безпекових організаціях та ініціативах; розвиненість двосторонніх та багатосторонніх механізмів безпекової співпраці; здатність національної системи використовувати переваги міжнародної кооперації; внесок країни в забезпечення регіональної та глобальної безпеки.

Результативна зрілість як інтегральний критерій відображає кінцеву ефективність системи управління національною безпекою в досягненні своєї основної мети – забезпечення захищеності національних інтересів. Цей критерій фокусується не на процесах чи структурах, а на реальних результатах діяльності безпекової системи. Ключові показники включають: динаміку рівня захищеності від різних типів загроз; ефективність попередження та нейтралізації безпекових інцидентів; мінімізацію збитків від реалізованих загроз; стійкість критичної інфраструктури; рівень суспільної безпеки та стабільності; міжнародні рейтинги безпекового становища країни.

Таким чином, комплексна оцінка інституційної зрілості вимагає застосування інтегрованої методології, яка поєднує кількісні та якісні методи, об’єктивні індикатори та експертні оцінки (табл. 1.1), при цьому важливо враховувати взаємозв’язки між різними критеріями та їх синергетичний вплив

на загальну ефективність системи.

Таблиця 1.1

Критерії та показники інституційної зрілості системи управління національною безпекою

Критерій зрілості	Сутнісна характеристика	Основні показники/індикатори
Структурна зрілість	Ступінь сформованості організаційної архітектури системи управління національною безпекою	Наявність всіх необхідних інституційних ланок Чіткість вертикальних та горизонтальних зв'язків Відсутність дублювання функцій та інституційних лакун Збалансованість централізації та децентралізації Гнучкість організаційної структури
Функціональна зрілість	Здатність системи ефективно виконувати весь спектр необхідних функцій від стратегічного планування до оперативного реагування	Ефективність системи раннього попередження Якість стратегічного планування Швидкість та адекватність реагування на кризи Здатність до міжвідомчої координації Результативність превентивних заходів
Нормативно-правова зрілість	Ступінь розвитку правової бази, що регулює функціонування системи національної безпеки	Повнота правового регулювання Відсутність правових колізій та прогалин Чіткість механізмів розподілу повноважень Наявність правових процедур для різних режимів Регулярність оновлення нормативної бази
Ресурсна зрілість	Спроможність системи акумулювати, розподіляти та ефективно використовувати необхідні ресурси	Достатність фінансового забезпечення Ефективність бюджетного планування Оптимальність структури видатків Якість кадрового забезпечення Рівень технологічного оснащення Розвиненість резервних потужностей
Процесна зрілість	Ступінь формалізації, стандартизації та оптимізації управлінських процесів	Наявність формалізованих процедур Ступінь автоматизації операцій Швидкість управлінських циклів Ефективність моніторингу процесів Регулярність аудиту та оптимізації Інтегрованість процесів різних відомств

Закінчення табл. 1.1

Критерій зрілості	Сутнісна характеристика	Основні показники/індикатори
Інформаційно-аналітична зрілість	Розвиненість системи інформаційного забезпечення прийняття рішень	Повнота та достовірність інформаційних потоків Швидкість обробки критичної інформації Якість аналітичних продуктів Рівень інтеграції інформаційних систем Захищеність інформаційної інфраструктури Розвиненість систем підтримки рішень
Адаптивна зрілість	Здатність системи еволюціонувати відповідно до змін середовища	Швидкість реагування на нові загрози Гнучкість організаційних структур Наявність механізмів організаційного навчання Інноваційність у розробці підходів Здатність до проактивної адаптації Ефективність механізмів зворотного зв'язку
Культурна зрілість	Ступінь розвитку організаційної культури безпекових інституцій та культури безпеки в суспільстві	Рівень професійної етики та доброчесності Ступінь довіри між інституціями Розвиненість традицій служби Рівень безпекової свідомості громадян Готовність суспільства підтримувати безпекові заходи Ефективність передачі досвіду
Інтеграційна зрілість	Ступінь включеності національної системи в міжнародні безпекові структури	Рівень гармонізації зі міжнародними стандартами Ефективність участі в міжнародних організаціях Розвиненість механізмів безпекової співпраці Здатність використовувати переваги кооперації Внесок у регіональну та глобальну безпеку
Результативна зрілість	Кінцева ефективність системи в досягненні мети забезпечення національної безпеки	Динаміка рівня захищеності від загроз Ефективність попередження інцидентів Мінімізація збитків від реалізованих загроз Стійкість критичної інфраструктури Рівень суспільної безпеки Міжнародні рейтинги безпеки

Представлена система критеріїв та показників інституційної зрілості створює методологічну основу для комплексного оцінювання стану системи управління національною безпекою та ідентифікації пріоритетних напрямів її розвитку. Важливо підкреслити, що всі десять критеріїв перебувають у тісному взаємозв'язку та взаємозалежності, формуючи цілісну систему характеристик інституційного розвитку. Так, структурна зрілість створює

організаційні передумови для реалізації функцій, нормативно-правова зрілість легітимізує діяльність інституцій, ресурсна зрілість забезпечує матеріальну базу функціонування, а культурна зрілість формує ціннісне підґрунтя ефективної роботи системи. Застосування цієї методології на практиці дозволяє не лише діагностувати поточний стан інституціалізації, а й прогнозувати траєкторії подальшого розвитку, своєчасно виявляти системні дисбаланси та розробляти обґрунтовані стратегії інституційного реформування у сфері національної безпеки.

1.2. Гібридна війна як детермінанта трансформації системи публічного управління національною безпекою

Феномен гібридної війни став одним із визначальних викликів для систем національної безпеки у XXI столітті, фундаментально змінюючи уявлення про природу конфліктів та вимагаючи переосмислення традиційних підходів до публічного управління у безпековій сфері. Концептуалізація гібридної війни в контексті публічного управління передбачає не просто визначення цього явища, а глибинне розуміння його сутнісних характеристик, механізмів реалізації та наслідків для функціонування державних інституцій.

Термін «гібридна війна» увійшов до наукового та політичного дискурсу відносно нещодавно, хоча самі практики поєднання різних форм та методів ведення конфлікту мають давню історію. Сучасне розуміння гібридної війни сформувалось під впливом аналізу конфліктів початку XXI століття, зокрема війни в Лівані 2006 року, російсько-грузинської війни 2008 року та особливо російської агресії проти України, що розпочалась у 2014 році. Саме український досвід став своєрідною лабораторією для вивчення гібридних стратегій та їх впливу на систему публічного управління.

Гібридна війна характеризується синхронізованим застосуванням широкого спектру інструментів впливу – від традиційних військових дій до

економічного тиску, від кібератак до інформаційних операцій, від використання іррегулярних формувань до дипломатичного шантажу. Ключовою особливістю є розмивання меж між війною та миром, між комбатантами та цивільним населенням, між внутрішніми та зовнішніми загрозами [135]. Така амбівалентність створює фундаментальні виклики для системи публічного управління, яка традиційно побудована на чітких правових та організаційних розмежуваннях.

У контексті публічного управління гібридна війна постає як комплексний виклик, що потребує координованої відповіді всієї системи державних інституцій. На відміну від класичної війни, де основна відповідальність покладається на військові структури, гібридна агресія спрямована на всі сфери життєдіяльності держави та суспільства. Економічні санкції підривають фінансову стабільність, інформаційні атаки деморалізують населення та підривають довіру до влади, кібератаки паралізують критичну інфраструктуру, а використання внутрішніх протиріч дестабілізує політичну систему. Все це вимагає від системи публічного управління здатності діяти в умовах постійної невизначеності та багатовекторних загроз.

Концептуалізація гібридної війни неможлива без розуміння її стратегічної логіки. Агресор прагне досягти своїх цілей, уникаючи прямого військового зіткнення та формальної декларації війни, що дозволяє йому залишатися в «сірій зоні» міжнародного права [126]. Використання проксі-сил, приховані операції, маніпулювання інформацією створюють ситуацію «правдоподібного заперечення», коли важко однозначно ідентифікувати агресора та притягнути його до відповідальності. Для системи публічного управління це означає необхідність діяти в умовах правової невизначеності, коли традиційні механізми реагування на агресію виявляються неефективними.

Особливо важливим аспектом є темпоральний вимір гібридної війни. На відміну від класичних воєн з відносно чіткими початком та завершенням, гібридна агресія може тривати роками або навіть десятиліттями, періодично

загострюючись та затухаючи. Фази активної ескалації змінюються періодами «заморожування» конфлікту, але підривна діяльність не припиняється. Це створює ефект «стратегічної втоми», коли суспільство та державні інституції виснажуються від постійної напруги. Система публічного управління повинна бути готова до функціонування в режимі перманентної кризи, що вимагає особливих підходів до планування, ресурсного забезпечення та кадрової політики.

Інформаційний компонент гібридної війни заслуговує на особливу увагу в контексті публічного управління. Маніпулювання інформацією, поширення дезінформації, створення альтернативної реальності стають потужними інструментами підриву державності. Атаки спрямовуються не лише на масову свідомість, а й на системи прийняття рішень, коли за допомогою спеціально сконструйованої інформації управлінці підштовхуються до помилкових висновків та рішень. Концепція «рефлексивного управління», розроблена ще радянськими військовими теоретиками, набуває нового виміру в епоху соціальних мереж та big data [157].

Економічний вимір гібридної війни проявляється через використання економічних залежностей як інструменту тиску та контролю. Енергетичний шантаж, торговельні війни, атаки на фінансову систему, створення штучних економічних криз – все це стає зброєю в руках агресора. Для системи публічного управління це означає необхідність переосмислення концепції економічної безпеки, розробки механізмів швидкого реагування на економічні загрози, забезпечення стійкості критичних секторів економіки. Традиційне розмежування між економічною політикою та безпековою політикою втрачає сенс в умовах гібридної агресії.

Соціальний вимір гібридної війни пов’язаний з експлуатацією внутрішніх протиріч та конфліктів у суспільстві. Етнічні, релігійні, мовні, регіональні розбіжності стають об’єктом маніпулювання з метою дестабілізації. Створення та підтримка радикальних груп, провокування протестів, поглиблення соціальної поляризації – все це інструменти гібридної

агресії. Система публічного управління стикається з дилемою: як забезпечити національну безпеку, не обмежуючи при цьому демократичні свободи та права громадян. Надмірна секюритизація може призвести до згортання демократії, що фактично означатиме досягнення агресором своїх цілей.

Правовий вимір гібридної війни створює особливі виклики для публічного управління. Міжнародне право, сформоване для регулювання класичних міждержавних конфліктів, виявляється недостатньо ефективним в умовах гібридної агресії. Відсутність формального стану війни, використання недержавних акторів, приховані операції – все це створює правові лакуни. На національному рівні виникає потреба в адаптації законодавства до нових реалій, але це має відбуватися без порушення конституційних принципів та міжнародних зобов'язань. Концептуалізація гібридної війни в правовому полі залишається однією з найскладніших проблем сучасного публічного управління.

Технологічний вимір гібридної війни постійно еволюціонує, створюючи нові виклики для системи публічного управління. Кібератаки на критичну інфраструктуру можуть завдати збитків, співмірних з наслідками конвенційних бомбардувань. Використання штучного інтелекту для створення deepfake відео чи масового поширення дезінформації відкриває нові горизонти маніпулювання. Атаки на системи публічного управління через вразливості в програмному забезпеченні можуть паралізувати надання публічних послуг. Все це вимагає від системи публічного управління постійної технологічної модернізації та розвитку відповідних компетенцій.

Важливим аспектом концептуалізації є розуміння асиметричності гібридної війни. Агресор часто має перевагу в можливості вибору часу, місця та способу атаки, тоді як обороняюча сторона змушена захищати весь спектр потенційних цілей. Ця асиметрія посилюється різницею в обмеженнях: демократична держава зв'язана правовими та етичними нормами, тоді як агресор може діяти без таких обмежень. Для публічного управління це означає необхідність розробки асиметричних стратегій відповіді, які б компенсували

структурні недоліки оборонної позиції (табл. 1.2).

Таблиця 1.2

Порівняльна характеристика традиційних та гібридних загроз національній безпеці

Параметр порівняння	Традиційні загрози	Гібридні загрози
Характер загроз	Переважно військові, чітко визначені	Комплексні, багатовимірні, синергетичні (військові, політичні, економічні, інформаційні, соціальні одночасно)
Актори	Держави, регулярні збройні сили	Держави + недержавні актори (приватні військові компанії, хакерські угруповання, терористичні організації, НУО, медіа)
Просторовий вимір	Чітке розмежування внутрішніх та зовнішніх загроз, географічна локалізація	Розмиття меж між внутрішнім та зовнішнім, транскордонний характер, мультидоменність (фізичний, кібер-, інформаційний, когнітивний простір)
Темпоральний вимір	Відносно чіткі часові рамки (початок і завершення конфлікту)	Перманентний характер, тривалість роками/десятиліттями, періоди ескалації та затухання, ефект «стратегічної втоми»
Ідентифікація	Легко ідентифікувати агресора та природу загрози	Амбівалентність, складність атрибуції, дії в «сірих зонах», «правдоподібне заперечення»
Методи реалізації	Переважно військова сила, пряма агресія	Синхронізоване застосування широкого спектру інструментів: кібератаки, інформаційні операції, економічний тиск, використання проксі-сил, дипломатичний шантаж
Правове регулювання	Чітко врегульовано міжнародним гуманітарним правом	Правові лакуни, невідповідність існуючих норм новим реаліям, експлуатація легальних інструментів для нелегітимних цілей
Цільова спрямованість	Військові об’єкти, збройні сили, критична інфраструктура	Усі сфери життєдіяльності держави та суспільства, когнітивні вразливості, свідомість населення, довіра до інститутів

Закінчення таблиці 1.2

Параметр порівняння	Традиційні загрози	Гібридні загрози
Логіка дій	Пряме силове протистояння, контроль над територією	Досягнення цілей без прямого зіткнення, контроль над смислами та інтерпретаціями, рефлексивне управління
Передбачуваність	Відносно передбачувані сценарії розвитку	Висока невизначеність, адаптивність та еволюційність загроз, каскадні ефекти
Режим функціонування	Чіткий перехід від миру до війни	Континуум проміжних станів, розмиття меж між війною та миром
Методи протидії	Військове стримування, оборона, альянси	Комплексна стійкість (resilience), міжвідомча координація, стратегічні комунікації, кіберзахист, соціальна згуртованість
Відповідальні структури	Переважно міністерство оборони та збройні сили	Вся система державних інституцій, потреба в цілісному підході
Ефект впливу	Переважно фізичні руйнування, людські жертви	Багатовимірний: фізичний + психологічний + економічний + соціальний + політичний
Роль технологій	Традиційні військові технології	Критична роль ШІ, big data, соціальних мереж, кібертехнологій, deepfake
Соціальний вимір	Обмежений вплив на суспільство в мирний час	Цілеспрямована експлуатація соціальних розколів, поглиблення поляризації, підрив соціальної згуртованості

Концептуалізація гібридної війни в контексті публічного управління не може оминути питання стійкості системи до гібридних загроз. На відміну від традиційного підходу, орієнтованого на запобігання та відсіч агресії, концепція стійкості визнає неможливість повного захисту від усіх загроз та зосереджується на здатності системи абсорбувати удари, адаптуватися та відновлюватися. Це вимагає фундаментального переосмислення принципів організації публічного управління – від жорстких ієрархічних структур до гнучких мережевих форм, від централізованого контролю до розподіленої відповідальності, від реактивного реагування до проактивної адаптації.

Слід наголосити, що гібридні загрози представляють собою якісно новий тип викликів для системи національної безпеки, що характеризуються

безпрецедентною складністю, багатовимірністю та синергетичним ефектом від одночасного застосування різних деструктивних інструментів. Розуміння особливостей цих загроз є критично важливим для вироблення адекватних механізмів протидії та адаптації системи публічного управління до нових реалій безпекового середовища.

Першою визначальною особливістю гібридних загроз є їх комплексність та взаємопов'язаність. На відміну від традиційних загроз, які можна було відносно чітко категоризувати та локалізувати, гібридні загрози діють одночасно в різних сферах – військовій, політичній, економічній, інформаційній, соціальній, створюючи кумулятивний ефект [116]. Кібератака на енергетичну інфраструктуру може супроводжуватися інформаційною кампанією про «неспроможність влади», що провокує соціальні протести, які, в свою чергу, використовуються для політичного тиску. Така мультиплікація ефектів робить гібридні загрози особливо небезпечними.

Друга особливість – це розмитість та амбівалентність, що проявляється у складності ідентифікації джерела загрози, визначення її природи та масштабів. Гібридні актори навмисно діють у «сірих зонах», уникаючи чітких маркерів агресії.

Масові протести можуть бути як проявом громадянської активності, так і результатом зовнішнього втручання. Економічні проблеми можуть виникати природним шляхом або бути штучно створеними. Кібератаки проводяться через ланцюжки проксі-серверів, що унеможливлює встановлення реального замовника [172]. Ця амбівалентність паралізує традиційні механізми прийняття рішень у системі національної безпеки, які базуються на чіткій ідентифікації загрози.

Третьою особливістю є адаптивність та еволюційність гібридних загроз. Вони постійно трансформуються, пристосовуючись до заходів протидії, експлуатуючи нові вразливості, використовуючи технологічні інновації. Те, що було ефективним інструментом гібридної агресії вчора, може бути замінено новими методами сьогодні. Ця динамічність вимагає від системи

національної безпеки не лише реактивних заходів, а й здатності до прогнозування еволюції загроз, превентивного закриття потенційних вразливостей, постійного оновлення стратегій та тактик протидії.

Використання легальних інструментів для досягнення нелегітимних цілей становить ще одну важливу особливість. Гібридні актори експлуатують відкритість демократичних суспільств, використовуючи свободу слова для поширення дезінформації, демократичні процедури для просування деструктивних сил, економічні свободи для встановлення контролю над критичними активами. НУО, медіа, політичні партії, бізнес-структури можуть ставати інструментами гібридного впливу, формально залишаючись в правовому полі [186]. Це створює для системи національної безпеки складну дилему: як протидіяти таким загрозам, не підриваючи при цьому демократичні основи суспільства.

Каскадний ефект гібридних загроз проявляється в їх здатності запускати ланцюгові реакції дестабілізації. Початкова атака може бути відносно обмеженою, але вона розрахована на запуск процесів, які призведуть до непропорційно великих наслідків. Невеликий інцидент на етнічному ґрунті може спровокувати масштабний конфлікт. Локальна економічна криза може підірвати довіру до всієї фінансової системи. Витік компромату на одного політика може призвести до системної політичної кризи. Розуміння цих каскадних механізмів критично важливе для системи національної безпеки.

Однією з найбільш витончених особливостей гібридних загроз є експлуатація когнітивних вразливостей. Вони спрямовані не лише на фізичні об’єкти чи інституції, а й на свідомість людей, їх сприйняття реальності, систему цінностей та переконань. Використовуючи досягнення психології, нейронауки, біхевіоральної економіки, гібридні актори конструюють повідомлення та наративи, що експлуатують когнітивні упередження, емоційні тригери, соціальні стереотипи [187]. Результатом стає не просто дезінформованість, а глибинна трансформація світогляду, що робить людей вразливими до маніпуляцій.

У той же час, персоналізація та таргетованість гібридних загроз відображає їх здатність до точкового впливу на конкретні цільові аудиторії. Використовуючи big data та алгоритми штучного інтелекту, гібридні актори можуть створювати персоналізовані повідомлення для різних соціальних груп, експлуатуючи їх специфічні страхи, надії, упередження. Політики отримують одні меседжі, військові – інші, молодь – треті. Така сегментація дозволяє максимізувати ефективність впливу та мінімізувати ризик викриття.

Тривалість та перманентність гібридних загроз відрізняє їх від традиційних безпекових викликів, які зазвичай мають більш-менш визначені часові рамки. Гібридна агресія може тривати роками та десятиліттями, з періодами загострення та відносного затишшя. Це створює ефект «нормалізації» загрози, коли суспільство та державні інституції звикають до постійного тиску та втрачають здатність до мобілізації. Система національної безпеки стикається з проблемою підтримання готовності в умовах «вічної війни», що виснажує ресурси та підриває морально-психологічний стан.

Мережевий характер гібридних загроз проявляється у використанні розгалужених неформальних структур замість традиційних ієрархічних організацій. Гібридні актори створюють складні мережі, що включають державні та недержавні елементи, легальні та нелегальні структури, формальні та неформальні зв’язки. Ці мережі характеризуються високою живучістю – знищення окремих вузлів не призводить до колапсу всієї системи. Для традиційних безпекових структур, побудованих за ієрархічним принципом, протидія таким мережевим загрозам становить серйозний виклик.

Вплив гібридних загроз на систему національної безпеки проявляється в кількох вимірах. По-перше, вони призводять до розмивання традиційних функціональних меж між різними безпековими відомствами. Коли загроза одночасно має військовий, кримінальний, інформаційний та економічний виміри, стає неможливим чітко визначити, яке відомство має нести основну відповідальність. Це вимагає переходу від секторального до інтегрованого підходу в організації системи національної безпеки.

По-друге, гібридні загрози трансформують темпоральну логіку функціонування безпекової системи. Традиційний цикл «загроза – оцінка – рішення – дія» стає занадто повільним в умовах швидкоплинних гібридних атак. Виникає потреба в механізмах випереджувального реагування, проактивних стратегіях, системах раннього попередження нового типу. Водночас довготривалий характер гібридних загроз вимагає стратегічного планування на десятиліття вперед.

По-третє, гібридні загрози фундаментально змінюють ресурсні потреби системи національної безпеки. Традиційний акцент на військових витратах має бути доповнений інвестиціями в кібербезпеку, інформаційну стійкість, соціальну згуртованість, економічну резильєнтність. Виникає проблема балансування ресурсів між різними вимірами безпеки в умовах їх обмеженості.

Таким чином, гібридна агресія фундаментально трансформує безпекове середовище, створюючи якісно нові умови функціонування системи національної безпеки та публічного управління в цілому. Ця трансформація виходить далеко за межі простої зміни характеру загроз – вона переформатовує саму логіку безпекових відносин, правила гри, критерії успіху та поразки. І найбільш радикальною зміною є ерозія традиційних бінарних опозицій, які структурували безпекове мислення протягом століть. Межа між війною та миром стає розмитою – замість чіткого переходу від мирного стану до воєнного виникає континуум проміжних станів, «сірі зони», де застосовується насильство, але формально зберігається мир [209]. Це унеможливлює використання традиційних правових та організаційних механізмів, розроблених для чітко визначених станів. Система публічного управління опиняється в ситуації постійної невизначеності щодо характеру середовища, в якому вона функціонує.

Аналогічно розмивається межа між внутрішнім та зовнішнім вимірами безпеки. Гібридна агресія використовує внутрішні вразливості для досягнення зовнішньополітичних цілей, а зовнішні інструменти – для впливу на внутрішні

процеси. Протести, інспіровані ззовні, але здійснювані громадянами країни; економічні кризи, спровоковані зовнішніми акторами через внутрішні механізми; інформаційні кампанії, що ведуться з-за кордону, але резонують з внутрішніми проблемами – все це приклади такого взаємопроникнення. Традиційний поділ на відомства, що відповідають за внутрішню та зовнішню безпеку, втрачає функціональність.

Трансформується також співвідношення між державними та недержавними акторами в безпековому середовищі. Якщо раніше держава мала монополію на застосування організованого насильства та була основним суб'єктом безпекових відносин, то в умовах гібридної агресії зростає роль недержавних акторів – від приватних військових компаній до хакерських угруповань, від терористичних організацій до транснаціональних корпорацій [154]. Ці актори можуть діяти автономно або бути інструментами державної політики, що ускладнює атрибуцію дій та відповідальності.

Можна стверджувати, що інформаційний простір перетворюється на основне поле битви в умовах гібридної агресії. Безпекове середовище стає гіперінформаційним – насиченим потоками даних, повідомлень, наративів, які формують сприйняття реальності різними аудиторіями. Боротьба ведеться не стільки за фізичний контроль над територією чи ресурсами, скільки за контроль над смислами, інтерпретаціями, емоціями. Концепція «постправди» відображає ситуацію, коли об'єктивні факти стають менш важливими, ніж емоційний резонанс та відповідність наявним упередженням. Для системи національної безпеки це означає необхідність розвитку принципово нових компетенцій – від фактчекінгу до стратегічних комунікацій, від кіберрозвідки до психологічних операцій.

Темпоральні характеристики безпекового середовища також зазнають глибокої трансформації. З одного боку, швидкість розгортання подій радикально зростає – кібератака може паралізувати критичну інфраструктуру за хвилини, інформаційна кампанія може змінити громадську думку за години, фінансова паніка може обвалити ринки за дні. Це вимагає від системи

національної безпеки здатності до миттєвого реагування, прийняття рішень в режимі реального часу. З іншого боку, стратегічні процеси гібридної агресії розгортаються в довготривалій перспективі – формування агентурних мереж, культивування потрібних наративів, створення економічних залежностей може тривати роками або навіть десятиліттями.

Простір безпекових взаємодій стає мультидоменним та взаємопов'язаним. До традиційних фізичних доменів – суші, моря, повітря – додаються кіберпростір, інформаційний простір, когнітивний простір. Події в одному домені миттєво резонують в інших – кібератака призводить до фізичних руйнувань, які стають приводом для інформаційної кампанії, що впливає на когнітивний стан населення.

Економічне середовище перетворюється на поле безпекового протистояння. Глобалізація створила складні ланцюги взаємозалежностей, які можуть бути використані як інструменти тиску. Енергетичні поставки, фінансові потоки, технологічні ланцюги, інвестиції – все це стає зброєю в гібридній війні [103]. Концепція «економічної зброї» передбачає використання легальних економічних інструментів для досягнення геополітичних цілей. Санкції, торговельні війни, валютні маніпуляції, боргові пастки стають звичайними інструментами міждержавного протистояння.

Соціальне середовище в умовах гібридної агресії характеризується зростаючою поляризацією та фрагментацією. Гібридні актори цілеспрямовано поглиблюють існуючі розколи в суспільстві – етнічні, релігійні, мовні, ідеологічні, регіональні. Створюються «ехо-камери» та «інформаційні бульбашки», де різні групи населення живуть в паралельних реальностях, споживаючи радикально відмінну інформацію та формуючи несумісні картини світу. Це підриває соціальну згуртованість, яка є основою стійкості до гібридних загроз.

Технологічне середовище стає все більш визначальним фактором безпекової динаміки. Штучний інтелект, квантові обчислення, 5G мережі, інтернет речей, блокчейн – ці та інші технології створюють як нові можливості

для забезпечення безпеки, так і нові вразливості. Технологічна перевага стає критичним фактором в гібридному протистоянні, але водночас залежність від складних технологічних систем створює нові вектори атак.

Правове середовище опиняється в стані кризи через невідповідність існуючих норм новим реаліям. Міжнародне гуманітарне право, розроблене для регулювання класичних воєн, погано пристосоване до гібридних конфліктів. Національне законодавство часто не встигає за швидкістю технологічних та соціальних змін. Виникають правові лакуни, які експлуатуються гібридними акторами. Водночас спроби адаптації правового середовища стикаються з ризиком надмірної секюритизації та обмеження громадянських свобод.

Психологічне середовище характеризується зростанням рівня тривожності, невизначеності, недовіри. Постійний інформаційний шум, суперечливі повідомлення, складність розрізнення правди та фейків створюють стан когнітивного перевантаження. Феномен «інформаційної втоми» призводить до апатії та байдужості, коли люди втрачають здатність критично оцінювати інформацію. Це створює сприятливі умови для маніпуляцій та пропаганди.

Інституційне середовище зазнає тиску через систематичні спроби підриву довіри до державних інститутів. Корупційні скандали, витоки конфіденційної інформації, дискредитація політичних лідерів – все це інструменти ерозії інституційної легітимності. Коли громадяни втрачають віру в спроможність держави захистити їхні інтереси, вони стають більш вразливими до альтернативних центів впливу, включаючи тих, що контролюються гібридними акторами.

Культурне середовище стає об’єктом цілеспрямованого впливу через «м’яку силу» та культурні війни. Історична пам’ять, національна ідентичність, цінності та символи стають предметом маніпуляцій та переінтерпретацій. Нав’язування чужих культурних кодів, руйнування традиційних цінностей, створення кризи ідентичності – все це елементи гібридної стратегії довгострокового підриву національної стійкості.

Через все це трансформація безпекового середовища в умовах гібридної агресії вимагає від системи публічного управління фундаментального переосмислення базових принципів організації та функціонування. Лінійні моделі планування мають поступитися місцем адаптивним стратегіям. Жорсткі ієрархічні структури повинні доповнюватись гнучкими мережевими формами. Реактивне реагування має змінитись проактивним формуванням безпекового середовища. Вузька спеціалізація повинна поєднуватись з міждисциплінарним підходом. Тільки така комплексна трансформація може забезпечити адекватність системи національної безпеки новим викликам гібридної епохи.

Адаптивність системи публічного управління до викликів гібридної війни становить критичний фактор виживання та збереження державності в умовах перманентної безпекової турбулентності. На відміну від традиційних управлінських моделей, орієнтованих на стабільність та передбачуваність, адаптивне управління визнає постійну мінливість середовища як базову умову функціонування.

Концептуальною основою адаптивності є розуміння системи публічного управління як складної динамічної системи, що функціонує в умовах високої невизначеності. Класичні кібернетичні моделі управління, засновані на принципах негативного зворотного зв’язку та гомеостазу, виявляються недостатніми в ситуації, коли саме середовище постійно трансформується [98]. Гібридна війна створює умови, в яких параметри системи, цілі управління та критерії успіху постійно змінюються під впливом дій противника.

Адаптивність проявляється насамперед у здатності системи публічного управління до швидкої реконфігурації своїх структур та процесів відповідно до характеру загроз. Традиційна бюрократична модель з її emphasis на стандартизацію, формалізацію та спеціалізацію стає перешкодою в умовах, коли загрози мають гібридний характер і вимагають нестандартних міжвідомчих рішень.

Виникає потреба в модульній архітектурі управлінської системи, де

окремі елементи можуть швидко перегруповуватись для вирішення конкретних завдань. Досвід країн, що зіткнулися з гібридною агресією, показує ефективність створення тимчасових міжвідомчих груп, кризових штабів, ситуаційних центрів, які функціонують паралельно з традиційними структурами [151]. Ключовим є баланс між збереженням базової інституційної структури та гнучкістю операційних форм.

Темпоральна адаптивність передбачає здатність системи функціонувати в різних часових режимах одночасно. Гібридна війна вимагає поєднання стратегічного планування на десятиліття вперед з тактичним реагуванням у режимі реального часу. Система публічного управління повинна вміти «стискати» час прийняття рішень в кризових ситуаціях та «розтягувати» його для стратегічного аналізу. Це досягається через створення паралельних контурів управління з різними темпоральними характеристиками – оперативного (години, дні), тактичного (тижні, місяці) та стратегічного (роки, десятиліття).

Когнітивна адаптивність стосується здатності управлінської системи переосмислювати базові уявлення про природу загроз, методи протидії, критерії успіху. Гібридна війна постійно кидає виклик усталеним ментальним моделям, експлуатуючи когнітивні упередження та стереотипи. Система публічного управління повинна культивувати «стратегічну емпатію» – здатність зрозуміти логіку дій противника, навіть якщо вона суперечить власним уявленням про раціональність. Водночас необхідно розвивати механізми захисту від рефлексивного управління з боку противника, коли він намагається нав’язати хибні інтерпретації ситуації.

Ресурсна адаптивність проявляється у здатності швидко перерозподіляти ресурси між різними напрямками діяльності відповідно до зміни пріоритетів. Традиційна бюджетна система з її річними циклами планування та жорсткими статтями витрат погано пристосована до динаміки гібридної війни. Необхідні механізми гнучкого бюджетування, резервні фонди для швидкого реагування, можливість перекидання ресурсів між відомствами

без тривалих бюрократичних процедур. Особливо критичним є розвиток механізмів мобілізації позабюджетних ресурсів – від краудфандингу до публічно-приватного партнерства.

Інформаційна адаптивність передбачає створення системи, здатної функціонувати в умовах інформаційного хаосу, характерного для гібридної війни. Потоки дезінформації, інформаційний шум, навмисне спотворення даних – все це вимагає розвитку витончених механізмів фільтрації, верифікації, агрегації інформації. Але ще важливішою є здатність приймати рішення в умовах неповної та суперечливої інформації, розвиток «толерантності до невизначеності» на всіх рівнях управління. Система повинна вміти функціонувати не лише в режимі «повної інформованості», а й в режимі «інформаційного туману».

Мережева адаптивність відображає здатність системи публічного управління переходити від жорстких ієрархічних структур до гнучких мережевих форм організації. Гібридні загрози часто мають мережевий характер, і протидіяти їм ефективно можуть лише відповідні мережеві структури [96]. Це не означає відмову від ієрархії як такої, але передбачає її доповнення горизонтальними зв’язками, неформальними комунікаціями, розподіленими центрами прийняття рішень. Критичним є розвиток «мережевого лідерства» – здатності координувати дії автономних акторів без прямого адміністративного підпорядкування.

Нормативна адаптивність стосується здатності правової системи еволюціонувати відповідно до нових викликів без втрати базових принципів верховенства права. Гібридна війна експлуатує ригідність правових норм, створюючи ситуації, не передбачені чинним законодавством. Водночас надмірна «гнучкість» у тлумаченні законів може призвести до правового свавілля. Необхідний делікатний баланс між правовою визначеністю та адаптивністю, що досягається через розвиток механізмів швидкого правового реагування – від прискореного прийняття законів у кризових ситуаціях до розширеного тлумачення існуючих норм у межах конституційних принципів.

Культурна адаптивність є, можливо, найскладнішим аспектом, оскільки стосується глибинних змін в управлінській культурі. Традиційна бюрократична культура з її акцентом на дотримання процедур, уникнення ризиків, кар'єрну стабільність погано сумісна з вимогами гібридної війни. Необхідна нова культура, що цінує ініціативність, готовність до розумного ризику, міжвідомчу кооперацію, постійне навчання. Це вимагає змін у системі мотивації, кар'єрного просування, оцінки результатів діяльності державних службовців.

Особливим аспектом адаптивності є здатність до організаційного навчання – екстракції уроків з власного та чужого досвіду, їх інституціоналізації та поширення. Гібридна війна є «learning competition», де перемагає той, хто швидше навчається. Система публічного управління повинна створити механізми систематичного аналізу кризових ситуацій, документування кращих практик, проведення навчань та симуляцій. Критичною є здатність вчитися не лише на успіхах, а й на помилках, створюючи культуру, де помилки розглядаються як джерело цінного досвіду, а не привід для покарання.

Технологічна адаптивність передбачає не просто впровадження нових технологій, а здатність швидко освоювати їх та інтегрувати в управлінські процеси. Гібридна війна характеризується швидкою зміною технологічного ландшафту – від соціальних мереж до штучного інтелекту. Система публічного управління повинна подолати традиційний технологічний консерватизм, створити механізми швидкого тестування та впровадження інновацій. Водночас необхідно розуміти, що технології самі по собі не є панацеєю – вони ефективні лише в поєднанні з відповідними організаційними та культурними змінами.

Міжнародна адаптивність відображає здатність системи публічного управління ефективно функціонувати в мінливому міжнародному середовищі. Гібридна війна часто ведеться на міжнародній арені, використовуючи міжнародні інституції, альянси, правові механізми. Система повинна вміти

швидко формувати коаліції, адаптувати національні практики до вимог міжнародних партнерів, використовувати міжнародні механізми для протидії гібридним загрозам. Це вимагає розвитку «дипломатичної спритності» – здатності маневрувати в складному міжнародному середовищі.

Соціальна адаптивність стосується взаємодії системи публічного управління з суспільством в умовах гібридної війни. Традиційна модель «держава знає краще» стає вразливістю, оскільки створює розрив між владою та громадянами, який експлуатується противником. Необхідна модель партнерства, де громадяни є не пасивними об’єктами захисту, а активними учасниками забезпечення національної стійкості. Це вимагає розвитку механізмів громадської участі, прозорості, підзвітності, що підвищують легітимність та ефективність державних дій.

Слід зазначити, що парадоксальність адаптивності в умовах гібридної війни полягає в необхідності поєднання стійкості та мінливості. Система повинна зберігати свою ідентичність, базові цінності та принципи, водночас радикально змінюючи форми та методи діяльності. Це вимагає чіткого розуміння того, що є «ядром» системи (і має залишатися незмінним), а що є «периферією» (і може гнучко адаптуватися). Втрата цього балансу веде або до ригідності (нездатності адаптуватися), або до хаотичності (втрати ідентичності).

Тому формування ефективних інституційних механізмів протидії гібридним загрозам становить одне з найскладніших завдань сучасного публічного управління у безпековій сфері. Комплексність та багатовимірність гібридних загроз вимагає створення відповідно складних та інтегрованих механізмів, здатних забезпечувати скоординовану відповідь на всьому спектрі можливих викликів.

Центральним елементом інституційної архітектури протидії гібридним загрозам є механізм стратегічної координації, який забезпечує узгодження дій різних відомств та рівнів управління. Досвід показує, що традиційні координаційні органи, створені для умов мирного часу або конвенційної

війни, виявляються недостатньо ефективними в гібридному протистоянні [130]. Необхідна нова модель координації, що поєднує постійні інституційні структури з гнучкими оперативними форматами.

Ключовою інновацією стає створення інтегрованих ситуаційних центрів, які функціонують як «нервові вузли» системи протидії гібридним загрозам. На відміну від традиційних командних пунктів, орієнтованих на управління військовими операціями, сучасні ситуаційні центри мають міждисциплінарний характер. Вони об'єднують представників силових структур, дипломатів, економістів, фахівців з кібербезпеки, психологів, комунікаторів, аналітиків різного профілю. Технологічною основою таких центрів є системи збору та обробки великих даних, візуалізації інформації, підтримки прийняття рішень на основі штучного інтелекту.

При цьому механізм раннього попередження та виявлення гібридних загроз кардинально відрізняється від традиційних систем, орієнтованих на фіксацію військових приготувань противника. Гібридні загрози часто розвиваються латентно, маскуються під природні процеси, використовують легальні канали. Їх виявлення вимагає аналізу слабких сигналів, виявлення аномалій у звичайних процесах, розпізнавання патернів скоординованої діяльності. Система раннього попередження нового покоління має включати моніторинг соціальних мереж для виявлення координованих інформаційних кампаній; аналіз фінансових потоків для ідентифікації підозрілого фінансування; відстеження міграційних процесів для виявлення організованої інфільтрації; моніторинг енергетичної та технологічної залежності для оцінки вразливостей; аналіз політичних процесів для виявлення зовнішнього втручання. Критичною є здатність системи відрізняти справжні загрози від природних флуктуацій та помилкових тривог.

Інституційний механізм стратегічних комунікацій відіграє ключову роль у протидії інформаційному компоненту гібридної агресії. Традиційна модель урядової комунікації, заснована на односторонньому інформуванні через офіційні канали, виявляється неефективною в епоху соціальних мереж та

постправди. Необхідний перехід до проактивної моделі, що включає постійний моніторинг інформаційного простору, швидке реагування на дезінформацію, формування власних наративів, залучення широкого кола комунікаторів. Стратегічні комунікації в умовах гібридної війни виходять далеко за межі простого спростування фейків. Вони включають формування стійких смислових конструкцій, які роблять аудиторію менш вразливою до маніпуляцій; створення емоційно резонансних меседжів, здатних конкурувати з пропагандою; розбудову мереж довіри, які забезпечують поширення достовірної інформації; культивування критичного мислення та медіаграмотності населення [184]. Інституційно це вимагає не лише створення спеціалізованих підрозділів, а й трансформації всієї системи урядової комунікації.

Механізм забезпечення критичної інфраструктури набуває особливого значення в контексті гібридних загроз. Сучасна критична інфраструктура – енергетична, транспортна, телекомунікаційна, фінансова – характеризується високим рівнем взаємозалежності та вразливості до каскадних ефектів. Гібридні актори можуть завдати непропорційно великої шкоди через точкові удари по критичних вузлах.

Інституційний механізм захисту критичної інфраструктури має базуватися на принципах резильєнтності – здатності поглинати удари, адаптуватися та швидко відновлюватися. Це передбачає не лише фізичний захист об’єктів, а й резервування критичних функцій, диверсифікацію постачальників, створення автономних контурів управління, розробку планів безперервності діяльності. Особливо важливою є координація між державним та приватним секторами, оскільки значна частина критичної інфраструктури перебуває в приватній власності.

Фінансово-економічний механізм протидії гібридним загрозам охоплює широкий спектр інструментів – від контролю за іноземними інвестиціями в стратегічні сектори до протидії відмиванню коштів, від забезпечення стійкості фінансової системи до диверсифікації економічних зв’язків. Гібридна агресія

часто використовує економічні важелі – створення боргової залежності, монополізацію критичних ринків, маніпулювання цінами на стратегічні товари [119].

Інституційна відповідь включає також створення механізмів скринінгу іноземних інвестицій на предмет безпекових ризиків; розробку планів економічної мобілізації на випадок кризи; формування стратегічних резервів критичних товарів; створення альтернативних фінансових каналів на випадок блокування основних; розвиток національних виробничих потужностей у критичних секторах. Ключовим є баланс між економічною відкритістю (необхідною для розвитку) та безпековими застереженнями (необхідними для виживання).

Правоохоронний механізм протидії гібридним загрозам стикається з особливими викликами через розмитість межі між кримінальною діяльністю та актами агресії. Організована злочинність може бути інструментом гібридної війни, а державні актори можуть використовувати кримінальні методи. Традиційне розмежування між правоохоронною діяльністю та контррозвідкою втрачає чіткість.

Тому необхідна інтеграція правоохоронних та безпекових функцій через створення спільних оперативних груп, обмін інформацією в режимі реального часу, координацію оперативних заходів. Особливо важливим є розвиток спроможностей у сфері фінансових розслідувань, кіберкриміналістики, протидії організованій злочинності. Водночас критично важливо зберегти правові гарантії та не допустити перетворення правоохоронних органів на інструмент політичних репресій.

Механізм мобілізації суспільства для протидії гібридним загрозам відображає розуміння того, що в гібридній війні основним об’єктом атаки є саме суспільство. Традиційна модель, де держава захищає пасивне населення, стає анахронізмом. Необхідна модель «суспільства-учасника», де громадяни є активними суб’єктами забезпечення національної стійкості. Інституційно це реалізується через розвиток територіальної оборони з широким залученням

цивільного населення; створення волонтерських мереж для підтримки безпекових зусиль; формування системи цивільної освіти з питань національної безпеки; розбудову механізмів краудсорсингу безпекової інформації; підтримку громадських ініціатив у сфері протидії дезінформації, кібербезпеки, соціальної згуртованості. Ключовим викликом є забезпечення балансу між мобілізацією та мілітаризацією суспільства.

Науково-аналітичний механізм забезпечує інтелектуальну основу для протидії гібридним загрозам. Складність та новизна цих загроз вимагає постійних досліджень, розробки нових концепцій, тестування інноваційних підходів. Традиційна модель відомчих аналітичних підрозділів виявляється недостатньою через міждисциплінарний характер проблематики. Необхідним є створення мережі дослідницьких центрів, що поєднує державні, академічні та незалежні аналітичні інституції. Ці центри мають займатися не лише аналізом поточних загроз, а й прогнозуванням майбутніх викликів, розробкою сценаріїв, проведенням ігрових симуляцій, тестуванням нових концепцій. Особливо важливим є розвиток міждисциплінарних досліджень на стику безпекових студій, психології, соціології, кібернетики, теорії складності.

Міжнародний механізм протидії гібридним загрозам відображає транснаціональний характер цих викликів. Гібридна агресія часто спрямована одночасно проти кількох країн або використовує територію третіх країн. Ефективна протидія неможлива без міжнародної координації зусиль. Інституційні форми міжнародної співпраці включають обмін інформацією про гібридні загрози в режимі реального часу; координацію заходів протидії дезінформації; спільні навчання з відпрацювання сценаріїв гібридної агресії; гармонізацію законодавства для закриття правових лакун; створення спільних оперативних центрів для протидії конкретним загрозам. Але при цьому особливим викликом є подолання традиційної міждержавної недовіри та небажання ділитися чутливою інформацією.

1.3. Основні підходи до дослідження інституціалізації публічного управління національною безпекою

Враховуючи специфіку об’єкта та предмета нашого дослідження доцільним є використання трьох основних підходів: системного, інституційного та синергетичного. Розглянемо їх докладніше.

Системний підхід у дослідженні безпекових інституцій являє собою фундаментальну методологічну парадигму, що дозволяє осягнути складність та багатовимірність інституційної архітектури національної безпеки в її цілісності та динаміці. Застосування системної методології обумовлено самою природою безпекових інституцій, які функціонують не як ізольовані організаційні одиниці, а як взаємопов’язані елементи складної системи, що перебуває в постійній взаємодії із зовнішнім середовищем. Онтологічні засади системного підходу в контексті безпекових інституцій базуються на розумінні системи національної безпеки як емерджентної цілісності, властивості якої не зводяться до простої суми властивостей її компонентів. Безпекові інституції, взаємодіючи між собою, породжують якісно нові властивості – синергетичні ефекти, що забезпечують вищий рівень безпекової спроможності порівняно з автономним функціонуванням окремих структур. Ця емерджентність [102] проявляється в здатності системи генерувати колективні рішення, координувати розподілені ресурси, формувати спільне розуміння безпекової ситуації.

Епістемологічний вимір системного підходу передбачає специфічну оптику дослідження, що фокусується не стільки на окремих інституціях, скільки на зв’язках та відносинах між ними. Традиційний редукціоністський підхід, що намагається зрозуміти систему через детальне вивчення її частин, виявляється недостатнім для осягнення складних безпекових феноменів. Системне мислення вимагає холістичного погляду, що схоплює патерни взаємодій, контури зворотних зв’язків, динаміку цілого.

Структурний аспект системного підходу до безпекових інституцій

передбачає виявлення та дослідження різних типів структур – ієрархічних, мережевих, матричних – та їх взаємного накладання. Сучасна система національної безпеки рідко має просту деревоподібну структуру; частіше вона являє собою складну констеляцію різнорідних структурних форм. Вертикальні ієрархії командування поєднуються з горизонтальними мережами координації, формальні структури доповнюються неформальними зв'язками, постійні організаційні форми співіснують з тимчасовими проєктними структурами.

Функціональний вимір системного підходу зосереджується на дослідженні того, як безпекові інституції виконують свої функції в контексті загальносистемних цілей. Ключовим є розуміння функціональної диференціації та інтеграції – як різні інституції спеціалізуються на виконанні специфічних функцій, водночас забезпечуючи їх узгодження для досягнення синергії [183]. Системний аналіз дозволяє виявити функціональні дублювання, лакуни, неузгодженості, що знижують ефективність системи.

Процесуальний аспект розкриває динамічну природу функціонування безпекових інституцій. Система національної безпеки постає не як статична структура, а як сукупність взаємопов'язаних процесів – інформаційних потоків, процедур прийняття рішень, циклів планування та виконання, контурів управління та контролю. Системний підхід дозволяє простежити, як імпульси (інформація, рішення, ресурси) поширюються через систему, трансформуються, посилюються або гасяться.

Особливої уваги в рамках системного підходу заслуговує концепція зворотних зв'язків – позитивних (підсилюючих) та негативних (стабілізуючих). В безпекових системах негативні зворотні зв'язки забезпечують стабільність та передбачуваність – механізми контролю, системи стримувань та противаг, процедури корекції відхилень. Позитивні зворотні зв'язки можуть призводити як до бажаних ефектів (швидка мобілізація ресурсів у кризовій ситуації), так і до небажаних (ескалація конфліктів, бюрократизація).

Темпоральний вимір системного підходу розкриває різночасовість процесів у безпекових інституціях. Різні компоненти системи функціонують у різних часових масштабах – від оперативного реагування в режимі реального часу до довгострокового стратегічного планування на десятиліття. Системний аналіз дозволяє виявити темпоральні неузгодженості, коли швидкість змін у середовищі перевищує адаптивну спроможність інституцій, або коли короткострокові рішення суперечать довгостроковим цілям.

Просторовий аспект системного підходу враховує багаторівневу природу безпекових інституцій – від локального до глобального рівня. Сучасна система національної безпеки функціонує одночасно на субнаціональному (регіональні структури), національному (центральні органи), міжнародному (двосторонні відносини) та наднаціональному (міжнародні організації) рівнях. Системний аналіз дозволяє зрозуміти, як ці рівні взаємодіють, які виникають міжрівневі напруження та як забезпечується вертикальна інтеграція.

Середовищний контекст також є невід'ємною частиною системного аналізу безпекових інституцій. Система національної безпеки є відкритою системою, що постійно обмінюється енергією, інформацією та ресурсами із середовищем. Це середовище включає політичну систему країни, економіку, суспільство, міжнародне оточення, технологічний ландшафт. Зміни в середовищі створюють виклики та можливості для безпекових інституцій, вимагаючи постійної адаптації. Критично важливим є розуміння границь системи – що входить до системи національної безпеки, а що залишається в середовищі. Ці границі не є фіксованими та непроникними; вони постійно переосмислюються та пересуваються. Процеси секюритизації розширюють границі системи, включаючи нові сфери (кібербезпека, екологічна безпека), тоді як процеси десекюритизації можуть звужувати їх [109].

Кібернетичний аспект системного підходу фокусується на механізмах управління та контролю в безпекових інституціях. Концепція гомеостазу пояснює, як система підтримує стабільність ключових параметрів попри

зовнішні збурення. Проте в умовах гібридних загроз важливішою стає концепція гомеорезу – здатності системи підтримувати траєкторію розвитку, адаптуючись до змін. Це вимагає не просто реактивного управління відхиленнями, а проактивного управління еволюцією системи.

Інформаційний вимір системного підходу розглядає безпекові інституції як інформаційно-процесуючі системи. Якість функціонування системи національної безпеки критично залежить від її здатності збирати, обробляти, інтерпретувати та використовувати інформацію. Системний аналіз дозволяє виявити інформаційні патології – затримки в передачі інформації, її спотворення, інформаційні перевантаження, інформаційні лакуни.

У свою чергу, комплексність як ключова характеристика безпекових систем вимагає особливих методологічних підходів. Традиційні лінійні моделі причинно-наслідкових зв'язків виявляються недостатніми для розуміння систем з високим рівнем взаємозалежності, нелінійності, емерджентності. Теорія складності пропонує нові концептуальні інструменти – атрактори, біфуркації, фазові переходи, самоорганізація – які збагачують системний аналіз безпекових інституцій [171].

Еволюційний аспект системного підходу розглядає безпекові інституції не як статичні утворення, а як системи, що постійно еволюціонують. Ця еволюція включає процеси адаптації до змін середовища, селекції успішних організаційних форм, мутації через інновації, коеволюції з іншими системами. Розуміння еволюційної динаміки критично важливе для прогнозування майбутнього розвитку безпекових інституцій та управління їх трансформацією.

Отже, як можна бачити, практичне застосування системного підходу в дослідженні безпекових інституцій вимагає поєднання різних методів та технік. Системне картування дозволяє візуалізувати структуру зв'язків між інституціями. Моделювання системної динаміки допомагає зрозуміти поведінку системи в часі. Сценарний аналіз розкриває можливі траєкторії розвитку. Аналіз чутливості виявляє критичні точки системи. Всі ці методи в

сукупності формують потужний інструментарій системного дослідження.

Інституційний аналіз як методологічний підхід до вивчення процесів управління національною безпекою відкриває унікальні можливості для розуміння глибинних механізмів функціонування безпекової системи, що виходять за межі формальних організаційних структур та офіційних процедур. Цей підхід дозволяє осягнути складну взаємодію формальних правил та неформальних практик, організаційних структур та культурних норм, раціональних стратегій та історично сформованих патернів поведінки.

Теоретичні витоки інституційного аналізу в контексті національної безпеки сягають класичних робіт з політичної економії та соціології, проте сучасне його застосування збагачене досягненнями нового інституціоналізму, який подолав обмеженість суто формально-юридичного підходу. Ключовою тезою є розуміння інститутів не просто як організацій чи правил, а як стійких патернів взаємодії, що структурують поведінку акторів у сфері національної безпеки [163]. Ці патерни включають формальні норми (закони, статути, регламенти) та неформальні практики (традиції, неписані правила, рутини), які в сукупності визначають «правила гри» в безпековій сфері.

Онтологічна специфіка інституційного підходу полягає в розумінні інститутів як конститутивних елементів соціальної реальності, що не просто регулюють поведінку, а формують саму ідентичність та інтереси акторів. В контексті національної безпеки це означає, що безпекові інституції не лише виконують функцію захисту, а й визначають саме розуміння того, що є загрозою, які цінності підлягають захисту, які методи є прийнятними. Інституційне середовище формує «безпекову свідомість» як на рівні еліт, так і суспільства загалом.

Центральною категорією інституційного аналізу є концепція інституційної логіки – глибинних принципів організації та легітимації діяльності в певній сфері. У сфері національної безпеки можуть співіснувати та конкурувати різні інституційні логіки: мілітаристська (пріоритет силових методів), дипломатична (акцент на переговорах та компромісах),

технократична (віра в технологічні рішення), демократична (підзвітність та прозорість). Конфлікти між цими логіками часто лежать в основі інституційних дисфункцій та неефективності управління.

Методологічна цінність інституційного аналізу проявляється в його здатності пояснити стійкість неефективних практик та опір реформам у безпековій сфері. Концепція залежності від попереднього шляху (path dependence) розкриває, як історично сформовані інституційні конфігурації створюють інерцію, що ускладнює впровадження навіть очевидно необхідних змін. Початкові інституційні вибори, зроблені в критичні моменти (critical junctures), можуть визначати траєкторію розвитку безпекових інституцій на десятиліття вперед.

Особливої уваги в інституційному аналізі заслуговує феномен інституційного ізоморфізму – тенденції організацій в певному полі ставати схожими одна на одну. У безпековій сфері це проявляється через наслідування «кращих практик», впровадження стандартів союзників, копіювання організаційних форм [118]. Проте механічне запозичення інституційних форм без урахування локального контексту часто призводить до появи «порожніх оболонок» – формально існуючих, але реально недієздатних інституцій.

Аналіз інституційної комплементарності розкриває важливість системної узгодженості різних інститутів у сфері національної безпеки. Ефективність окремого інституту залежить не лише від його внутрішньої організації, а й від того, наскільки він узгоджується з іншими елементами інституційної системи. Наприклад, демократичний цивільний контроль над силовими структурами може бути ефективним лише за наявності незалежних медіа, розвиненого громадянського суспільства, професійної бюрократії. Відсутність такої комплементарності призводить до інституційних дисбалансів.

Динамічний аспект інституційного аналізу фокусується на процесах інституційних змін у безпековій сфері. На відміну від уявлення про інститути як статичні структури, сучасний підхід визнає їх здатність до еволюції через

різні механізми: поступове наростання малих змін (layering), заміщення старих практик новими (displacement), перетворення існуючих інститутів для нових цілей (conversion), поступове витіснення (drift) [161]. Розуміння цих механізмів критично важливе для управління інституційними реформами.

Когнітивний вимір інституційного аналізу звертає увагу на роль ідей, переконань, ментальних моделей у формуванні та функціонуванні безпекових інститутів. Інститути не просто обмежують поведінку через санкції – вони формують когнітивні рамки, через які актори інтерпретують реальність. Безпекові доктрини, стратегічні культури, організаційні міфи створюють призму, через яку оцінюються загрози та формулюються відповіді на них.

Особливу методологічну цінність має аналіз неформальних інститутів у сфері національної безпеки. Ці неписані правила та практики часто мають більший вплив на реальну поведінку, ніж формальні норми. Патрон-клієнтські мережі в силових структурах, неформальні канали прийняття рішень, традиції «телефонного права», корупційні схеми – все це приклади неформальних інститутів, які можуть як доповнювати, так і підривати формальну інституційну систему. Аналіз інституційних акторів розкриває складність агентських відносин у безпековій сфері. Інституційний підхід долає спрощене уявлення про унітарних раціональних акторів, показуючи, як інституційна позиція формує інтереси та стратегії. Міністр оборони діє не просто як індивід, а як носій інституційної ролі з відповідними обмеженнями, очікуваннями, ресурсами. Конфлікти в безпековій сфері часто є не особистими, а інституційними – відображенням різних організаційних інтересів та логік.

Порівняльний інституційний аналіз дозволяє виявити варіації в організації безпекових систем різних країн та їх вплив на ефективність. Чому одні країни успішно адаптуються до нових загроз, а інші – ні? Чому схожі реформи дають різні результати в різних контекстах? Інституційний підхід дає відповіді через аналіз національних особливостей інституційного дизайну, історичних траєкторій, культурних факторів. Мікрорівень інституційного аналізу фокусується на повсякденних практиках функціонування безпекових

установ. Як проводяться наради? Як циркулюють документи? Як приймаються кадрові рішення? Ці на перший погляд дрібні деталі насправді формують інституційну культуру та визначають ефективність системи. Етнографічні методи дозволяють проникнути в «чорну скриньку» безпекових інституцій та зрозуміти логіку їх функціонування зсередини.

Інституційний аналіз політики пам'яті в безпековій сфері розкриває, як історичний досвід кодується в інституційних формах. Війни, кризи, успіхи та поразки минулого залишають інституційні «шрами» та «трофеї», що впливають на сучасні рішення. Інституційна пам'ять може бути як ресурсом (накопичений досвід), так і тягарем (застарілі уявлення). Селективність інституційної пам'яті – що згадується, а що забувається – формує безпекову ідентичність.

У цілому, практичне значення інституційного аналізу для реформування безпекового сектору важко переоцінити. Він дозволяє зрозуміти, чому формально правильні реформи часто не дають очікуваних результатів, як неформальні практики саботують офіційні зміни, які інституційні конфігурації сприяють або перешкоджають інноваціям. Без глибокого інституційного аналізу реформи ризикують залишитися поверховими імітаціями змін.

Синергетичний підхід у дослідженні динаміки безпекового управління відкриває принципово нові горизонти розуміння процесів самоорганізації, нелінійності та емерджентності в системі національної безпеки. Базуючись на теорії складних систем та нелінійної динаміки, синергетика пропонує революційну оптику, що дозволяє побачити безпекове управління не як механістичний процес командування та контролю, а як живу, самоорганізовану систему з власними законами розвитку.

Фундаментальним положенням синергетичного підходу є визнання того, що система національної безпеки належить до класу складних адаптивних систем, які характеризуються великою кількістю взаємодіючих елементів, нелінійними зв'язками між ними, здатністю до самоорганізації та емерджентною поведінкою [132]. Ці системи принципово відрізняються від

простих механічних систем, для яких характерна лінійність, передбачуваність та можливість редукції до суми частин.

Концепція нелінійності є наріжним каменем синергетичного підходу до безпекового управління. В лінійних системах існує пропорційність між причиною та наслідком – малі впливи породжують малі зміни, великі впливи – великі зміни. Натомість у нелінійних системах ця пропорційність порушується: незначний вплив може призвести до катастрофічних наслідків (ефект метелика), тоді як масштабні зусилля можуть не дати жодного результату. У контексті національної безпеки це означає, що невелика кібератака може паралізувати критичну інфраструктуру країни, а мільярдні інвестиції в оборону можуть виявитися марними проти асиметричних загроз.

Синергетичний підхід розкриває феномен самоорганізації в безпекових системах – здатність спонтанного виникнення порядку з хаосу без зовнішнього керуючого впливу. Класичні приклади самоорганізації в безпековій сфері включають формування волонтерських рухів під час криз, спонтанну координацію дій різних акторів у надзвичайних ситуаціях, виникнення неформальних мереж обміну інформацією між безпековими структурами [147]. Розуміння механізмів самоорганізації дозволяє не боротися з нею, а використовувати її потенціал для підвищення ефективності системи.

Концепція атракторів – станів, до яких тяжіє система, – має глибоке значення для розуміння динаміки безпекового управління. Система національної безпеки може мати кілька атракторів: стабільна рівновага (мирний стан), циклічні коливання (періодичні загострення), хаотична динаміка (перманентна криза). Завдання управління полягає не в жорсткому утриманні системи в певному стані, а в створенні умов для переходу до бажаного атрактора та уникнення небажаних.

Особливе значення має концепція біфуркацій – критичних точок, в яких система може піти різними шляхами розвитку. В історії національної безпеки такими точками біфуркації часто стають кризи, війни, революції – моменти, коли малі фактори можуть визначити подальшу траєкторію на роки вперед.

Синергетичний підхід підкреслює важливість розпізнавання наближення до точок біфуркації та готовності до швидкого реагування в ці критичні моменти.

Флуктуації – випадкові відхилення від середнього стану – в синергетичній парадигмі розглядаються не як шум, який треба придушити, а як джерело інновацій та адаптації. У безпековому управлінні флуктуації можуть проявлятися як несанкціоновані ініціативи окремих підрозділів, експерименти з новими методами, відхилення від стандартних процедур. Замість жорсткого придушення таких флуктуацій, синергетичний підхід пропонує створювати «простір для експериментів», де корисні інновації можуть бути виявлені та масштабовані.

Принцип підпорядкування (принцип Хакена) розкриває механізм виникнення колективної поведінки в складних системах. Коли система наближається до критичного стану, виникають параметри порядку, які підпорядковують собі поведінку всіх елементів системи. У безпековому контексті такими параметрами порядку можуть бути домінуючі наративи (наприклад, «країна у стані війни»), які визначають поведінку всіх акторів незалежно від їх індивідуальних переконань.

Концепція дисипативних структур Пригожина має пряме відношення до розуміння безпекових систем. Ці структури підтримують свою організацію за рахунок постійного обміну енергією та інформацією із середовищем, перебуваючи далеко від термодинамічної рівноваги. Система національної безпеки є класичною дисипативною структурою – вона потребує постійного припливу ресурсів, інформації, кадрів для підтримання своєї організованості. Спроби створити «закриту» безпекову систему приречені на деградацію.

Фрактальність як властивість складних систем проявляється в самоподібності структур на різних масштабах. У безпековій системі можна спостерігати подібні патерни організації на рівні окремого підрозділу, регіональної структури, національної системи, міжнародних альянсів. Розуміння фрактальної природи дозволяє екстраполювати закономірності з одного масштабу на інший, але з урахуванням емерджентних властивостей

кожного рівня [162].

Синергетичний підхід радикально переосмислює роль хаосу в безпекових системах. Замість розгляду хаосу як виключно деструктивного явища, синергетика показує його конструктивну роль як джерела варіативності, необхідної для адаптації. Контрольований хаос (наприклад, конкуренція між різними аналітичними підрозділами) може підвищувати креативність та інноваційність системи. Водночас надмірний порядок може призводити до ригідності та втрати адаптивності.

Концепція коеволюції розкриває взаємозалежність розвитку безпекової системи та її середовища. Система національної безпеки не просто адаптується до загроз – вона співеволюціонує з ними. Кожна дія безпекових структур змінює середовище, що, в свою чергу, вимагає нової адаптації. Гонка озброєнь, еволюція терористичних тактик у відповідь на контртерористичні заходи, розвиток кіберзагроз паралельно з розвитком кіберзахисту – все це приклади коеволюційної динаміки.

Мережева динаміка в синергетичній перспективі виявляє emergent properties безпекових мереж, що виникають зі взаємодії вузлів. Сила мережі визначається не лише кількістю та якістю вузлів, а й топологією зв’язків, наявністю хабів, ступенем зв’язності. Синергетичний аналіз показує, як локальні взаємодії між елементами мережі породжують глобальні патерни – від інформаційних каскадів до колективної мобілізації.

Темпоральна складність безпекових систем у синергетичній інтерпретації виявляється через співіснування різних часових масштабів та ритмів. Швидкі процеси (оперативні рішення) накладаються на повільні (інституційні зміни), створюючи складну темпоральну динаміку. Резонанси між різними ритмами можуть призводити до непередбачуваних ефектів – від синхронізації дій до системних криз [189].

Концепція edge of chaos (край хаосу) має особливе значення для безпекового управління. Дослідження показують, що складні адаптивні системи найбільш інноваційні та адаптивні, коли функціонують на межі між

порядком та хаосом. Занадто жорсткий порядок робить систему ригідною, занадто сильний хаос – некерованою. Мистецтво управління полягає в утриманні системи в цій продуктивній зоні.

Практичні імплікації синергетичного підходу для безпекового управління є революційними. Замість спроб тотального контролю та планування, синергетика пропонує «м'яке управління» через створення умов для бажаної самоорганізації. Замість боротьби з невизначеністю – використання її творчого потенціалу. Замість лінійних стратегій – адаптивні стратегії з множинними сценаріями. Замість централізованого командування – розподілене лідерство з автономією локальних акторів.

Слід наголосити, що синергетичний підхід не заперечує важливості планування та контролю, але поміщає їх у новий контекст розуміння меж керованості складних систем. Він пропонує нову філософію безпекового управління, адекватну складності та динамічності сучасних викликів, де гнучкість важливіша за жорсткість, адаптивність – за стабільність, а мудрість управління полягає в гармонізації з природними процесами самоорганізації системи.

Як можна бачити з викладеного вище, у попередніх параграфах, гібридні безпекові виклики за своєю природою є трансграничними феноменами, що перетинають традиційні дисциплінарні межі та вимагають принципово нового методологічного підходу, здатного інтегрувати знання та методи з різних галузей науки. Тому можна стверджувати, що міждисциплінарна методологія постає не просто як бажана опція, а як імператив для адекватного осмислення та ефективного реагування на комплексні загрози, що характеризують сучасне безпекове середовище. При цьому епістемологічні засади міждисциплінарного підходу до гібридних викликів базуються на визнанні принципової обмеженості монодисциплінарної перспективи. Військова наука може пояснити тактику гібридних операцій, але не їх інформаційно-психологічний вплив. Політологія розкриває механізми підриву легітимності, але не технічні аспекти кібератак. Економіка аналізує фінансову зброю, але не

культурні коди, через які вона діє [192]. Лише синтез різних дисциплінарних оптик дозволяє побачити гібридну загрозу в її цілісності.

Відтак, методологічний плюралізм стає необхідною умовою дослідження гібридних викликів. Кожна дисципліна приносить власні методи: військові науки – оперативний аналіз та воєнні ігри; кібернетика – моделювання складних систем; психологія – експерименти з когнітивними упередженнями; соціологія – мережевий аналіз; антропологія – етнографічні дослідження; комунікативістика – дискурс-аналіз. Інтеграція цих методів вимагає не еклектичного змішування, а продуманого синтезу на основі чіткої методологічної рамки.

Трансдисциплінарність як вищий рівень інтеграції передбачає не просто комбінування існуючих дисциплінарних підходів, а створення нових концептуальних рамок, що виходять за межі окремих дисциплін. У контексті гібридних загроз це означає розробку нових понять та теорій, які не належать жодній окремій дисципліні, але необхідні для осмислення феномену. Концепції «гібридності», «сірих зон», «когнітивної безпеки» є прикладами таких трансдисциплінарних конструктів.

Інтеграція кількісних та якісних методів набуває особливого значення при дослідженні гібридних викликів. Кількісні методи дозволяють виявляти патерни в великих масивах даних – від аналізу соціальних мереж до моделювання каскадних ефектів. Якісні методи розкривають смисли, мотивації, культурні коди, що лежать в основі гібридних стратегій. Метод «змішаних досліджень» дозволяє використовувати сильні сторони обох підходів: кількісні дані забезпечують широту охоплення, якісні – глибину розуміння.

Когнітивна інтеграція різнодисциплінарних знань становить окремий методологічний виклик. Представники різних дисциплін не просто використовують різні методи – вони мислять різними категоріями, оперують різними базовими припущеннями, мають різні критерії валідності знання. Військовий стратег мислить в термінах сили та стримування, психолог – в

термінах сприйняття та упереджень, економіст – в термінах стимулів та раціональності. Створення спільної мови та концептуальних мостів між дисциплінами вимагає спеціальних зусиль.

Системна інтеграція є ключовим принципом міждисциплінарної методології. Гібридні виклики є системними феноменами, де військові, політичні, економічні, інформаційні, психологічні компоненти взаємодіють синергетично. Методологія повинна схоплювати ці взаємодії, а не розкладати явище на окремі дисциплінарні шухлядки. Теорія складних адаптивних систем пропонує метамову для такої інтеграції, дозволяючи описувати емерджентні властивості гібридних загроз.

Контекстуальна чутливість міждисциплінарного підходу визнає, що гібридні виклики завжди розгортаються в конкретному історичному, культурному, геополітичному контексті. Універсальні моделі та теорії повинні адаптуватися до локальних умов. Це вимагає залучення регіональних досліджень, що поєднують історію, культурологію, політичну географію конкретних регіонів. Розуміння локального контексту часто виявляється критичним для правильної інтерпретації гібридних загроз.

Темпоральна складність гібридних викликів вимагає інтеграції різних часових перспектив. Історичні науки розкривають довгі цикли та залежності. Політологія фокусується на середньострокових політичних процесах. Кібернетика та комунікативістика досліджують миттєві інформаційні каскади. Футурологія прогнозує можливі сценарії розвитку. Міждисциплінарна методологія повинна інтегрувати ці різні темпоральності в coherent understanding динаміки гібридних загроз.

Практична орієнтованість міждисциплінарних досліджень гібридних викликів відрізняє їх від суто академічних студій. Action research підхід передбачає тісну взаємодію дослідників з практиками безпекового сектору, ітеративний процес генерування та тестування рішень, швидкий зворотний зв’язок від реальності до теорії. Це вимагає особливих форм організації досліджень – від наявності окремих дослідників в безпекових структурах до

спільних дослідницько-практичних лабораторій.

Критична рефлексивність є необхідною умовою міждисциплінарної методології. Дослідники повинні усвідомлювати власні дисциплінарні упередження, культурні припущення, політичні позиції, що впливають на їх аналіз. Особливо це важливо при дослідженні гібридних загроз, де об'єктивність ускладнена інформаційним туманом та навмисними маніпуляціями. Методи критичної саморефлексії, наукової колоборації та інші допомагають підвищити об'єктивність досліджень.

Інноваційні методи збору та аналізу даних відкривають нові можливості для міждисциплінарних досліджень. Так, соціальні науки останнім часом активно використовують big data та машинне навчання для аналізу соціальних процесів. Представники гуманітарних наук застосовують цифрові методи до культурних артефактів. Нейроекономіка поєднує нейронауку з економічною теорією для розуміння прийняття рішень. І всі ці гібридні методологічні підходи особливо релевантні для дослідження гібридних загроз.

Мережева організація міждисциплінарних досліджень відображає мережеву природу самих гібридних викликів. Традиційні ієрархічні дослідницькі структури поступаються місцем гнучким мережам, що об'єднують дослідників з різних інституцій та країн. Віртуальні дослідницькі простори дозволяють співпрацювати в реальному часі, незважаючи на географічні відстані, а краудсорсингові дослідження залучає широке коло експертів до аналізу конкретних проблем.

Етичні виклики міждисциплінарних досліджень гібридних загроз є особливо гострими. Різні дисципліни мають різні етичні стандарти: що прийнятно для військових досліджень, може бути неетичним для соціальної психології. Дослідження гібридних загроз часто торкаються чутливих питань національної безпеки, що створює дилеми між науковою відкритістю та безпековими міркуваннями. Розробка спільних етичних рамок для міждисциплінарних безпекових досліджень є нагальним завданням [193].

Педагогічні імплікації міждисциплінарного підходу вимагають

переосмислення освіти в сфері безпеки. Традиційна вузькоспеціалізована підготовка не готує фахівців до розуміння гібридних викликів. Необхідні нові освітні програми, що поєднують безпекові студії з кібернетикою, психологією, комунікативістикою, регіональними дослідженнями. T-shaped professionals – фахівці з глибокими знаннями в одній галузі та широким розумінням суміжних – стають новим ідеалом.

Інституційні форми підтримки міждисциплінарних досліджень вимагають інновацій в організації науки. Традиційні дисциплінарні департаменти та фінансування за галузями створюють бар'єри для міждисциплінарної співпраці. Необхідні нові форми – міждисциплінарні дослідницькі центри, проблемно-орієнтовані дослідницькі програми, гнучкі схеми фінансування досліджень. Особливо важливим є створення кар'єрних траєкторій для міждисциплінарних дослідників, чиї роботи можуть не вписуватися в традиційні дисциплінарні рамки.

Подібна особливість дослідження гібридних загроз і протидії ним призводить до того, що сучасне оцінювання ефективності інституційних перетворень у безпековій сфері становить одну з найскладніших методологічних проблем сучасного публічного управління, оскільки вимагає врахування множинності критеріїв, довготривалості ефектів, складності причинно-наслідкових зв'язків та специфічності безпекового контексту. У той же час, розробка адекватних методів оцінювання є критично важливою для забезпечення підходу, що базується на доказах, до реформування безпекового сектору та уникнення імітаційних змін.

І тут концептуальною основою оцінювання ефективності інституційних перетворень є розуміння багатовимірності самого поняття ефективності в безпековому контексті. На відміну від бізнес-сектору, де ефективність часто може бути зведена до фінансових показників, у безпековій сфері необхідно враховувати технічну ефективність (досягнення поставлених цілей), економічну ефективність (оптимальне використання ресурсів), соціальну ефективність (відповідність суспільним очікуванням), політичну ефективність

(зміцнення легітимності) [173]. Ці виміри можуть перебувати в складних, іноді конфліктних відносинах між собою.

Темпоральна проблематика оцінювання полягає в розбіжності між короткостроковими та довгостроковими ефектами інституційних перетворень. Реформи, що дають швидкі позитивні результати, можуть мати негативні довгострокові наслідки, і навпаки. Наприклад, швидке скорочення чисельності силових структур може дати короткострокову економію бюджету, але призвести до втрати інституційної пам'яті та зниження обороноздатності в довгостроковій перспективі. Методологія оцінювання повинна враховувати різні часові горизонти та динаміку розгортання ефектів.

Контрфактуальна проблема є центральною для оцінювання ефективності: як визначити, що саме інституційні перетворення призвели до спостережуваних змін, а не інші фактори? У безпековій сфері ця проблема ускладнюється унікальністю кожної ситуації та неможливістю проведення контрольованих експериментів. Методи квазіекспериментального дизайну, адаптовані до безпекового контексту, дозволяють частково вирішити цю проблему, але вимагають обережної інтерпретації [95].

Проблема вимірюваності є особливо гострою в безпековій сфері, де багато критично важливих аспектів важко квантифікувати. Як виміряти рівень довіри між безпековими відомствами? Як оцінити якість стратегічного мислення? Як квантифікувати готовність до майбутніх невідомих загроз? Поєднання кількісних та якісних методів стає необхідністю, але вимагає розробки складних методологічних рамок для їх інтеграції.

Індикаторний підхід є найпоширенішим методом оцінювання, але його застосування в безпековій сфері має специфічні обмеження. Традиційні індикатори типу «кількість проведених навчань» або «відсоток укомплектованості» можуть створювати ілюзію об'єктивності, але не відображати реальної ефективності. Необхідна розробка smart indicators, які б відображали не лише кількісні параметри діяльності, а й якісні зміни в спроможностях. Критично важливим є баланс між індикаторами процесу

(process indicators), результату (output indicators) та впливу (impact indicators).

Методологія збалансованої системи показників (Balanced Scorecard), адаптована до безпекового контексту, пропонує комплексний підхід до оцінювання [146]. Чотири перспективи – фінансова, клієнтська (суспільство), внутрішніх процесів та навчання/розвитку – дозволяють охопити різні аспекти інституційної ефективності. Специфіка безпекової сфери вимагає додавання п'ятої перспективи – міжвідомчої координації та міжнародної співпраці.

Бенчмаркінг як метод порівняльного оцінювання дозволяє співставити ефективність національних безпекових інституцій з кращими міжнародними практиками. Проте механічне порівняння без урахування контекстуальних факторів може призводити до хибних висновків. Розробка контекстуально-чутливого бенчмаркінгу вимагає ідентифікації порівнянних країн (peer countries), нормалізації показників з урахуванням національних особливостей, якісного аналізу факторів успіху.

Мережевий аналіз ефективності фокусується на оцінюванні якості взаємодій між різними інституціями безпекового сектору. Традиційні ієрархічні моделі оцінювання не схоплюють горизонтальні зв'язки та мережеві ефекти, які часто є критичними для ефективності. Методи аналізу соціальних мереж дозволяють візуалізувати та квантифікувати щільність зв'язків, центральність акторів, наявність структурних дірок, що впливають на швидкість та якість координації.

Оцінювання організаційної спроможності (capacity assessment) виходить за межі простого вимірювання ресурсів та активностей, фокусуючись на здатності інституцій виконувати свої функції в динамічному середовищі. Методологія включає аналіз п'яти вимірів спроможності: стратегічної (здатність формулювати візію та стратегію), організаційної (ефективність структур та процесів), кадрової (компетенції персоналу), ресурсної (адекватність та ефективність використання ресурсів), контекстуальної (здатність взаємодіяти із середовищем) [175].

Тому експертні методи оцінювання залишаються важливими в умовах,

коли формальні індикатори не можуть охопити всю складність безпекових процесів. Проте традиційні експертні опитування часто страждають від суб'єктивності та упереджень. Сучасні методи структурованого експертного оцінювання – метод Дельфі, номінальних груп, аналітичних ієрархій – дозволяють підвищити об'єктивність та надійність експертних суджень. Критичним є формування збалансованих експертних панелей з представників різних секторів та перспектив.

Партисипативне оцінювання залучає різні групи стейкхолдерів до процесу оцінки ефективності інституційних перетворень. У безпековій сфері це особливо важливо, оскільки успіх реформ залежить від їх сприйняття не лише професіоналами, а й суспільством. Методи включають фокус-групи з представниками громадськості, опитування довіри до безпекових інституцій, громадські слухання щодо результатів реформ. Виклик полягає в балансуванні між залученням громадськості та збереженням необхідного рівня конфіденційності.

Оцінювання стійкості (resilience assessment) фокусується на здатності безпекових інституцій витримувати шоки та адаптуватися до змін. Традиційні методи оцінювання часто фіксують ефективність в стабільних умовах, але не враховують поведінку системи в кризових ситуаціях. Методологія включає стрес-тестування інституцій через симуляції та сценарні вправи, аналіз попередніх криз та реакції на них, оцінку резервування та гнучкості системи [70].

Процесне оцінювання (process evaluation) доповнює оцінювання результатів аналізом того, як саме впроваджуються інституційні зміни. Це особливо важливо для розуміння розривів між задумом реформ та їх реалізацією. Методи включають спостереження за процесами впровадження, аналіз документообігу, інтерв'ю з учасниками процесу, відстеження ключових рішень. Процесне оцінювання дозволяє виявити приховані перешкоди та неформальні практики, що впливають на успіх реформ.

Оцінювання впливу (impact evaluation) намагається встановити

причинно-наслідкові зв’язки між інституційними перетвореннями та змінами в безпековій ситуації. Це найскладніший тип оцінювання, оскільки безпекові результати залежать від множини факторів. Методи включають побудову теорій змін (theories of change), що експліцитно визначають механізми впливу; використання змішаних методів для тріангуляції доказів; довгострокових досліджень для відстеження довгострокових ефектів.

Таким чином, комплексність сучасних безпекових викликів вимагає розвитку методів оцінювання, здатних охопити системні ефекти та емерджентні властивості. При цьому агент-базоване моделювання дозволяє симулювати поведінку безпекової системи за різних інституційних конфігурацій. Аналіз складних адаптивних систем розкриває нелінійні ефекти інституційних змін. А аналіз великих даних відкриває нові можливості для виявлення патернів та аномалій у функціонуванні безпекових інституцій.

Висновки до першого розділу

1. Дослідження теоретико-методологічних засад інституціалізації публічного управління національною безпекою в умовах гібридної війни дозволило встановити, що інституціалізація виступає фундаментальним процесом трансформації спонтанних та ситуативних управлінських практик у стійкі організаційні форми, здатні забезпечувати ефективне функціонування системи національної безпеки в умовах високої невизначеності та багатовекторних загроз. Сутність інституціалізації в безпековій сфері полягає не лише у формальному створенні організаційних структур та нормативно-правової бази, а й у глибинній трансформації управлінської культури, формуванні нових ціннісних орієнтирів та поведінкових моделей, які визначають характер взаємодії між різними суб’єктами забезпечення національної безпеки. При цьому ефективність інституціалізації визначається здатністю створюваних інституцій поєднувати стабільність базових принципів

функціонування з гнучкістю та адаптивністю до динамічних змін безпекового середовища.

2. Концептуалізація національної безпеки як об’єкта публічного управління в сучасних умовах вимагає переходу від традиційного державоцентричного та мілітаристського розуміння до комплексного багатовимірного підходу, що охоплює військові, політичні, економічні, соціальні, інформаційні, кібернетичні та інші виміри безпеки. Взаємозв’язок між інституціалізацією та ефективністю управління національною безпекою має діалектичний характер: з одного боку, розвинене інституційне середовище створює передумови для ефективного безпекового управління через забезпечення координації, легітимності та ресурсної бази; з іншого боку, ефективність управління стимулює подальший інституційний розвиток через накопичення досвіду та вдосконалення організаційних форм. Структурно-функціональні компоненти інституціалізації безпекового управління утворюють складну архітектуру, ефективність якої визначається не лише якістю окремих елементів, а й їх системною узгодженістю та синергією.

3. Феномен гібридної війни фундаментально трансформує парадигму публічного управління національною безпекою, розмиваючи традиційні межі між війною та миром, внутрішніми та зовнішніми загрозами, державними та недержавними акторами, створюючи якісно нове безпекове середовище, що характеризується високим рівнем невизначеності, амбівалентності та взаємопов’язаності різнорідних загроз. Гібридні загрози відрізняються комплексністю, адаптивністю, використанням легальних інструментів для досягнення нелегітимних цілей, експлуатацією когнітивних вразливостей, довготривалим характером та мережевою організацією, що вимагає від системи публічного управління розвитку принципово нових компетенцій та механізмів реагування. Адаптивність публічного управління до викликів гібридної війни передбачає здатність до швидкої реконфігурації структур та процесів, функціонування в різних темпоральних режимах, когнітивної гнучкості, ресурсної мобільності та організаційного навчання.

4. Інституційні механізми протидії гібридним загрозам у системі національної безпеки мають базуватися на принципах комплексності, міжвідомчої координації, проактивності та стійкості. Ключовими елементами інституційної архітектури протидії виступають: інтегровані ситуаційні центри як «нервові вузли» системи; механізми раннього попередження, здатні виявляти слабкі сигнали та латентні загрози; система стратегічних комунікацій для протидії інформаційним атакам; механізми захисту критичної інфраструктури на принципах резильєнтності; фінансово-економічні інструменти протидії гібридному впливу; інтегровані правоохоронні та безпекові функції; механізми мобілізації суспільства як активного суб'єкта забезпечення національної стійкості. Ефективність цих механізмів визначається не лише їх окремою функціональністю, а й здатністю до синхронізованої дії в умовах динамічного та непередбачуваного безпекового середовища.

5. Методологічний інструментарій дослідження інституціалізації публічного управління національною безпекою в умовах гібридної війни вимагає поєднання різних наукових підходів та методів. Системний підхід дозволяє осягнути безпекові інституції як цілісну систему з емерджентними властивостями, складними зворотними зв'язками та динамічною взаємодією з середовищем. Інституційний аналіз розкриває глибинні механізми функціонування безпекових структур через дослідження формальних правил та неформальних практик, інституційних логік та залежностей від попереднього шляху. Синергетичний підхід відкриває розуміння процесів самоорганізації, нелінійності та біфуркацій у безпековому управлінні. Міждисциплінарна методологія забезпечує інтеграцію знань з різних галузей для адекватного осмислення комплексної природи гібридних викликів.

6. Критерії та показники інституційної зрілості системи управління національною безпекою формують багатовимірну систему оцінювання, що охоплює структурну, функціональну, нормативно-правову, ресурсну, процесну, інформаційно-аналітичну, адаптивну, культурну, інтеграційну та

результативну зрілість. Методи оцінювання ефективності інституційних перетворень у безпековій сфері мають враховувати специфіку безпекового контексту, зокрема множинність критеріїв ефективності, довготривалість ефектів, складність каузальних зв’язків та проблему контрфактуальності. Поєднання кількісних та якісних методів, індикаторного підходу з експертними оцінками, процесного оцінювання з оцінюванням впливу дозволяє створити комплексну картину інституційної динаміки та обґрунтувати напрями подальших реформ у сфері національної безпеки.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ІНСТИТУЦІАЛІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

2.1. Нормативно-правове та організаційне забезпечення системи управління національною безпекою України

Нормативно-правова база функціонування системи національної безпеки України формує юридичний фундамент, на якому базується вся архітектура безпекових інституцій, механізмів та процедур забезпечення захисту національних інтересів в умовах гібридної війни. Аналіз цієї бази дозволяє виявити як досягнення в інституційному розвитку, так і прогалини, що створюють вразливості в системі протидії гібридним загрозам.

Конституційні основи забезпечення національної безпеки закладені в Основному Законі України, який визначає фундаментальні принципи організації безпекової сфери. Конституція встановлює, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [36]. Водночас конституційні норми, прийняті в мирний час, виявилися недостатньо адаптованими до реалій гібридної агресії, що створює правові колізії при застосуванні особливих режимів та обмежувальних заходів.

Базовим документом у сфері національної безпеки є Закон України «Про національну безпеку України» від 2018 року, який замінив застарілий закон 2003 року та врахував досвід протидії російській агресії. Цей закон запровадив нову парадигму організації сектору безпеки і оборони, визначивши його як систему органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з

правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу, діяльність яких перебуває під демократичним цивільним контролем і за функціональним призначенням спрямована на захист національних інтересів України від загроз [57].

Принципово важливим є законодавче закріплення комплексного підходу до національної безпеки, що охоплює воєнну, зовнішньополітичну, державну, економічну, інформаційну, екологічну безпеку та кібербезпеку. Така широка концептуалізація відповідає природі гібридних загроз, які діють одночасно в різних сферах. Закон також встановлює механізми демократичного цивільного контролю, що є критично важливим для збереження демократичного характеру держави в умовах безпекових викликів.

Стратегічне планування у сфері національної безпеки регулюється системою документів, на чолі якої стоїть Стратегія національної безпеки України. Остання редакція Стратегії відображає еволюцію розуміння безпекових викликів та пріоритетів. Документ чітко ідентифікує Російську Федерацію як джерело актуальних загроз та довгострокових викликів для України, визначає стримування збройної агресії з боку РФ як пріоритет національної безпеки [63]. Стратегія також акцентує увагу на необхідності зміцнення стійкості держави та суспільства, що відповідає концепції resilience в протидії гібридним загрозам.

Воєнна доктрина України, затверджена в умовах вже розгорнутої агресії, стала першим стратегічним документом, що врахував реалії гібридної війни. Доктрина визначає тимчасову окупацію Російською Федерацією території Автономної Республіки Крим та міста Севастополя, розпалювання збройного конфлікту в східних регіонах України як воєнну агресію проти України. Документ також вводить поняття «воєнний конфлікт гібридного характеру», визнаючи нетрадиційний характер загроз.

Законодавство про оборону включає Закон України «Про оборону України», який визначає основи оборони держави, повноваження органів державної влади, основні функції та завдання органів військового управління,

місцевих державних адміністрацій, органів місцевого самоврядування, обов'язки підприємств, установ, організацій, посадових осіб та громадян у сфері оборони. Важливою новацією стало запровадження територіальної оборони як системи загальнодержавних і воєнних заходів, що здійснюються в особливий період, спрямованих на протидію диверсійним проявам та діям незаконних збройних формувань, що особливо актуально в контексті гібридних загроз [58].

Розвідувальна діяльність регулюється Законом України «Про розвідку», який став важливим кроком в інституціалізації розвідувальної спільноти. Закон визначає правові засади організації та діяльності розвідувальних органів України, встановлює механізми координації їх діяльності, регламентує парламентський контроль. Принципово важливим є визнання кіберрозвідки як окремого виду розвідувальної діяльності, що відповідає реаліям сучасного безпекового середовища.

Контррозвідувальна діяльність та боротьба з тероризмом регулюються відповідними законами, які адаптуються до нових викликів. Закон України «Про контррозвідувальну діяльність» визначає правові основи організації та діяльності контррозвідки. Закон України «Про боротьбу з тероризмом» встановлює правові та організаційні основи боротьби з цим явищем. Проте ці закони потребують оновлення з урахуванням того, що в умовах гібридної війни межі між розвідувальною діяльністю противника, терористичними актами та диверсійною діяльністю стають розмитими.

Правовий режим воєнного стану регулюється Законом України «Про правовий режим воєнного стану», який був суттєво оновлений після початку російської агресії. Закон визначає зміст правового режиму воєнного стану, порядок його введення та скасування, правові засади діяльності органів державної влади, військового командування, військових адміністрацій, органів місцевого самоврядування, підприємств, установ та організацій в умовах воєнного стану, гарантії прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб [61].

Особливого значення в контексті гібридної війни набуває законодавство про санкції. Закон України «Про санкції» від 2014 року став відповіддю на необхідність використання економічних та інших обмежувальних заходів як інструменту захисту національних інтересів. Закон визначає правові підстави, порядок застосування, види та порядок скасування санкцій. Практика застосування санкцій показала їх ефективність як інструменту протидії гібридним загрозам, хоча й виявила необхідність вдосконалення механізмів моніторингу їх дотримання.

Інформаційна безпека як критично важливий компонент протидії гібридним загрозам поки що не має комплексного законодавчого регулювання. Окремі аспекти регулюються різними законами, зокрема законами про інформацію, про телебачення і радіомовлення, про друковані засоби масової інформації. Доктрина інформаційної безпеки України, затверджена у 2017 році, визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Проте відсутність базового закону про інформаційну безпеку створює правові лакуни в регулюванні цієї сфери.

Кібербезпека регулюється Законом України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. Закон встановлює основні принципи забезпечення кібербезпеки, визначає об’єкти кібербезпеки та кіберзахисту, суб’єктів забезпечення кібербезпеки, їх основні завдання та функції. Стратегія кібербезпеки України деталізує пріоритети та напрями забезпечення кібербезпеки [59].

Правове регулювання державної таємниці та службової інформації здійснюється Законом України «Про державну таємницю», який визначає правові засади віднесення інформації до державної таємниці, засекречування, розсекречування її матеріальних носіїв, охорони державної таємниці з метою

захисту національної безпеки України. В умовах гібридної війни, коли інформація стає зброєю, питання захисту чутливої інформації набуває особливої актуальності.

Міжнародно-правові аспекти забезпечення національної безпеки регулюються через імплементацію міжнародних договорів України. Особливе значення мають договори про дружбу, співробітництво та партнерство, угоди про військово-технічне співробітництво, договори в рамках участі України в міжнародних безпекових організаціях. Важливим є також застосування норм міжнародного гуманітарного права в умовах збройного конфлікту.

Узагальнена нормативно-правова база з проблематики дослідження наведена у таблиці 2.1.

Таблиця 2.1

Динаміка розвитку нормативно-правової бази управління національною безпекою України (2014-2024)

Рік прийняття	**Нормативно-правовий акт**	**Основні положення**	**Значення для протидії гібридним загрозам**
2014	Закон України «Про санкції»	Визначає правові підстави, порядок застосування, види та порядок скасування спеціальних економічних та інших обмежувальних заходів	Створення правової основи для економічної протидії агресії
2015	Воєнна доктрина України	Визначає тимчасову окупацію РФ території АР Крим та збройний конфлікт на сході як воєнну агресію; вводить поняття «гібридний конфлікт»	Перше офіційне визнання гібридного характеру загроз
2017	Закон України «Про основні засади забезпечення кібербезпеки України»	Визначає правові та організаційні основи захисту життєво важливих інтересів у кіберпросторі, об’єкти та суб’єкти кібербезпеки	Формування правових основ протидії кіберзагрозам як компоненту гібридної війни

Продовження табл. 2.1

Рік прийняття	Нормативно-правовий акт	Основні положення	Значення для протидії гібридним загрозам
2017	Доктрина інформаційної безпеки України	Визначає національні інтереси в інформаційній сфері, загрози та пріоритети державної політики у протидії інформаційній агресії	Концептуальна основа протидії інформаційній складовій гібридної агресії
2018	Закон України «Про національну безпеку України»	Визначає систему органів сектору безпеки і оборони, принципи їх діяльності, механізми демократичного цивільного контролю	Комплексна реформа правових засад національної безпеки з урахуванням досвіду протидії гібридній агресії
2020	Закон України «Про розвідку»	Визначає правові засади організації розвідувальної діяльності, механізми координації розвідувальних органів, парламентський контроль	Інституціоналізація розвідувальної спільноти для ефективної протидії гібридним загрозам
2020	Стратегія національної безпеки України	Визначає РФ як джерело загроз, встановлює пріоритети у воєнній, економічній, інформаційній, екологічній безпеці та кібербезпеці	Стратегічне бачення протидії комплексним гібридним загрозам
2020	Стратегія кібербезпеки України	Деталізує пріоритети забезпечення кібербезпеки, визначає завдання суб'єктів та механізми реалізації	Операціоналізація протидії кіберскладовій гібридних загроз
2021	Закон України «Про правовий режим воєнного стану» (оновлений)	Визначає повноваження органів влади, обмеження прав та свобод, особливості функціонування економіки в умовах воєнного стану	Правове забезпечення функціонування держави в умовах повномасштабної агресії
2021	Закон України «Про корінні народи України»	Визначає гарантії прав кримських татар, караїмів, кримчаків в умовах тимчасової окупації	Протидія спробам асиміляції та використання етнічного чинника для дестабілізації

Закінчення табл. 2.1

Рік прийняття	Нормативно-правовий акт	Основні положення	Значення для протидії гібридним загрозам
2022	Закон України «Про медіа»	Регулює діяльність медіа, встановлює вимоги до контенту, механізми протидії дезінформації	Посилення правових механізмів протидії інформаційним операціям
2023	Закон України «Про основні засади державної політики у сфері стратегічних комунікацій»	Визначає правові засади координації інформаційної діяльності держави, механізми стратегічних комунікацій	Інституціоналізація системи стратегічних комунікацій як відповіді на інформаційну агресію
2024	Закон України «Про мобілізаційну підготовку та мобілізацію» (оновлений)	Удосконалює механізми мобілізації, ведення військового обліку, бронювання працівників критичних підприємств	Адаптація мобілізаційної системи до реалій затяжної гібридної війни

Отже, аналіз нормативно-правової бази виявляє як значний прогрес в адаптації законодавства до викликів гібридної війни, так і проблемні зони. До досягнень можна віднести оновлення базового законодавства з урахуванням досвіду протидії агресії, розширення концепції національної безпеки, запровадження нових правових інструментів. Водночас залишаються прогалини в регулюванні інформаційної безпеки, протидії гібридним загрозам, координації діяльності різних суб’єктів, що потребує подальшого вдосконалення правової бази.

Організаційна структура суб’єктів забезпечення національної безпеки України являє собою складну багаторівневу систему державних органів, військових формувань та спеціальних служб, яка в умовах гібридної війни зазнала суттєвої трансформації, спрямованої на підвищення ефективності протидії комплексним загрозам. Аналіз цієї структури дозволяє оцінити інституційну спроможність держави реагувати на виклики гібридної агресії та виявити напрями необхідних організаційних змін (рис. 2.1).

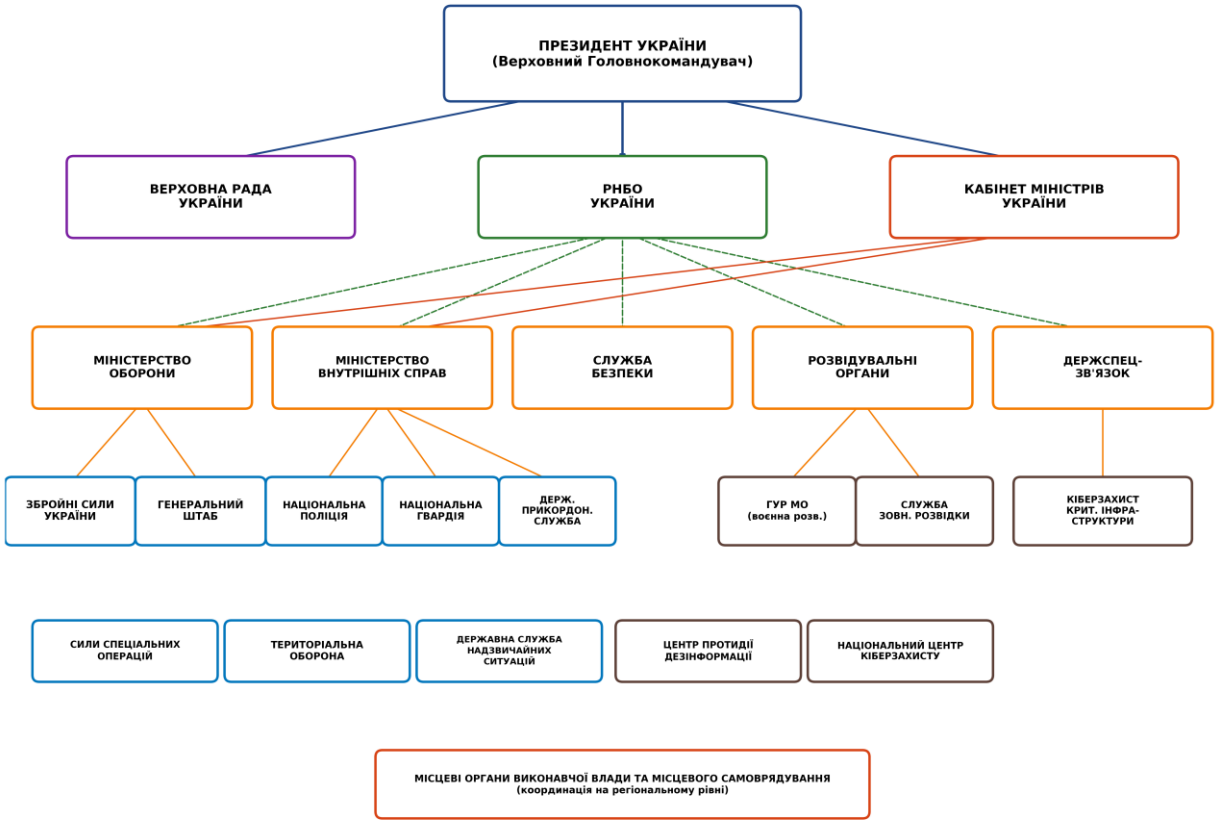

Рис. 2.1. Організаційна структура сектору безпеки і оборони України

На вершині організаційної піраміди системи національної безпеки перебуває Президент України, який відповідно до Конституції є Верховним Головнокомандувачем Збройних Сил України та головою Ради національної безпеки і оборони України. В умовах гібридної війни роль Президента як координатора всієї системи національної безпеки суттєво зросла. Офіс Президента України через відповідні структурні підрозділи забезпечує аналітичну підтримку прийняття рішень у безпековій сфері, координацію діяльності різних відомств, стратегічні комунікації.

Рада національної безпеки і оборони України функціонує як координаційний орган з питань національної безпеки і оборони при Президентові України. В умовах гібридної агресії РНБО перетворилася з дорадчого органу на ключову інституцію оперативного реагування на

безпекові виклики. Розширення функцій РНБО включає координацію діяльності органів виконавчої влади у сфері національної безпеки, здійснення контролю за виконанням рішень з питань національної безпеки, введення санкцій. Апарат РНБО забезпечує організаційне, інформаційно-аналітичне та матеріально-технічне забезпечення діяльності Ради, що включає функціонування ситуаційних центрів, проведення комплексного аналізу загроз, підготовку проектів рішень.

Верховна Рада України як єдиний орган законодавчої влади відіграє критичну роль у формуванні правових основ національної безпеки. Комітет Верховної Ради України з питань національної безпеки, оборони та розвідки є ключовим парламентським органом, що забезпечує законодавче супроводження безпекової політики, здійснює парламентський контроль за діяльністю органів сектору безпеки і оборони. В умовах гібридної війни особливого значення набула здатність парламенту оперативно приймати необхідні закони для протидії новим загрозам.

Кабінет Міністрів України як вищий орган у системі органів виконавчої влади забезпечує реалізацію державної політики у сфері національної безпеки. Урядовий комітет з питань оборони, правоохоронної діяльності, боротьби з корупцією та забезпечення національної безпеки координує діяльність міністерств та відомств у безпековій сфері. В умовах гібридної війни зросла роль економічного блоку уряду в забезпеченні економічної безпеки, протидії економічним загрозам, забезпеченні функціонування економіки в умовах конфлікту.

Міністерство оборони України є центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва. В умовах гібридної війни Міноборони трансформувалося з органу адміністративного управління в ефективну структуру стратегічного планування та забезпечення обороноздатності. Реформування міністерства включало запровадження стандартів НАТО, розмежування функцій

формування політики (міністерство) та військового управління (Генеральний штаб), розвиток спроможностей оборонного планування.

Генеральний штаб Збройних Сил України є головним органом військового управління, що відповідає за оборонне планування, стратегічне керівництво Збройними Силами. В умовах гібридної війни Генштаб адаптував свою структуру для ефективного управління військами в умовах конфлікту, що включає функціонування об'єднаного оперативного штабу, координацію з іншими військовими формуваннями, планування операцій в умовах гібридних загроз. Створення окремих командувань видів збройних сил, а також командувань за функціональним призначенням (Сили спеціальних операцій, Десантно-штурмові війська) підвищило гнучкість військового управління.

Міністерство внутрішніх справ України відповідає за формування державної політики у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку. В контексті гібридної війни МВС відіграє критичну роль у забезпеченні внутрішньої стабільності, протидії диверсійно-розвідувальним групам, підтримці режиму воєнного стану. Національна поліція, Національна гвардія, Державна прикордонна служба, Державна служба з надзвичайних ситуацій функціонують як складові системи МВС, кожна з власними специфічними завданнями в умовах гібридних загроз [16].

Служба безпеки України як державний орган спеціального призначення з правоохоронними функціями забезпечує державну безпеку України. В умовах гібридної війни СБУ стала ключовою структурою протидії широкому спектру загроз – від традиційної контррозвідувальної діяльності до протидії тероризму, кіберзагрозам, економічній та інформаційній агресії. Реформування СБУ спрямоване на трансформацію з пострадянської спецслужби в сучасну службу безпеки європейського типу, що включає демілітаризацію, зосередження на контррозвідувальних функціях, посилення аналітичних спроможностей.

Розвідувальні органи України включають Головне управління розвідки

Міністерства оборони України (воєнна розвідка) та Службу зовнішньої розвідки України. ГУР МО відповідає за ведення воєнної, воєнно-технічної, воєнно-економічної розвідки, здійснення спеціальних заходів, спрямованих на підтримку національних інтересів і державної політики України у воєнно-політичній, воєнно-технічній, воєнно-економічній, інформаційній та екологічній сферах. СЗР здійснює розвідувальну діяльність у політичній, економічній, науково-технічній, інформаційній та екологічній сферах. Координація діяльності розвідувальних органів здійснюється через розвідувальний комітет при Президентові України [65].

Державна служба спеціального зв'язку та захисту інформації України забезпечує функціонування урядового зв'язку, захист державних інформаційних ресурсів та інформації, кіберзахист критичної інфраструктури. В умовах гібридної війни, де кібератаки стали повсякденною реальністю, роль Держспецзв'язку критично зросла. Створення окремих підрозділів кіберзахисту, CERT-UA, розвиток національної телекомунікаційної мережі спеціального призначення стали важливими кроками в інституційному розвитку.

Національний банк України, хоча формально не входить до сектору безпеки і оборони, відіграє важливу роль у забезпеченні економічної безпеки держави. В умовах гібридної війни НБУ протидіє спробам дестабілізації фінансової системи, забезпечує стабільність національної валюти, здійснює моніторинг фінансових потоків для виявлення підозрілих операцій. Координація НБУ з безпековими структурами в питаннях протидії фінансуванню тероризму та відмиванню коштів стала важливим елементом системи національної безпеки.

Місцеві державні адміністрації та органи місцевого самоврядування в умовах гібридної війни набули нових безпекових функцій. Обласні та районні державні адміністрації відповідають за організацію територіальної оборони, забезпечення мобілізаційних заходів, координацію дій в умовах надзвичайних ситуацій. Створення обласних координаційних штабів з питань безпеки,

розвиток місцевих підрозділів територіальної оборони, налагодження взаємодії з військовими адміністраціями стали важливими елементами децентралізованої системи забезпечення безпеки.

Особливе місце в організаційній структурі займають новостворені інституції, що виникли як відповідь на специфічні виклики гібридної війни. Міністерство з питань реінтеграції тимчасово окупованих територій координує державну політику щодо тимчасово окупованих територій, забезпечує захист прав громадян України, які проживають на цих територіях. Державний центр кіберзахисту забезпечує координацію діяльності суб'єктів сектору безпеки і оборони у сфері кібербезпеки. Центр протидії дезінформації при РНБО координує зусилля з протидії інформаційним загрозам.

Аналіз організаційної структури виявляє як значні досягнення в інституційному розвитку, так і проблемні аспекти. До позитивних змін належать: створення нових структур для протидії гібридним загрозам, посилення координаційних механізмів, адаптація традиційних безпекових органів до нових викликів. Водночас залишаються виклики: дублювання функцій між різними відомствами, недостатня горизонтальна координація, інерція організаційних структур, брак кваліфікованих кадрів для роботи з новими типами загроз. Подальший розвиток організаційної структури має бути спрямований на підвищення гнучкості, посилення міжвідомчої взаємодії, розвиток мережевих форм організації, що відповідають природі гібридних викликів.

Критично важливий аспект інституційної архітектури системи національної безпеки України становить функціональний розподіл повноважень у сфері безпекового управління, визначаючи ефективність протидії гібридним загрозам через чіткість компетенцій, уникнення дублювання функцій та забезпечення синергії зусиль різних суб'єктів. В умовах гібридної війни традиційні функціональні межі між різними відомствами розмиваються, що вимагає переосмислення класичних підходів до розподілу повноважень.

Президент України як глава держави, гарант державного суверенітету та територіальної цілісності наділений широкими повноваженнями у сфері національної безпеки. Його функції включають здійснення керівництва у сферах національної безпеки та оборони держави, очолювання Ради національної безпеки і оборони, здійснення верховного головнокомандування Збройними Силами, прийняття рішення про загальну або часткову мобілізацію та введення воєнного стану, внесення до Верховної Ради подання про оголошення стану війни [62]. В умовах гібридної агресії особливого значення набули повноваження Президента щодо застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій), координації діяльності всіх органів державної влади у сфері національної безпеки.

Рада національної безпеки і оборони України виконує координаційні та контрольні функції, що включають координацію діяльності органів виконавчої влади з питань національної безпеки і оборони, внесення пропозицій Президенту щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони, координацію та контроль діяльності органів виконавчої влади з відбиття збройної агресії, організації захисту населення та забезпечення його життєдіяльності, охорони життя, здоров’я, конституційних прав і свобод громадян. Важливою функцією РНБО стала координація розвідувальної, контррозвідувальної та оперативно-розшукової діяльності, заходів політичного, соціально-економічного, інформаційного, кібернетичного характеру.

Верховна Рада України реалізує законодавчі функції у сфері національної безпеки, що охоплюють визначення засад внутрішньої і зовнішньої політики, основ національної безпеки, затвердження загальнодержавних програм, схвалення рішення про надання військової допомоги іншим державам, про направлення підрозділів Збройних Сил України до іншої держави чи про допуск підрозділів збройних сил інших держав на територію України. Контрольна функція парламенту реалізується

через затвердження державного бюджету та контроль за його виконанням у частині видатків на національну безпеку, заслуховування звітів про діяльність органів сектору безпеки і оборони, проведення парламентських розслідувань.

Кабінет Міністрів України здійснює виконавчі функції щодо забезпечення державного суверенітету та економічної безпеки України, здійснення заходів щодо забезпечення обороноздатності України, організації розробки та виконання загальнодержавних програм у сфері національної безпеки. Уряд забезпечує фінансування потреб національної безпеки в межах бюджетних призначень, координує діяльність міністерств та інших центральних органів виконавчої влади з виконання завдань у сфері національної безпеки, організовує матеріально-технічне забезпечення сил безпеки і оборони [56].

Міністерство оборони України виконує функції з формування та реалізації державної політики з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва. Ключові функції включають організаційне забезпечення застосування Збройних Сил, здійснення в межах повноважень міжнародного співробітництва, забезпечення розвитку озброєння та військової техніки, здійснення державних закупівель товарів, робіт і послуг оборонного призначення. В умовах гібридної війни до функцій Міноборони додалися координація заходів територіальної оборони, участь у забезпеченні кібербезпеки критичної інфраструктури оборонного комплексу, стратегічні комунікації у воєнній сфері.

Генеральний штаб Збройних Сил України відповідає за планування застосування та безпосереднє військове управління Збройними Силами. Його функції охоплюють стратегічне та оперативне планування застосування Збройних Сил, організацію та проведення заходів оперативної, бойової та мобілізаційної підготовки, розвідувальну діяльність в інтересах оборони, організацію зв’язку та управління військами, координацію діяльності державних органів та органів місцевого самоврядування щодо виконання завдань оборони.

Міністерство внутрішніх справ реалізує функції забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку. В умовах гібридної війни функціональне навантаження МВС значно розширилося, включаючи забезпечення режиму воєнного стану, охорону критичної інфраструктури, протидію диверсійно-розвідувальним групам, участь у територіальній обороні через підрозділи Національної гвардії, контроль за дотриманням прикордонного режиму через Державну прикордонну службу, забезпечення кібербезпеки об'єктів критичної інфраструктури.

Служба безпеки України виконує широкий спектр функцій у сфері державної безпеки: контррозвідувальну діяльність, боротьбу з тероризмом, контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки. В умовах гібридної війни особливого значення набули функції протидії спеціальним інформаційним операціям, спрямованим проти України, виявлення та припинення діяльності незаконних збройних формувань, організованих злочинних угруповань, що становлять загрозу державній безпеці [66].

Розвідувальні органи виконують специфічні функції здобування, аналітичної обробки та надання визначеним законом споживачам розвідувальної інформації. Головне управління розвідки МО спеціалізується на воєнній, воєнно-політичній, воєнно-технічній, воєнно-економічній, інформаційній, екологічній розвідці, здійсненні спеціальних операцій. Служба зовнішньої розвідки фокусується на політичній, економічній, науково-технічній, інформаційній розвідці. Функціональний розподіл між розвідувальними органами базується на сферах відповідальності, проте в умовах гібридних загроз зростає необхідність інтеграції розвідувальних зусиль.

Державна служба спеціального зв'язку та захисту інформації України виконує функції забезпечення функціонування урядового зв'язку, формування

та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом. В умовах гібридної війни критично важливими стали функції забезпечення кіберзахисту об’єктів критичної інфраструктури, координації діяльності з реагування на кіберінциденти, проведення аудиту інформаційної безпеки.

Центральні органи виконавчої влади поза сектором безпеки і оборони також мають важливі безпекові функції. Міністерство закордонних справ забезпечує дипломатичний вимір протидії гібридним загрозам через формування міжнародної коаліції підтримки України, просування національних інтересів на міжнародній арені, консульський захист громадян. Міністерство економіки відповідає за економічну безпеку, координацію санкційної політики, захист стратегічних галузей економіки. Міністерство енергетики забезпечує енергетичну безпеку в умовах гібридних атак на енергетичну інфраструктуру.

Місцеві органи виконавчої влади та органи місцевого самоврядування в умовах децентралізації отримали розширені функції у сфері безпеки. Обласні державні адміністрації координують територіальну оборону, забезпечують мобілізаційні заходи, організовують цивільний захист населення. Органи місцевого самоврядування відповідають за функціонування місцевих систем оповіщення, створення умов для розміщення військових підрозділів, участь у заходах територіальної оборони.

Слід зазначити, що проблемним аспектом функціонального розподілу залишається наявність «сірих зон» компетенції, особливо у сферах протидії гібридним загрозам, які не вписуються в традиційні функціональні межі. Інформаційна безпека, протидія дезінформації, захист критичної інфраструктури, протидія економічній агресії часто потребують спільних зусиль кількох відомств, що створює виклики координації та відповідальності. Механізми міжвідомчої взаємодії, хоча й розвиваються, ще не повною мірою відповідають динаміці та складності гібридних загроз.

Але поряд з цим еволюція функціонального розподілу в умовах гібридної війни демонструє тенденцію до більшої інтеграції та гнучкості. Створення міжвідомчих координаційних органів, запровадження механізмів спільного планування, розвиток горизонтальних зв'язків між відомствами стають необхідними умовами ефективної протидії комплексним загрозам. Водночас важливо зберегти баланс між інтеграцією зусиль та збереженням спеціалізації, між гнучкістю реагування та чіткістю відповідальності, між централізацією координації та децентралізацією виконання.

Через це проблеми координації та взаємодії безпекових інституцій України в умовах гібридної війни являють собою один з найбільш критичних викликів для ефективного функціонування системи національної безпеки. Складність та багатовимірність гібридних загроз вимагають синхронізованих дій різних відомств, проте інституційна спадщина, відомчі інтереси та організаційні бар'єри часто перешкоджають досягненню необхідного рівня координації.

Структурні проблеми координації коріняться в історично сформованій фрагментації безпекового сектору, де кожне відомство розвивалося як відносно автономна структура з власною культурою, процедурами та пріоритетами. Пострадянська модель жорсткого відомчого розмежування, посилена взаємною недовірою між силовими структурами, створила інституційні «силоси», що ускладнюють горизонтальну взаємодію. Навіть в умовах війни, коли необхідність координації є очевидною, відомчі бар'єри продовжують впливати на ефективність спільних дій.

Найгостріше проблема координації проявляється у сфері обміну інформацією між безпековими структурами. Кожне відомство має власні інформаційні системи, бази даних, канали отримання розвідувальної інформації, які часто є несумісними та закритими для інших структур. СБУ, військова розвідка, Національна поліція, прикордонна служба можуть володіти фрагментами критично важливої інформації про гібридні загрози, але відсутність ефективних механізмів обміну не дозволяє скласти цілісну

картину. Проблема ускладнюється різними рівнями секретності, відомчими інструкціями щодо обмеження доступу, технічною несумісністю інформаційних систем.

Конкуренція за ресурси та вплив між безпековими відомствами створює додаткові перешкоди для координації. В умовах обмежених бюджетних ресурсів кожна структура прагне максимізувати власну частку фінансування, що може призводити до дублювання функцій та створення паралельних структур. Наприклад, кілька відомств можуть розвивати власні підрозділи кіберзахисту або аналітичні центри, замість створення єдиної потужної структури. Боротьба за політичний вплив та доступ до вищого керівництва держави також підриває готовність до рівноправної співпраці [45].

Правові та процедурні проблеми координації пов’язані з недостатньою чіткістю розмежування повноважень в зонах перетину компетенцій різних відомств. Протидія гібридним загрозам часто вимагає дій на стику повноважень – наприклад, кібератака на критичну інфраструктуру може одночасно бути предметом відання СБУ (державна безпека), Держспецзв’язку (кіберзахист), Національної поліції (кіберзлочинність), власника інфраструктури (корпоративна безпека). Відсутність чітких протоколів взаємодії призводить до затримок, конфліктів компетенції або, навпаки, ситуацій, коли жодне відомство не бере на себе відповідальність.

Проблеми оперативної координації найяскравіше проявляються під час кризових ситуацій, коли необхідна швидка синхронізація дій різних структур. Досвід показує, що навіть за наявності формальних координаційних механізмів, таких як оперативні штаби чи координаційні центри, реальна взаємодія часто буксує через відсутність відпрацьованих процедур, неготовність до роботи в єдиному інформаційному просторі, різні темпи прийняття рішень у різних відомствах. Кожна структура схильна діяти за власними алгоритмами, що призводить до неузгодженості дій.

Міжвідомча координація у сфері стратегічного планування також стикається з серйозними викликами. Хоча формально існує система

документів стратегічного планування у сфері національної безпеки, на практиці кожне відомство розробляє власні стратегії та плани, які не завжди узгоджуються між собою. Відсутність єдиної методології оцінки загроз призводить до того, що різні структури можуть мати різне бачення пріоритетів та шляхів їх досягнення. Слабкість механізмів моніторингу виконання стратегічних документів не дозволяє своєчасно виявляти та усувати неузгодженості.

Технологічні аспекти проблем координації пов'язані з відсутністю єдиної інформаційно-телекомунікаційної платформи для безпекового сектору. Різні відомства використовують різні системи зв'язку, різне програмне забезпечення, різні стандарти обробки даних. Спроби створення інтегрованих систем часто наштовхуються на технічні складнощі, брак фінансування, опір змінам. Навіть успішні проекти, такі як система «Дельта» для ситуаційної обізнаності, не охоплюють всіх учасників безпекового сектору та не забезпечують повної інтеграції.

Культурно-психологічні бар'єри координації часто виявляються найбільш стійкими. Кожна безпекова структура має власну організаційну культуру, традиції, неформальні норми поведінки, які формувалися десятиліттями. Військові, співробітники спецслужб, поліцейські, прикордонники мають різне професійне світосприйняття, різні підходи до оцінки ризиків, різні стилі комунікації. Взаємна недовіра, стереотипи, професійна замкненість створюють невидимі, але потужні перешкоди для ефективної співпраці.

Проблема «відомчого его» проявляється в небажанні визнавати власні помилки, ділитися успіхами, приймати допомогу від інших структур. Кожне відомство прагне продемонструвати власну ефективність та незамінність, що може призводити до приховування проблем, перебільшення власних досягнень, применшення внеску партнерів. В умовах публічної уваги до безпекових питань це створює додатковий тиск на керівництво відомств демонструвати результати, навіть якщо це йде на шкоду загальній справі.

Координація з недержавними акторами – волонтерськими організаціями, приватними охоронними компаніями, бізнес-структурами – представляє окремий виклик. В умовах гібридної війни ці актори часто відіграють важливу роль у забезпеченні безпеки, але механізми їх залучення та координації залишаються недостатньо розвиненими. Правові обмеження, брак довіри, відсутність налагоджених каналів комунікації ускладнюють використання потенціалу громадянського суспільства та приватного сектору.

Міжнародний вимір координації також містить проблемні аспекти. Взаємодія з іноземними партнерами у безпековій сфері вимагає узгодження не лише між українськими відомствами, а й з процедурами та вимогами міжнародних партнерів. Різні країни можуть надавати допомогу різним українським структурам, що без належної координації може призводити до дублювання або, навпаки, прогалин у підтримці. Мовні бар'єри, різниця в стандартах та процедурах додатково ускладнюють координацію [155].

Спроби вирішення проблем координації через створення нових координаційних органів часто призводять до ще більшого ускладнення системи управління. Численні координаційні ради, комітети, робочі групи можуть створювати ілюзію координації, але насправді лише додавати нові бюрократичні ланки. Без зміни базових принципів взаємодії, створення довіри між відомствами, впровадження ефективних механізмів обміну інформацією формальні координаційні структури залишаються малоефективними.

Вплив проблем координації на ефективність протидії гібридним загрозам є критичним. Затримки в обміні інформацією можуть дозволити ворожим агентам уникнути викриття. Неузгодженість дій різних структур створює вразливості, які експлуатуються противником. Дублювання зусиль призводить до неефективного використання обмежених ресурсів. Конфлікти між відомствами підривають довіру суспільства до безпекових інституцій. В умовах, коли противник діє скоординовано та цілеспрямовано, відсутність ефективної координації на боці України стає стратегічною вразливістю.

Ресурсне забезпечення інституцій національної безпеки України в

умовах гібридної війни становить ще один критичний фактор їх спроможності ефективно виконувати покладені функції та протидіяти комплексним загрозам. Аналіз стану ресурсного забезпечення дозволяє оцінити реальну готовність безпекових інституцій до виконання завдань, виявити диспропорції та обґрунтувати пріоритети розподілу обмежених ресурсів в умовах триваючої агресії.

Фінансове забезпечення сектору безпеки і оборони зазнало радикальної трансформації після початку російської агресії. Якщо у 2013 році видатки на оборону становили лише 1% ВВП, що було одним з найнижчих показників у Європі, то вже у 2015 році вони зросли до 2,5% ВВП, а в наступні роки стабілізувалися на рівні 5-6% ВВП [208]. Загальні видатки на сектор безпеки і оборони, включаючи Міністерство оборони, Міністерство внутрішніх справ, Службу безпеки, розвідувальні органи та інші структури, у 2023 році перевищили 1,7 трильйона гривень, що становило понад 40% видатків державного бюджету.

Структура фінансового забезпечення відображає пріоритети протидії гібридним загрозам. Найбільша частка припадає на Міністерство оборони та Збройні Сили – близько 70% загальних видатків на сектор безпеки. Це включає утримання особового складу, закупівлю озброєння та військової техніки, проведення бойової підготовки, розвиток військової інфраструктури. Міністерство внутрішніх справ отримує близько 15% коштів, що спрямовуються на утримання Національної поліції, Національної гвардії, Державної прикордонної служби. Решта розподіляється між СБУ, розвідувальними органами, Державною службою спеціального зв’язку та іншими структурами.

Проблемою залишається недостатнє фінансування капітальних видатків порівняно з поточними. Основна частина бюджету йде на утримання особового складу – виплату грошового забезпечення, харчування, речове забезпечення. На закупівлю нового озброєння, модернізацію техніки, розвиток інфраструктури часто залишається недостатньо коштів, що стримує

модернізацію сил безпеки і оборони. Особливо гостро стоїть питання фінансування науково-дослідних та дослідно-конструкторських робіт у сфері оборони, що критично важливо для розробки власних систем озброєння [5].

Кадрове забезпечення безпекових інституцій характеризується як кількісними, так і якісними викликами. Так, загальна чисельність особового складу сектору безпеки і оборони після 2014 року суттєво зросла. Водночас кількісне зростання не завжди супроводжувалося відповідним якісним розвитком кадрового потенціалу, хоча система підготовки кадрів для сектору безпеки і оборони включає мережу військових навчальних закладів, навчальних центрів, курсів підвищення кваліфікації. Національний університет оборони України, Національна академія СБУ, Національна академія Національної гвардії, військові академії видів збройних сил забезпечують підготовку офіцерських кадрів. Проте система військової освіти потребує модернізації відповідно до стандартів НАТО та вимог сучасної війни. Особливо гостро стоїть питання підготовки фахівців з кібербезпеки, інформаційних операцій, стратегічних комунікацій – напрямків, критично важливих для протидії гібридним загрозам [53].

Проблемою кадрового забезпечення є відтік кваліфікованих фахівців до приватного сектору через нижчий рівень оплати праці в державних структурах. Це особливо стосується ІТ-спеціалістів, аналітиків, фахівців з комунікацій. Середня заробітна плата в секторі безпеки, хоча й зросла останніми роками, залишається нижчою за ринкову для висококваліфікованих спеціалістів. Система мотивації та кар’єрного зростання часто базується на застарілих принципах, що не відповідають сучасним вимогам.

Матеріально-технічне забезпечення сектору безпеки і оборони демонструє контрастну картину. З одного боку, відбулося суттєве переоснащення Збройних Сил сучасними зразками озброєння та військової техніки, як вітчизняного виробництва, так і отриманих від міжнародних партнерів. Надходження протитанкових комплексів Javelin та NLAW, систем HIMARS, ППО різних типів якісно підвищило спроможності української

армії. З іншого боку, значна частина техніки та озброєння залишається застарілою, потребує модернізації або заміни.

Розвиток вітчизняного оборонно-промислового комплексу став пріоритетом в умовах війни. Підприємства ДК «Укроборонпром» (нині АТ «Українська оборонна промисловість») нарощують виробництво боєприпасів, бронетехніки, безпілотних літальних апаратів, засобів радіоелектронної боротьби. Проте потенціал ОПК використовується не повною мірою через брак фінансування, застарілу виробничу базу, розрив кооперaційних зв'язків з Росією. Особливо актуальною є проблема виробництва високотехнологічних систем озброєння, де Україна має значну залежність від імпорту.

Інфраструктурне забезпечення безпекових інституцій включає військові містечка, полігони, навчальні центри, системи зв'язку та управління, склади та бази зберігання. Стан військової інфраструктури залишається неоднорідним – поряд з модернізованими об'єктами значна частина інфраструктури перебуває в незадовільному стані. Особливо це стосується казармового фонду, де значна частина будівель потребує капітального ремонту або реконструкції. Розвиток полігонної бази не встигає за потребами бойової підготовки в умовах інтенсивних бойових дій.

Інформаційно-технологічне забезпечення набуває критичного значення в умовах гібридної війни. Розвиток автоматизованих систем управління військами, систем розвідки та спостереження, засобів радіоелектронної боротьби стає пріоритетом. Впровадження системи «Дельта» для ситуаційної обізнаності, розгортання мережі Starlink для забезпечення стійкого зв'язку, створення системи «Дія» для цифрових послуг – приклади успішної цифровізації. Водночас рівень інформатизації різних безпекових структур залишається нерівномірним, часто використовуються несумісні системи, що ускладнює обмін інформацією [89].

Наукове та аналітичне забезпечення безпекових інституцій реалізується через мережу науково-дослідних установ, аналітичних центрів, експертних груп. Національний інститут стратегічних досліджень, Центр воєнно-

стратегічних досліджень НУО України, відомчі науково-дослідні установи проводять дослідження актуальних безпекових проблем. Проте фінансування наукових досліджень залишається недостатнім, бракує механізмів швидкого впровадження наукових розробок у практику, слабкою є координація між різними дослідницькими центрами.

Міжнародна допомога стала важливим джерелом ресурсного забезпечення сектору безпеки і оборони України. Військова допомога від США, країн ЄС, Великої Британії, Канади та інших партнерів включає постачання летального та нелетального озброєння, техніки, боєприпасів, обладнання на десятки мільярдів доларів. Програми навчання українських військових за кордоном, консультативна допомога, обмін розвідувальною інформацією суттєво посилюють спроможності України. Фінансова допомога міжнародних партнерів частково компенсує брак власних ресурсів.

Ефективність використання ресурсів залишається проблемним питанням. Корупційні ризики, хоча й знизилися порівняно з довоєнним періодом, все ще існують в системі оборонних закупівель. Відсутність повноцінної системи оборонного планування на основі спроможностей призводить до неоптимального розподілу ресурсів. Слабка координація між різними відомствами веде до дублювання зусиль та неефективного використання обмежених ресурсів. Недостатній контроль за цільовим використанням коштів створює ризики їх розпорошення.

Перспективи покращення ресурсного забезпечення пов’язані з комплексом заходів: оптимізацією структури видатків з переорієнтацією на капітальні інвестиції та інновації; розвитком механізмів державно-приватного партнерства в оборонній сфері; підвищенням ефективності використання міжнародної допомоги; впровадженням сучасних систем управління ресурсами; боротьбою з корупцією та підвищенням прозорості; розвитком власного оборонно-промислового комплексу. При цьому критично важливим є перехід від ресурсного до спроможнісного підходу в плануванні, коли ресурси розподіляються відповідно до необхідних спроможностей для

протидії конкретним загрозам.

2.2. Оцінювання ефективності механізмів публічного управління національною безпекою в умовах гібридної агресії

Десятирічний період протистояння російській гібридній агресії став безпрецедентним випробуванням для системи національної безпеки України, продемонструвавши як критичні вразливості початкового етапу, так і значну адаптивну спроможність українських інституцій. Аналіз еволюції реагування на гібридні виклики дозволяє виявити ключові уроки, успішні практики та залишкові проблеми в забезпеченні національної стійкості.

Початковий етап гібридної агресії (лютий-квітень 2014 року) виявив системну непідготовленість української держави до нового типу загроз. Анексія Криму продемонструвала фатальні прорахунки в оцінці намірів Росії, відсутність сценарного планування на випадок нетрадиційної агресії, слабкість механізмів раннього попередження. Використання Росією «зелених чоловічків», масована інформаційна кампанія, експлуатація проросійських настроїв частини населення, блокування українських військових частин – усе це застало систему національної безпеки зненацька [74].

Реакція на окупацію Криму характеризувалася розгубленістю, відсутністю чіткого плану дій, суперечливими сигналами від різних органів влади. Спроби дипломатичного врегулювання, звернення до міжнародних організацій, оголошення часткової мобілізації виявилися неефективними в умовах швидкого розвитку подій. Критичними факторами поразки стали: деморалізація особового складу через роки недофінансування та корупції; масове зрадництво серед офіцерського корпусу та співробітників спецслужб; відсутність планів оборони та евакуації; ефективна інформаційно-психологічна операція противника.

Початок агресії на Донбасі (квітень-серпень 2014 року) застав Україну в

стані інституційного хаосу. Захоплення адміністративних будівель озброєними групами, проголошення «ДНР» та «ЛНР», розгортання терористичної діяльності відбувалися на тлі слабкості центральної влади та паралічу силових структур. Перші спроби проведення Антитерористичної операції виявили критичний стан Збройних Сил – брак боєздатних підрозділів, відсутність засобів зв'язку та розвідки, застаріле озброєння, низький моральний дух [2].

Переломним моментом стала громадянська мобілізація – створення добровольчих батальйонів, розгортання волонтерського руху, формування громадської підтримки армії. Феномен добробатів, при всіх його суперечливостях, дозволив заповнити критичний розрив у обороноздатності в найскладніший період. Паралельно почалася інституційна відбудова: відновлення Національної гвардії, початок мобілізації, налагодження системи управління військами, перші кроки з очищення силових структур від зрадників та агентів.

Період активних бойових дій (серпень 2014 – лютий 2015 року) став випробуванням на здатність системи національної безпеки адаптуватися в умовах війни. Трагедії Іловайська та Дебальцевого виявили проблеми військового планування, координації між різними силовими структурами, розвідувального забезпечення. Водночас цей період продемонстрував зростаючу ефективність української армії, здатність до навчання на власних помилках, формування нової генерації командирів з бойовим досвідом.

Важливим аспектом стало усвідомлення комплексного характеру загроз. Поряд з військовими діями Росія вела економічну війну (торговельні обмеження, газовий шантаж), інформаційну агресію (пропаганда через медіа та соцмережі), кібератаки (на енергетичну та фінансову інфраструктуру), дипломатичний тиск. Це вимагало вироблення комплексної відповіді, координації зусиль різних відомств, залучення невійськових інструментів протидії.

Період після Мінських угод (2015-2021 роки) характеризувався

переходом до позиційного протистояння та зосередженням на інституційних реформах. Ключовими напрямками стали: реформа оборонного планування з переходом на стандарти НАТО; створення нових структур (Сили спеціальних операцій, кібервійська); модернізація системи військової освіти; розвиток оборонно-промислового комплексу; посилення розвідувальних спроможностей; реформування СБУ. Водночас цей період виявив небезпеку «заморожування» конфлікту та послаблення уваги до безпекових питань.

Реагування на невійськові аспекти гібридної агресії поступово вдосконалювалося. У сфері енергетичної безпеки вдалося диверсифікувати постачання газу, припинити пряму залежність від Росії, розпочати інтеграцію в європейську енергосистему. В інформаційній сфері були заборонені російські телеканали та соцмережі, створено систему стратегічних комунікацій, розпочато мовлення на окуповані території. У фінансовій сфері запроваджено санкції проти російських банків, посилено контроль за підозрілими операціями.

Кібербезпека стала окремим пріоритетом після масштабних кібератак 2015-2017 років. Атаки на енергетичні компанії, вірус NotPetya, що завдав мільярдних збитків, продемонстрували вразливість критичної інфраструктури. Відповіддю стало створення системи кіберзахисту, включаючи CERT-UA, кіберполіцію, підрозділи кіберзахисту в різних відомствах. Прийняття Стратегії кібербезпеки, налагодження міжнародної співпраці, проведення кібернавчань підвищили стійкість до кібератак [195].

Повномасштабне вторгнення 24 лютого 2022 року стало новим випробуванням, але система національної безпеки продемонструвала якісно інший рівень готовності порівняно з 2014 роком. Ефективне стримування першого удару, збереження системи управління, організована оборона Києва та інших міст, успішні контрнаступальні операції свідчили про успішність проведених реформ. Критичними факторами успіху стали: завчасна підготовка до відсічі агресії на основі розвідувальних даних; високий моральний дух суспільства та армії; ефективна система територіальної

оборони; налагоджена міжнародна підтримка; успішні інформаційні операції.

Адаптація до умов повномасштабної війни продемонструвала сильні та слабкі сторони системи. До успіхів можна віднести: швидку мобілізацію ресурсів; ефективну координацію між різними силовими структурами; інтеграцію нових видів озброєння; розвиток власного виробництва дронів та боєприпасів; стійкість критичної інфраструктури до масованих ударів. Проблемними залишаються: система мобілізації та підготовки резервів; забезпечення війська в умовах затяжної війни; психологічна підтримка військових та цивільного населення; протидія ворожій агентурі [223].

Еволюція інституційного реагування демонструє перехід від реактивної до проактивної моделі. Якщо у 2014 році домінувало ситуативне реагування на вже реалізовані загрози, то до 2024 року сформувалася система превентивних заходів, сценарного планування, підготовки до різних варіантів розвитку подій. Створення Центру протидії дезінформації, Національного центру кіберзахисту, системи стратегічних комунікацій свідчить про інституціоналізацію нових функцій протидії гібридним загрозам.

Роль громадянського суспільства в протидії гібридній агресії виявилася критично важливою. Волонтерський рух, громадські організації, незалежні медіа, ІТ-спільнота стали невід'ємною частиною системи національної стійкості. Феномен «народної війни» проти агресора включає не лише пряму підтримку армії, а й інформаційну протидію, кібератаки на ворожу інфраструктуру, економічний тиск через бойкот російських товарів. Інтеграція громадянського потенціалу в систему національної безпеки стала унікальною особливістю українського досвіду [190].

Міжнародний вимір реагування на гібридну агресію еволюціонував від початкової ізоляції до формування широкої коаліції підтримки. Якщо у 2014 році міжнародна спільнота була шокована та не готова до адекватної відповіді, то до 2024 року сформувався безпрецедентний рівень військової, економічної, гуманітарної підтримки України. Санкції проти Росії, постачання зброї, фінансова допомога, дипломатична ізоляція агресора стали результатом

ефективної української дипломатії та комунікації.

Загальна оцінка десятирічного досвіду протидії гібридній агресії демонструє траєкторію від інституційного колапсу до формування ефективної системи національної стійкості (рис. 2.2).

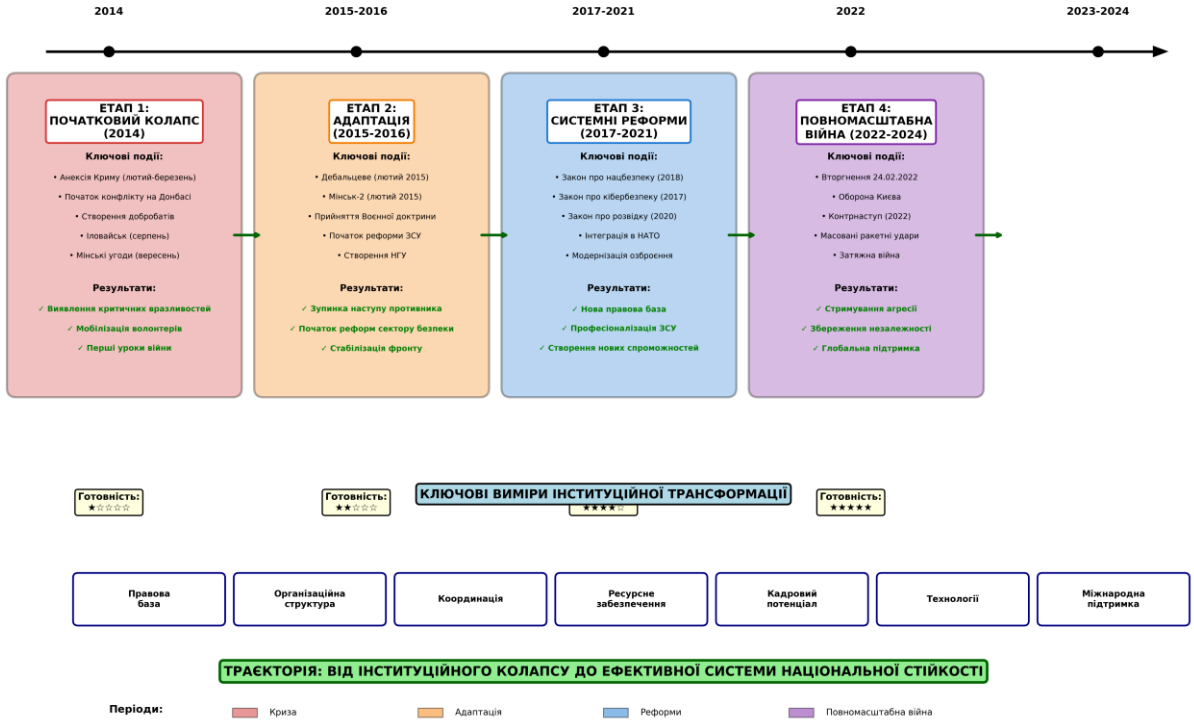

Рис. 2.2. Еволюція реагування України на гібридні загрози (2014-2024): від хаосу до системності

Рисунок 2.2 ілюструє чотири основні етапи трансформації системи національної безпеки України: початковий колапс 2014 року, адаптацію 2015-2016 років, системні реформи 2017-2021 років та період повномасштабної війни 2022-2024 років. Кожен етап характеризується специфічними викликами, інституційними змінами та досягнутими результатами. Динаміка готовності системи зростає від критично низького рівня до високого рівня спроможності протидіяти комплексним гібридним загрозам.

Ключовими факторами успішної адаптації стали: здатність до швидкого навчання та змін; мобілізація суспільного потенціалу; ефективне

використання міжнародної підтримки; розвиток інноваційних підходів; збереження демократичного характеру держави попри безпекові виклики. Зараз вже можна констатувати, що реформування сектору безпеки і оборони України в період 2014-2024 років стало найбільш масштабною та глибокою трансформацією безпекових інституцій в історії незалежної України, що відбувалася в унікальних умовах одночасного ведення бойових дій та системних перетворень. Оцінка результативності цих реформ дозволяє визначити досягнення, виявити недоліки та обґрунтувати напрями подальшого інституційного розвитку в умовах триваючої гібридної війни.

Концептуальною основою реформування стала переорієнтація від пострадянської моделі до євроатлантичних стандартів організації сектору безпеки і оборони. Стратегічний курс на інтеграцію в НАТО, закріплений у Конституції України, визначив вектор трансформації. Ключовими принципами реформ стали: демократичний цивільний контроль над силовими структурами; прозорість та підзвітність; професіоналізація особового складу; сумісність з арміями країн НАТО; орієнтація на спроможності, а не на чисельність. Імплементація цих принципів вимагала не просто організаційних змін, а глибинної трансформації інституційної культури.

Реформа системи управління обороною стала одним з найбільш успішних напрямків трансформації. Розмежування функцій між Міністерством оборони як органом формування політики та Генеральним штабом як органом військового управління відповідає кращим практикам демократичних країн. Міністр оборони став цивільною особою, що посилило демократичний контроль. Запровадження посад заступників міністра з ключових напрямків (євроатлантична інтеграція, цифрова трансформація, стратегічні комунікації) забезпечило професійне управління реформами. Створення Головної інспекції Міністерства оборони як незалежного органу внутрішнього аудиту підвищило прозорість та ефективність використання ресурсів.

Трансформація Збройних Сил України продемонструвала вражаючу

динаміку переходу від деморалізованої армії 2014 року до боєздатної сили, що ефективно протистоїть агресії. Структурні зміни включали перехід від радянської чотирьохвидової до тривидової структури (Сухопутні війська, Повітряні Сили, Військово-Морські Сили), створення нових високомобільних родів військ (Десантно-штурмові війська, Сили спеціальних операцій), формування територіальної оборони як окремої компоненти. Оперативно-тактичний рівень управління був оптимізований через створення оперативних командувань замість громіздких армійських корпусів.

Професіоналізація особового складу стала пріоритетом реформ. Запровадження контрактної служби як основної форми комплектування дозволило підвищити якість особового складу. Якщо у 2014 році контрактники становили менше 20% чисельності ЗСУ, то у 2024 році їх частка перевищила 60%. Грошове забезпечення військовослужбовців зросло в десятки разів, що зробило військову службу конкурентоспроможною на ринку праці. Система кар'єрного зростання була реформована відповідно до принципів меритократії, що дозволило висунути на командні посади офіцерів з бойовим досвідом та лідерськими якостями.

Реформа військової освіти спрямовувалася на підготовку нового покоління офіцерів, здатних діяти в умовах сучасної війни. Впровадження стандартів НАТО в систему військової освіти включало перегляд навчальних програм, розвиток лідерських якостей, вивчення англійської мови, акцент на практичну підготовку. Програма «L-підготовка» для різних рівнів командування стала важливим інструментом трансформації командної культури. Залучення інструкторів з країн НАТО, стажування українських офіцерів за кордоном, участь у міжнародних навчаннях сприяли трансферу кращих практик.

Модернізація озброєння та військової техніки відбувалася в складних умовах розриву кооперaційних зв'язків з Росією та обмежених фінансових ресурсів. Пріоритетом стало відновлення та модернізація наявної техніки, розробка нових зразків озброєння, налагодження виробництва боєприпасів.

Успішними прикладами стали: модернізація танків до рівня Т-64БВ/Т-84; виробництво протитанкових комплексів «Стугна» та «Корсар»; розробка оперативно-тактичного ракетного комплексу «Грім-2»; масове виробництво безпілотних літальних апаратів. Міжнародна військово-технічна допомога якісно посилила спроможності ЗСУ – постачання Javelin, NLAW, HIMARS, артилерійських систем, засобів ППО змінило баланс сил на полі бою [143].

Реформування Національної гвардії України перетворило її з внутрішніх військ радянського зразка на сучасну військову формацію з правоохоронними функціями. НГУ стала важливим компонентом системи територіальної оборони, резервом для ЗСУ, силою реагування на внутрішні загрози. Створення в структурі НГУ спеціальних підрозділів – «Азов», «Kraken», інших – продемонструвало здатність до інновацій та адаптації. Підвищення стандартів підготовки, оснащення сучасною технікою, участь у бойових діях зробили НГУ ефективною бойовою силою.

Трансформація Служби безпеки України виявилася одним з найскладніших напрямків реформ через опір змінам, вкоріненість пострадянських практик, політизацію діяльності. Проте поступово вдалося досягти прогресу: звільнення СБУ від невластивих функцій боротьби з економічними злочинами; демілітаризація та скорочення чисельності; посилення контррозвідувальних та антитерористичних підрозділів; розвиток аналітичних спроможностей; очищення від агентів впливу противника. Ефективність СБУ в протидії ворожій агентурі, розвідувально-диверсійним групам, тероризму значно зросла.

Розбудова розвідувальної спільноти стала критичним фактором успіху в протидії гібридній агресії. Головне управління розвідки Міноборони трансформувалося з другорядної структури в потужну спецслужбу, здатну проводити складні операції в глибокому тилу противника. Успіхи ГУР в отриманні стратегічної інформації, проведенні спеціальних операцій, психологічних кампаній стали важливим фактором стримування агресора. Служба зовнішньої розвідки також підвищила ефективність, забезпечуючи

політичне керівництво важливою інформацією про наміри противника та позиції міжнародних партнерів.

Створення нових інституцій для протидії гібридним загрозам стало важливим елементом реформ. Державний центр кіберзахисту координує зусилля різних відомств у протидії кіберзагрозам. Центр протидії дезінформації став інноваційною структурою для боротьби з інформаційною агресією. Сили територіальної оборони, розгорнуті в усіх регіонах, створили додатковий рівень безпеки. Ці нові інституції заповнили прогалини в системі національної безпеки, які виявила гібридна агресія.

Розвиток оборонно-промислового комплексу в умовах війни продемонстрував як успіхи, так і системні проблеми. Корпоратизація «Укроборонпрому» та створення АТ «Українська оборонна промисловість» мало на меті підвищити ефективність управління державними підприємствами ОПК. Локалізація виробництва боєприпасів, розвиток приватних оборонних компаній, міжнародна кооперація дозволили частково задовольнити потреби фронту. Проте проблеми з фінансуванням, бюрократичні перешкоди, корупційні ризики продовжують стримувати потенціал вітчизняного ОПК.

Фінансове забезпечення реформ стало можливим завдяки безпрецедентному зростанню оборонного бюджету та міжнародній допомозі. Видатки на оборону зросли з 27 млрд грн у 2014 році до понад 1 трлн грн у 2024 році. Програми НАТО з розвитку спроможностей, двостороння допомога від США, Великої Британії, Канади, інших партнерів забезпечили не лише матеріальні ресурси, а й експертну підтримку реформ. Створення траст-фондів НАТО дозволило фінансувати специфічні проекти – від розмінування до кіберзахисту.

Оцінка результативності реформ демонструє значний прогрес у більшості напрямків, хоча темпи та глибина змін є нерівномірними. До безумовних успіхів належать: підвищення боєздатності ЗСУ; створення нових спроможностей; покращення матеріального забезпечення; розвиток партнерства з НАТО; зростання довіри суспільства. Проблемними

залишаються: повільність реформи СБУ; недостатня координація між відомствами; корупційні ризики в оборонних закупівлях; брак кваліфікованих кадрів; опір змінам у частині керівництва. Головним підтвердженням результативності реформ стала здатність України ефективно протистояти повномасштабній агресії, що було б неможливим без проведеної трансформації сектору безпеки і оборони.

При цьому ефективність координаційних механізмів у протидії гібридним загрозам стала одним з визначальних факторів спроможності системи національної безпеки України адекватно реагувати на комплексні виклики, що поєднують військові, політичні, економічні, інформаційні та кіберкомпоненти. Аналіз функціонування цих механізмів протягом десятиліття гібридної війни виявляє еволюцію від початкової фрагментації до поступової інтеграції зусиль, хоча проблеми міжвідомчої координації залишаються одним з найслабших місць системи.

Рада національної безпеки і оборони України як вищий координаційний орган продемонструвала суттєву трансформацію своєї ролі. З дорадчого органу, що епізодично збирався для обговорення безпекових питань, РНБО перетворилася на оперативний центр прийняття стратегічних рішень. Розширення повноважень РНБО, особливо щодо введення санкцій, координації діяльності силових структур, контролю за виконанням рішень, дозволило створити єдиний центр управління безпековою сферою. Регулярність засідань зросла від кількох разів на рік до щотижневих в періоди загострення. Створення робочих груп РНБО з окремих напрямків (кібербезпека, енергетична безпека, протидія дезінформації) забезпечило спеціалізовану координацію.

Механізм ситуаційних центрів став інноваційним інструментом координації в режимі реального часу. Головний ситуаційний центр України при РНБО інтегрує інформацію від різних відомств, забезпечує візуалізацію оперативної обстановки, підтримку прийняття рішень. Мережа відомчих ситуаційних центрів – в Міноборони, МВС, СБУ, інших структурах – дозволяє

здійснювати розподілений моніторинг загроз. Проте проблемою залишається неповна інтеграція інформаційних систем, різні стандарти даних, обмеження доступу через режимні вимоги. Досвід показує, що технологічна інтеграція випереджає організаційну – наявність технічних можливостей не завжди трансформується в ефективну координацію.

Координація розвідувальної діяльності зазнала суттєвого покращення через створення розвідувального комітету при Президентові України та механізмів обміну розвідувальною інформацією. Регулярні наради керівників розвідувальних органів, спільні аналітичні продукти, узгоджене планування операцій підвищили ефективність розвідувальної спільноти. Критичним фактором стало подолання традиційної міжвідомчої конкуренції та недовіри. Створення єдиного банку цілей, механізмів деконфліктації операцій, спільних аналітичних груп дозволило уникнути дублювання та підвищити результативність. Водночас повна інтеграція розвідувальних зусиль ще не досягнута – кожне відомство зберігає власні джерела та методи, не завжди готове ділитися ексклюзивною інформацією [17].

Оперативна координація під час кризових ситуацій продемонструвала як успіхи, так і системні проблеми. Досвід реагування на масовані ракетні удари, кібератаки, диверсії показав здатність системи до швидкої мобілізації в умовах безпосередньої загрози. Створення міжвідомчих оперативних штабів, налагодження прямих каналів зв’язку між керівниками, відпрацювання алгоритмів спільних дій підвищили швидкість реагування. Позитивним прикладом стала координація дій під час відбиття наступу на Київ у 2022 році, коли ЗСУ, НГУ, СБУ, територіальна оборона, місцева влада діяли як єдиний механізм. Проте в менш критичних ситуаціях координація часто буксує через бюрократичні процедури, неузгодженість планів, різну інтерпретацію повноважень.

Координація у сфері кібербезпеки стала тестом на здатність створювати нові механізми для протидії новим загрозам. Національний координаційний центр кібербезпеки при РНБО об’єднує представників ключових відомств –

Держспецзв'язку, СБУ, розвідки, Нацполіції. Система реагування на кіберінциденти CERT-UA забезпечує оперативну координацію технічних заходів. Проведення спільних кібернавчань, розробка єдиних протоколів реагування, обмін інформацією про кіберзагрози підвищили стійкість критичної інфраструктури. Успішне відбиття масованих кібератак свідчить про ефективність координації. Проте проблемою залишається розпорошеність відповідальності – різні відомства відповідають за кіберзахист своїх об'єктів без достатньої координації.

Механізми координації в інформаційній сфері еволюціонували від повного хаосу 2014 року до структурованої системи стратегічних комунікацій. Створення Центру протидії дезінформації, запровадження посад з стратегічних комунікацій в ключових відомствах, розробка єдиних наративів підвищили ефективність інформаційної протидії. Щоденні координаційні наради спікерів, узгоджені інформаційні кампанії, швидке спростування фейків стали важливими елементами. Проте координація ускладнюється різними цільовими аудиторіями відомств, браком єдиної платформи для координації, конкуренцією за медійну увагу. Особливо складною є координація з недержавними акторами – медіа, блогерами, громадськими організаціями, які відіграють важливу роль в інформаційному просторі.

Територіальна координація безпекових зусиль набула критичного значення в умовах бойових дій та загрози поширення конфлікту. Обласні координаційні штаби з питань безпеки та оборони об'єднують представників силових структур, місцевої влади, критичної інфраструктури. Механізми взаємодії військових адміністрацій з цивільною владою забезпечують єдність управління в прифронтових регіонах. Система територіальної оборони створила додатковий рівень координації на місцевому рівні. Позитивним є залучення громадськості через координаційні ради, волонтерські штаби. Проте проблемою залишається різний рівень готовності регіонів, брак досвіду місцевої влади у безпекових питаннях, конфлікти повноважень між військовими та цивільними адміністраціями.

Координація міжнародної допомоги стала окремим напрямком, що вимагав створення специфічних механізмів. Міжнародний центр допомоги Україні координує військову підтримку від десятків країн. Механізми включають регулярні конференції донорів, систему заявок на потреби, логістичну координацію поставок, контроль за використанням. Створення контактної групи з оборони України (формат «Рамштайн») забезпечило стратегічну координацію підтримки. На національному рівні координація здійснюється через спеціальні підрозділи в Міноборони, МВС, інших відомствах. Викликом є узгодження різних процедур країн-донорів, синхронізація поставок з реальними потребами, уникнення дублювання.

Фінансова координація безпекових видатків залишається проблемною зоною попри спроби запровадження програмно-цільового методу. Кожне відомство планує та використовує бюджет автономно, що призводить до неоптимального розподілу ресурсів. Спроби створення єдиного оборонного бюджету, консолідованих закупівель, спільних програм розвитку спроможностей наштовхуються на відомчий опір. Відсутність єдиної системи оборонного планування не дозволяє оптимізувати видатки на основі пріоритетних спроможностей. Позитивним є розвиток механізмів громадського контролю, підвищення прозорості оборонних закупівель через систему ProZorro.

Оцінка ефективності координаційних механізмів на основі практичних результатів демонструє значний прогрес порівняно з 2014 роком, але й виявляє системні обмеження. До успіхів можна віднести: створення постійно діючих координаційних структур; налагодження оперативного обміну інформацією; відпрацювання алгоритмів спільних дій; підвищення рівня довіри між відомствами. Проблемами залишаються: формальний характер частини координаційних механізмів; домінування відомчих інтересів над загальними; брак горизонтальних зв’язків; недостатня інтеграція інформаційних систем; слабкість механізмів контролю за виконанням спільних рішень.

Порівняння з кращими міжнародними практиками показує, що Україна

пройшла значний шлях, але ще не досягла рівня інтегрованого безпекового управління провідних країн НАТО. Концепція comprehensive approach, що передбачає синхронізацію всіх інструментів національної могутності, лише частково імплементована. Відсутність єдиної доктрини міжвідомчої взаємодії, недостатня стандартизація процедур, слабкість механізмів стратегічного планування обмежують ефективність координації.

Вплив координаційних проблем на ефективність протидії гібридним загрозам проявляється в конкретних випадках: затримки в реагуванні на комплексні інциденти; неоптимальне використання ресурсів через дублювання функцій; прогалини в безпековому покритті на стиках відомчих компетенцій; втрата синергетичного ефекту від розрізнених дій. Водночас навіть неідеальна координація виявилася достатньою для стримування агресії, що свідчить про високу мотивацію та адаптивність персоналу безпекових структур, які часто компенсують інституційні недоліки особистою ініціативою.

Ще один критично важливий компонент національної безпеки України, особливо в умовах гібридної війни, де традиційні індикатори загроз часто не спрацьовують, а швидкість розгортання кризових ситуацій вимагає миттєвої реакції становить система раннього попередження та кризового реагування. Аналіз еволюції цієї системи протягом десятиліття протистояння гібридній агресії демонструє як болісні уроки початкового етапу, так і значний прогрес у розвитку спроможностей прогнозування та реагування на комплексні загрози.

Концептуальна трансформація підходів до раннього попередження стала наслідком гіркого досвіду 2014 року, коли традиційні системи моніторингу не змогли своєчасно ідентифікувати підготовку до анексії Криму та розпалювання конфлікту на Донбасі. Класична модель, орієнтована на виявлення концентрації військ, мобілізаційних заходів, дипломатичних демаршів, виявилася неефективною проти гібридної стратегії, що використовувала приховані операції, інформаційну підготовку, експлуатацію

внутрішніх вразливостей. Усвідомлення цього призвело до фундаментального переосмислення самого поняття раннього попередження – від моніторингу конкретних індикаторів до комплексного аналізу безпекового середовища [27].

Інституційна архітектура системи раннього попередження зазнала суттєвих змін. Якщо раніше функції моніторингу загроз були розпорошені між різними відомствами без належної координації, то поступово сформувалася більш інтегрована структура. Головний ситуаційний центр України при РНБО став ядром системи, що агрегує інформацію від різних джерел. Створення спеціалізованих аналітичних підрозділів у ключових відомствах – Центру оцінки безпекового середовища в Міноборони, аналітичних управлінь СБУ та розвідки – забезпечило експертну обробку первинної інформації. Важливим кроком стало залучення недержавних аналітичних центрів до системи раннього попередження, що розширило спектр джерел та підходів.

Методологія аналізу загроз еволюціонувала від лінійного прогнозування до сценарного планування та аналізу слабких сигналів. Розробка системи індикаторів гібридних загроз включила не лише традиційні військові показники, а й моніторинг інформаційного простору, соціальних настроїв, економічних залежностей, активності спецслужб противника. Впровадження методів Big Data аналізу дозволило обробляти величезні масиви неструктурованої інформації з відкритих джерел. Використання штучного інтелекту для виявлення аномалій та патернів підозрілої активності стало важливим технологічним проривом. Проте людський фактор – досвід аналітиків, їх інтуїція, здатність до нестандартного мислення – залишається незамінним [15].

Інформаційне забезпечення системи раннього попередження суттєво покращилося завдяки розширенню джерел даних та поліпшенню їх якості. Технічні засоби розвідки – супутникове спостереження, радіоелектронна розвідка, кіберрозвідка – надають об’єктивну інформацію про активність противника. Агентурна розвідка забезпечує доступ до планів та намірів

ворога. OSINT (розвідка з відкритих джерел) стала потужним інструментом завдяки розвитку соціальних мереж та цифрових технологій. Міжнародний обмін розвідувальною інформацією з партнерами суттєво розширив можливості раннього виявлення загроз. Критичним фактором стало навчання аналітиків працювати з суперечливою, неповною, часто дезінформаційною інформацією.

Система кризового реагування продемонструвала значну еволюцію від хаотичних дій 2014 року до структурованих алгоритмів 2024 року. Розробка типових планів реагування на різні сценарії – від терористичних атак до масованих кібератак – дозволила скоротити час прийняття рішень. Створення постійно діючих кризових штабів у ключових відомствах забезпечило готовність до негайних дій. Регулярні командно-штабні навчання відпрацьовують взаємодію в умовах різних кризових сценаріїв. Система оповіщення та мобілізації персоналу дозволяє розгорнути кризові структури протягом годин. Проте реальні кризи часто розвиваються за непередбаченими сценаріями, що вимагає гнучкості та імпровізації.

Технологічна модернізація стала ключовим фактором підвищення ефективності системи. Впровадження автоматизованих систем підтримки прийняття рішень дозволяє швидко моделювати розвиток ситуації та оцінювати наслідки різних варіантів дій. Геоінформаційні системи забезпечують візуалізацію оперативної обстановки в реальному часі. Захищені канали зв’язку гарантують безперебійну комунікацію навіть в умовах протидії противника. Системи штучного інтелекту допомагають фільтрувати інформаційний шум та виділяти критично важливі сигнали. Використання хмарних технологій забезпечує резервування та доступність критичних даних.

Міжвідомча інтеграція в системі раннього попередження та кризового реагування залишається найбільшим викликом. Попри створення координаційних механізмів, кожне відомство схильне покладатися на власні системи та процедури. Різні стандарти оцінки загроз, несумісність інформаційних систем, небажання ділитися ексклюзивною інформацією

знижують ефективність. Позитивним прикладом стала інтеграція систем ППО та РЕБ, що дозволяє виявляти та нейтралізовувати повітряні загрози в єдиному циклі. Проте в інших сферах рівень інтеграції залишається недостатнім. Особливо це стосується координації між військовими та цивільними структурами.

Регіональний вимір системи раннього попередження набув особливого значення в умовах загрози поширення конфлікту. Створення регіональних ситуаційних центрів, інтегрованих з центральною системою, дозволяє моніторити локальні загрози. Місцеві органи влади отримали нові повноваження та ресурси для розвитку систем моніторингу та реагування. Громадськість залучається через системи інформування про підозрілу активність. Однак при цьому рівень готовності регіонів суттєво відрізняється – прифронтові області розвинули ефективні системи, тоді як віддалені від бойових дій регіони часто недооцінюють загрози.

Психологічні аспекти функціонування системи виявилися критично важливими. Феномен «втоми від тривог» призводить до зниження пильності після численних попереджень, що не реалізувалися. Когнітивні упередження аналітиків можуть призводити до недооцінки або переоцінки загроз. Політичний тиск на систему раннього попередження створює ризики маніпулювання оцінками для досягнення кон’юнктурних цілей. Розробка механізмів захисту від цих викривлень – через колегіальність оцінок, залучення зовнішніх експертів, використання формалізованих методик – стала важливим напрямком удосконалення системи.

Практична ефективність системи раннього попередження та кризового реагування найкраще оцінюється через конкретні кейси. Успішне прогнозування та підготовка до повномасштабного вторгнення у 2022 році стали тріумфом оновленої системи – попри скептицизм частини суспільства, безпекові структури були готові до відсічі агресії. Ефективне реагування на масовані ракетні удари по критичній інфраструктурі продемонструвало злагодженість кризового менеджменту. Водночас були й провали – недооцінка

загрози в окремих напрямках, запізніле реагування на нові тактики противника. Кожен такий випадок став предметом аналізу та джерелом удосконалення системи.

Інтеграція громадянського суспільства в систему раннього попередження стала унікальною особливістю українського досвіду. Мережі громадських активістів, волонтерські організації, незалежні аналітичні центри часто виявляють загрози швидше за офіційні структури. Краудсорсинг інформації через мобільні додатки, соціальні мережі, спеціалізовані платформи суттєво розширив можливості моніторингу. Проте це створює виклики верифікації інформації, захисту від маніпуляцій, координації з офіційними структурами.

Міжнародний вимір системи раннього попередження став критично важливим фактором її ефективності. Обмін розвідувальною інформацією з партнерами, доступ до супутникових даних, участь у міжнародних системах моніторингу загроз якісно підвищили спроможності України. Особливо цінною виявилася допомога США та Великої Британії в передачі розвідданих напередодні повномасштабного вторгнення. Водночас надмірна залежність від іноземної розвідки створює ризики – партнери можуть мати власні інтереси, не завжди співпадаючі з українськими.

Перспективи розвитку системи раннього попередження та кризового реагування пов’язані з подальшою технологічною модернізацією, поглибленням аналітичних спроможностей, покращенням міжвідомчої координації. Критичними напрямками є: розвиток прогностичних моделей на основі штучного інтелекту; інтеграція всіх джерел інформації в єдину аналітичну платформу; стандартизація процедур оцінки загроз та реагування; підготовка нового покоління аналітиків з міждисциплінарними компетенціями; розвиток культури превентивного мислення в усіх безпекових структурах. У цілому, досвід показує, що ефективна система раннього попередження – це не лише технології та процедури, а й мистецтво передбачення, що поєднує науковий аналіз з інтуїцією досвідчених

професіоналів.

Окремо слід наголосити на адаптивності управлінських рішень до постійно змінюваної динаміки гібридних загроз, що також не в останню чергу визначає ефективність системи національної безпеки України в умовах перманентного протистояння з агресором, який постійно модифікує свої стратегії та тактики.

Аналіз еволюції управлінських підходів протягом десятиліття гібридної війни виявляє складну траєкторію переходу від ригідних бюрократичних процедур до більш гнучких механізмів прийняття та коригування рішень, хоча цей процес далекий від завершення. Парадигмальний зсув в управлінському мисленні став неминучим наслідком зіткнення з реальністю гібридної війни, де традиційні лінійні моделі планування та виконання виявилися неефективними. Класична модель «аналіз – планування – рішення – виконання – контроль» передбачала відносно стабільне середовище та передбачуваного противника. Гібридна агресія зруйнувала ці припущення, створивши ситуацію постійної невизначеності, де загрози можуть трансформуватися швидше, ніж бюрократична машина встигає відреагувати. Усвідомлення цього призвело до пошуку нових управлінських підходів, що поєднують стратегічну сталість з тактичною гнучкістю.

Швидкість прийняття рішень стала критичним фактором в умовах, коли вікно можливостей для ефективного реагування часто вимірюється годинами або навіть хвилинами. Досвід перших місяців війни 2014 року, коли бюрократичні процедури узгодження призводили до втрати ініціативи, змусив переглянути механізми прийняття рішень. Делегування повноважень нижчим рівням управління, створення механізмів прийняття рішень в обхід стандартних процедур у кризових ситуаціях, впровадження принципу «негативного узгодження» (рішення вважається прийнятим, якщо протягом визначеного часу не надійшло заперечень) – ці інновації дозволили суттєво скоротити управлінський цикл. При цьому ітеративність управлінських процесів замінила традиційну лінійність. Замість розробки «досконалих»

планів, що потім механічно виконуються, впроваджується підхід постійного коригування курсу на основі зворотного зв’язку. Концепція OODA loop (Observe-Orient-Decide-Act), запозичена з військової стратегії, стала основою для багатьох управлінських процесів. Регулярний перегляд рішень, готовність визнавати помилки та швидко змінювати курс стали новими управлінськими чеснотами, що контрастують з традиційною бюрократичною культурою «непогрішимості» рішень керівництва [106].

Децентралізація прийняття рішень також виявилася необхідною умовою адаптивності в умовах розподілених гібридних загроз. Традиційна модель жорсткої вертикалі, де всі важливі рішення приймаються на найвищому рівні, виявилася занадто повільною та негнучкою. Натомість розвивається модель «централізованого наміру та децентралізованого виконання» – вище керівництво визначає стратегічні цілі та обмеження, але тактичні рішення приймаються на місцях. Командири підрозділів, керівники регіональних структур, навіть окремі офіцери отримали більше повноважень для прийняття оперативних рішень в межах своєї компетенції.

Міжвідомча гнучкість стала викликом для системи, побудованої на чітких відомчих межах. Гібридні загрози часто вимагають негайної координації між структурами, що традиційно діють автономно. Створення механізмів швидкого формування міжвідомчих груп, спрощення процедур узгодження спільних дій, розвиток горизонтальних комунікацій між відомствами дозволили підвищити швидкість реагування. У той же час, глибинні проблеми відомчої замкненості, конкуренції за ресурси та вплив продовжують гальмувати адаптивність на міжвідомчому рівні [34].

Інформаційне забезпечення адаптивних рішень потребувало революції в системі збору, обробки та подання інформації керівництву. Традиційні багатосторінкові аналітичні довідки, що готувалися тижнями, виявилися неадекватними динаміці гібридних загроз. Натомість розвиваються системи оперативного інформування – дашборди з ключовими показниками, інтерактивні карти ситуації, стислі аналітичні продукти з чіткими висновками

та рекомендаціями. Використання систем штучного інтелекту для попередньої обробки інформації дозволяє керівникам зосередитися на прийнятті рішень, а не на пошуку та аналізі даних.

Сценарне планування стало важливим інструментом підвищення адаптивності. Замість спроб передбачити єдиний «найбільш ймовірний» розвиток подій, розробляються множинні сценарії з відповідними планами дій. Регулярні стратегічні сесії, воєнні ігри, симуляції дозволяють відпрацювати реакції на різні варіанти дій противника. Важливо, що сценарії включають не лише військові, а й комплексні гібридні загрози – від енергетичної блокади до масованих кібератак. Культура «підготовки до несподіванок» поступово витісняє традиційне прагнення до передбачуваності та контролю.

Механізми швидкого навчання та поширення досвіду стали критичними для адаптивності в масштабах всієї системи. Створення баз кращих практик, проведення регулярних розборів операцій, ротація персоналу між різними підрозділами та регіонами дозволяють швидко поширювати успішні рішення. Особливо ефективними виявилися неформальні мережі обміну досвідом – чати командирів в месенджерах, професійні спільноти в соціальних мережах. Водночас залишається проблема інституціоналізації уроків – перетворення індивідуального досвіду в організаційні процедури та доктрини.

Через це саме балансування між стабільністю та змінами стало мистецтвом адаптивного управління. Постійні зміни курсу можуть дезорієнтувати виконавців та підірвати довіру до керівництва. Водночас ригідне дотримання раз прийнятих рішень в умовах динамічних загроз веде до поразки. Вироблення критеріїв, коли потрібно наполягати на виконанні рішення, а коли – змінювати курс, стало важливою управлінською компетенцією. Комунікація причин змін, залучення виконавців до процесу адаптації рішень підвищує їх готовність до гнучкості.

Технологічна підтримка адаптивності включає впровадження сучасних інформаційних систем, що дозволяють моделювати наслідки рішень,

відстежувати їх виконання в реальному часі, швидко вносити корективи. Системи управління проектами адаптуються для безпекової сфери, дозволяючи координувати складні міжвідомчі операції. Мобільні технології забезпечують можливість прийняття рішень з будь-якої точки, що критично важливо в умовах розподіленого управління. Проте технології лише інструмент – без зміни управлінської культури вони не забезпечують справжньої адаптивності.

Правові аспекти адаптивності створюють особливі виклики в правовій державі. Гнучкість рішень не повинна означати правовий нігілізм або свавілля. Розробка механізмів швидкого прийняття нормативних актів в кризових ситуаціях, розширене тлумачення повноважень в межах закону, створення правових «пісочниць» для експериментів – ці підходи дозволяють поєднати адаптивність з верховенством права. Особливо важливим є механізм post-factum легалізації рішень, прийнятих в екстремальних умовах, з одночасним аналізом їх правомірності.

Психологічні бар'єри адаптивності часто виявляються найбільш стійкими. Страх відповідальності за «неправильні» рішення, кар'єрні ризики від визнання помилок, звичка до стабільності та передбачуваності – ці фактори гальмують готовність до гнучкості. Зміна системи мотивації, де заохочується розумний ризик та швидке виправлення помилок, а не бездіяльність та перестрахування, стала важливим напрямком організаційного розвитку. Лідерство через особистий приклад, коли керівники демонструють готовність до змін та визнання помилок, виявилося критичним фактором.

У цілому, оцінка результативності адаптивного управління через конкретні кейси демонструє як успіхи, так і провали. Швидка зміна тактики оборони Києва в перші дні повномасштабного вторгнення, гнучке реагування на зміну характеру бойових дій, адаптація до нових видів озброєння – приклади успішної адаптивності. Водночас були випадки, коли інерція мислення, бюрократичні процедури, міжвідомчі конфлікти призводили до запізнілого або неадекватного реагування на нові загрози. Кожен такий

випадок має бути предметом аналізу, хоча системні зміни відбуваються повільніше за накопичення уроків.

2.3. Компаративний аналіз міжнародного досвіду інституціалізації управління національною безпекою в умовах гібридних конфліктів

Дослідження моделей організації систем національної безпеки в країнах НАТО має критичне значення для України в контексті адаптації кращих практик до власних реалій протидії гібридним загрозам. Аналіз різноманітних підходів до побудови безпекових архітектур у державах-членах Альянсу дозволяє виявити спільні принципи, національні особливості та інноваційні рішення, що можуть бути корисними для подальшого розвитку української системи національної безпеки в умовах триваючої гібридної війни.

Концептуальна основа організації систем національної безпеки в країнах НАТО базується на спільних принципах, закріплених у Вашингтонському договорі та розвинутих у стратегічних документах Альянсу. Принцип колективної оборони, демократичного цивільного контролю над збройними силами, інтегрованого підходу до безпеки, поваги до верховенства права формують фундамент, на якому кожна країна будує власну національну систему. Водночас значна варіативність у конкретних організаційних рішеннях відображає різні історичні традиції, геополітичне становище, конституційні особливості та безпекові виклики кожної держави.

Американська модель організації системи національної безпеки характеризується чітким розподілом повноважень між федеральними відомствами та потужною роллю Ради національної безпеки як координаційного органу при Президенті. Департамент оборони відповідає за військову компоненту, Державний департамент – за дипломатичну, Департамент внутрішньої безпеки – за захист території США, розвідувальне співтовариство з 17 агенцій забезпечує інформаційну підтримку. Особливістю

є інтеграція всіх інструментів національної могутності через концепцію DIME (Diplomatic, Information, Military, Economic). Досвід США в координації масштабної безпекової системи через міжвідомчі процеси, використання технологій для інтеграції інформації, механізми стратегічного планування становлять цінність для України.

Британська модель демонструє ефективність централізованої координації через Кабінетний офіс та Раду національної безпеки. Система побудована на принципах колегіального прийняття рішень, де прем'єр-міністр головує, але рішення приймаються колективно. Особливістю є інтеграція розвідувальних служб (MI5, MI6, GCHQ) в єдину аналітичну систему через Об'єднаний розвідувальний комітет. Концепція Fusion Doctrine, прийнята у 2018 році, передбачає об'єднання всіх урядових можливостей для протидії сучасним загрозам, включаючи гібридні. Британський досвід створення Підрозділу гібридних загроз у структурі Кабінетного офісу, механізми швидкого реагування на кризи, система стратегічних комунікацій є особливо релевантними для України [134].

Німецька модель відображає федеральну структуру держави та особливості післявоєнної конституції, що обмежує використання збройних сил. Федеральна канцелярія координує безпекову політику, але значні повноваження мають федеральні міністерства – оборони, внутрішніх справ, закордонних справ. Бундесвер підпорядкований цивільному міністру оборони, внутрішня безпека забезпечується федеральними та земельними структурами. Особливістю є концепція «мережевої безпеки», що передбачає тісну співпрацю державних, приватних та громадських акторів. Створення Національної ради кібербезпеки, механізми цивільно-військової співпраці, система кризового менеджменту демонструють інноваційні підходи до організації безпеки.

Французька модель характеризується сильною роллю Президента як гаранта національної незалежності та головнокомандувача. Генеральний секретаріат національної оборони та безпеки при прем'єр-міністрі координує

міжвідомчу діяльність. Особливістю є концепція «глобальної безпеки», що інтегрує зовнішню та внутрішню безпеку, військові та цивільні аспекти. Білі книги з оборони та національної безпеки визначають стратегічні пріоритети. Досвід Франції в організації територіальної оборони, системі цивільної безпеки, механізмах реагування на терористичні загрози має практичну цінність для України [167].

Польська модель особливо цікава для України через схожість безпекових викликів та географічну близькість до Росії. Національна рада безпеки при Президенті координує безпекову політику, Бюро національної безпеки забезпечує аналітичну підтримку. Особливістю є розвинена система територіальної оборони, створена як окремий вид збройних сил. Концепція «східного флангу НАТО» визначає особливу роль Польщі в стримуванні російської агресії. Досвід інтеграції громадянського суспільства в систему безпеки, розвиток кіберспроможностей, механізми швидкого нарощування оборонного потенціалу є важливими для вивчення.

Естонська модель демонструє, як мала країна може ефективно організувати національну безпеку в умовах постійної загрози з боку Росії. Урядова комісія з безпеки координує діяльність всіх відомств, Рада безпеки при Президенті визначає стратегічні напрямки. Концепція «комплексної оборони» передбачає залучення всього суспільства до забезпечення безпеки. Кайтселійт (Союз оборони) як воєнізована громадська організація доповнює регулярні збройні сили. Естонія є лідером у кібербезпеці – досвід створення кіберкомандування, системи X-Road для безпечного обміну даними, механізмів захисту критичної інфраструктури становить особливу цінність [168].

Канадська модель відображає особливості федеративної держави з великою територією та обмеженими людськими ресурсами. Таємна рада координує безпекову політику, Департамент національної оборони інтегрує цивільну та військову компоненти. Особливістю є концепція «безпеки людини», що ставить захист громадян у центр безпекової політики.

Канадський досвід організації пошуково-рятувальних операцій, цивільно-військового співробітництва, миротворчих місій може бути корисним для України в контексті постконфліктного врегулювання.

Норвезька модель демонструє ефективність «тотальної оборони» – концепції, що передбачає мобілізацію всіх ресурсів суспільства для забезпечення безпеки. Рада безпеки при уряді координує діяльність, Директорат цивільної готовності забезпечує стійкість суспільства. Особливістю є тісна співпраця між державним та приватним секторами в забезпеченні критичної інфраструктури. Норвезький досвід організації територіальної оборони Home Guard, системи цивільної готовності, механізмів забезпечення стійкості в умовах гібридних загроз є релевантним для України.

Спільні риси моделей країн НАТО включають: чіткий демократичний цивільний контроль над силовими структурами; наявність координаційного органу на найвищому рівні; інтегрований підхід до різних вимірів безпеки; розвинені механізми міжвідомчої співпраці; залучення недержавних акторів; орієнтацію на спроможності, а не чисельність. Водночас кожна країна адаптує ці принципи до власних умов, створюючи унікальні організаційні рішення.

Еволюція моделей під впливом гібридних загроз демонструє спільні тенденції: посилення координаційних механізмів; створення спеціалізованих структур для протидії гібридним загрозам; розвиток кіберспроможностей; інтеграція інформаційного виміру в безпекову політику; посилення стійкості критичної інфраструктури; розширення співпраці з приватним сектором та громадянським суспільством. Ці тренди відображають усвідомлення того, що традиційні військово-центричні моделі недостатні для протидії сучасним викликам. Інноваційні організаційні рішення в країнах НАТО включають: створення гібридних центрів передового досвіду (Фінляндія); національних центрів кібербезпеки (Великобританія); агенцій психологічної стійкості (Швеція); підрозділів стратегічних комунікацій (Латвія). Ці нові інституційні форми відображають адаптацію до специфіки гібридних загроз та можуть служити прикладом для України.

Загальні уроки для України з досвіду країн НАТО включають важливість: сильної політичної волі для проведення реформ; чіткого розподілу повноважень з одночасною ефективною координацією; балансу між централізацією стратегічного управління та децентралізацією виконання; інвестицій у людський капітал та технології; розвитку культури співпраці між відомствами; залучення суспільства до забезпечення безпеки; постійної адаптації до нових викликів (табл. 2.2).

Таблиця 2.2

Компаративний аналіз моделей організації систем національної безпеки країн-партнерів України

Країна	**Координаційний орган**	**Структура сектору безпеки**	**Ключові інновації**	**Релевантні уроки для України**
США	Рада національної безпеки при Президенті	Департамент оборони, Держдепартамент, Департамент внутрішньої безпеки, 17 розвідувальних агенцій	Концепція DIME (Diplomatic, Information, Military, Economic); єдина система ситуаційної обізнаності	Важливість координації масштабної безпекової системи через міжвідомчі процеси та технологічну інтеграцію
Велико-британія	Рада національної безпеки при Кабінеті	Міноборони, МВС, МЗС, розвідслужби (MI5, MI6, GCHQ)	Fusion Doctrine - інтеграція всіх урядових можливостей; Підрозділ гібридних загроз	Ефективність централізованої координації та механізмів швидкого кризового реагування
Польща	Національна рада безпеки при Президенті	Міноборони, МВС, спецслужби, територіальна оборона як окремий вид ЗС	Розвинена система територіальної оборони; посилена присутність НАТО на східному фланзі	Важливість територіальної оборони та інтеграції громадянського суспільства в систему безпеки

Закінчення табл. 2.2

Країна	Координаційний орган	Структура сектору безпеки	Ключові інновації	Релевантні уроки для України
Естонія	Урядова комісія з безпеки	Міноборони, МВС, Департамент поліції, Служба зовнішньої розвідки	Концепція комплексної оборони; світове лідерство в кібербезпеці (X-Road, кіберкомандування)	Можливість малої країни ефективно протидіяти гібридним загрозам через технологічні інновації та суспільну мобілізацію
Латвія	Рада національної безпеки	Міноборони, МВС, Конституційне бюро захисту, Земессардзе (Нацгвардія)	Центр стратегічних комунікацій НАТО в Ризі; активна протидія російській пропаганді	Ефективність превентивних заходів у протидії дезінформації та важливість соціальної інтеграції
Литва	Рада оборони при Президенті	Міноборони, МВС, Департамент держбезпеки, Добровольчі сили національної оборони	Перша країна ЄС, що заборонила російське пропагандистське ТБ; активна підтримка білоруської опозиції	Важливість політичної волі та послідовності в протидії російському впливу

При цьому досвід країн Балтії – Естонії, Латвії та Литви – у протидії гібридним загрозам представляє особливу цінність для України через схожість викликів, що походять від спільного агресора – Російської Федерації, а також порівнянні масштаби держав та спільне радянське минуле. Балтійські країни першими зіткнулися з елементами гібридної агресії ще до подій 2014 року в Україні, що дозволило їм розробити превентивні механізми та інноваційні підходи до забезпечення національної стійкості, які довели свою ефективність.

Естонський досвід протидії гібридним загрозам є унікальним через поєднання технологічних інновацій з традиційними підходами до оборони. Кібератака 2007 року стала першим масштабним проявом гібридної агресії

проти Естонії, коли паралізація державних сайтів, банківської системи та критичної інфраструктури супроводжувалася масовими заворушеннями російськомовного населення. Відповіддю стало створення комплексної системи кібербезпеки, що включає Центр кіберзахисту, обов'язкові стандарти для критичної інфраструктури, регулярні кібернавчання Locked Shields. Естонія стала світовим лідером у цифровій стійкості – система X-Road забезпечує безпечний обмін даними між державними установами, а блокчейн-технології захищають критичні реєстри від маніпуляцій [112].

Концепція комплексної оборони Естонії передбачає залучення всього суспільства до протидії гібридним загрозам. Кайтселійт (Союз оборони) об'єднує понад 28 тисяч добровольців, які проходять регулярну військову підготовку та готові доповнити регулярні збройні сили. Молодіжні організації Noorkotkad та Kodutütred виховують патріотизм та базові військові навички з дитинства. Система психологічної оборони включає медіаграмотність в школах, підтримку естономовних медіа, протидію російській пропаганді. Закон про надзвичайний стан детально регламентує дії всіх інституцій в кризових ситуаціях, що було відпрацьовано під час пандемії COVID-19.

Латвійський підхід до протидії гібридним загрозам характеризується особливою увагою до інформаційної безпеки та соціальної інтеграції. Маючи найбільшу частку російськомовного населення серед країн Балтії (близько 25%), Латвія стикається з постійними спробами Росії експлуатувати мовні та етнічні розбіжності. Національна рада електронних мас-медіа активно протидіє російській пропаганді через заборону ретрансляції російських каналів, моніторинг контенту, підтримку якісних латвійськомовних медіа. Центр стратегічних комунікацій НАТО в Ризі став провідною установою з дослідження та протидії дезінформації, розробляючи методології виявлення та нейтралізації інформаційних атак [177].

Інституційні механізми Латвії включають Раду національної безпеки як координаційний орган, Конституційне бюро захисту як контррозвідувальну службу, Бюро запобігання та боротьби з корупцією. Особливістю є створення

Державної канцелярії мови, що просуває латиську як єдину державну мову, протидіючи спробам Росії використовувати мовне питання для дестабілізації. Програма інтеграції суспільства спрямована на формування єдиної громадянської ідентичності. Земессардзе (Національна гвардія) налічує понад 8 тисяч добровольців та відіграє важливу роль у територіальній обороні.

Литовський досвід демонструє важливість політичної волі та послідовності в протидії гібридним загрозам. Литва першою серед країн ЄС визнала російське телебачення загрозою національній безпеці та заборонила ретрансляцію пропагандистських каналів. Департамент державної безпеки активно викриває російську агентуру, публікуючи щорічні звіти про загрози національній безпеці з конкретними прикладами російських операцій. Литва послідовно підтримує демократичні сили в Білорусі, надаючи притулок опозиції, що створює додатковий буфер безпеки [196].

Енергетична безпека стала пріоритетом для всіх трьох країн як відповідь на енергетичний шантаж Росії. Естонія, Латвія та Литва синхронізували свої електромережі з континентальною Європою, припинивши залежність від російської системи. Клайпедський LNG термінал забезпечив альтернативу російському газу. Розвиток відновлюваної енергетики зменшує вразливість до енергетичних маніпуляцій. Цей досвід демонструє, що енергетична незалежність є критичним компонентом протидії гібридним загрозам.

Регіональна співпраця країн Балтії створює синергетичний ефект у протидії гібридним загрозам. Спільні військові проекти, такі як Baltic Air Policing, координація розвідувальних зусиль, обмін інформацією про гібридні загрози підвищують колективну стійкість. Балтійська асамблея та Рада міністрів країн Балтії координують політику у сфері безпеки. Спільні навчання з НАТО, включаючи Saber Strike та Baltic Fortress, відпрацьовують сценарії протидії гібридній агресії. Формат B3+1 (країни Балтії + Польща) розширює регіональну співпрацю.

Правові інновації країн Балтії включають криміналізацію заперечення радянської окупації, законодавство про люстрацію колишніх співробітників

КДБ, жорсткі вимоги до прозорості фінансування медіа та громадських організацій. Естонія прийняла закон про кібербезпеку, що встановлює обов'язкові стандарти для критичної інфраструктури. Латвія посилила законодавство про державну зраду та шпигунство. Литва ввела кримінальну відповідальність за публічне схвалення російської агресії. Ці правові інструменти створюють рамки для ефективної протидії гібридним загрозам [197].

Економічна стійкість як компонент протидії гібридним загрозам включає диверсифікацію торговельних партнерів, зменшення залежності від російського ринку, захист стратегічних активів від ворожого поглинання. Країни Балтії успішно переорієнтували свої економіки на ЄС, хоча це потребувало болісних структурних реформ. Механізми скринінгу іноземних інвестицій запобігають проникненню російського капіталу в критичні сектори. Розвиток цифрової економіки створює нові можливості та зменшує залежність від традиційних секторів, вразливих до російського впливу.

Соціальна стійкість забезпечується через інклюзивну політику, що протидіє спробам Росії розколоти суспільство. Програми вивчення державної мови, інтеграційні курси для негромадян, підтримка культурної різноманітності при збереженні національної ідентичності – ці заходи зменшують простір для маніпуляцій. Опитування показують зростання лояльності російськомовного населення до своїх країн та зниження впливу російської пропаганди.

Технологічні рішення країн Балтії включають використання штучного інтелекту для виявлення дезінформації, блокчейн для захисту критичних даних, системи раннього попередження про кіберзагрози. Естонська e-Residency програма створює глобальну мережу підтримки. Латвійські стартапи розробляють рішення для кібербезпеки. Литва інвестує в технології подвійного призначення. Ці інновації підвищують технологічну стійкість до гібридних атак.

Міжнародний вимір стратегій країн Балтії включає активну роботу в

НАТО та ЄС щодо визнання гібридних загроз, лобіювання посиленої присутності Альянсу, обмін досвідом з партнерами. Центри передового досвіду НАТО в Талліні (кібероборона) та Ризі (стратегічні комунікації) стали глобальними хабами експертизи. Країни Балтії активно підтримують Україну, ділячись досвідом та надаючи практичну допомогу.

Уроки для України з балтійського досвіду включають: важливість превентивних заходів до ескалації; необхідність комплексного підходу, що охоплює всі виміри безпеки; критичну роль суспільної стійкості та єдності; значення технологічних інновацій; ефективність регіональної співпраці; необхідність балансу між безпековими заходами та демократичними свободами. Водночас важливо враховувати різницю в масштабах – те, що працює для малих країн Балтії, потребує адаптації для України.

Взагалі ж, інституційні інновації у безпековому управлінні країн Європейського Союзу відображають фундаментальну трансформацію підходів до забезпечення безпеки в умовах появи гібридних загроз, що розмивають традиційні межі між внутрішньою та зовнішньою безпекою, військовими та цивільними викликами. Аналіз цих інновацій дозволяє виявити передові організаційні рішення, нові форми координації та механізми забезпечення стійкості, які можуть бути адаптовані до українського контексту з урахуванням специфіки триваючої гібридної війни.

Наднаціональний рівень інституційних інновацій ЄС демонструє спроби створення спільних механізмів протидії гібридним загрозам при збереженні національного суверенітету у безпековій сфері. Створення посади Високого представника ЄС з питань закордонних справ і політики безпеки, що одночасно є віце-президентом Єврокомісії, забезпечило інституційний зв’язок між зовнішньою та внутрішньою безпекою. Європейська служба зовнішніх справ інтегрує дипломатичні, безпекові та оборонні аспекти. Гібридний центр аналізу при ЄСЗС, створений у 2016 році, став першою спробою систематичного моніторингу та аналізу гібридних загроз на рівні ЄС [121].

Інноваційним механізмом стало створення Постійної структурованої

співпраці (PESCO) у сфері оборони, що дозволяє групам країн-членів розвивати спільні оборонні проекти. З 60 проектів PESCO значна частина спрямована на протидію гібридним загрозам: кіберрозвідка, захист критичної інфраструктури, військова мобільність, протидія дезінформації. Європейський оборонний фонд з бюджетом 8 мільярдів євро на 2021-2027 роки фінансує дослідження та розробки у сфері оборони, включаючи технології протидії гібридним загрозам. Ці механізми демонструють перехід від суто міжурядової до частково наднаціональної координації безпекової політики.

Французькі інституційні інновації відображають прагнення до стратегічної автономії та комплексного підходу до безпеки. Створення Національної ради розвідки при Президенті у 2021 році забезпечило кращу координацію розвідувальних служб. Інноваційним стало формування Командування кіберзахисту як четвертого роду військ поряд з армією, флотом та авіацією. Агентство національної безпеки інформаційних систем координує кіберзахист критичної інфраструктури. Особливістю є концепція «економічної розвідки», що поєднує захист економічних інтересів з традиційною безпекою [123].

Німецькі інновації зосереджені на подоланні фрагментації федеральної системи безпеки. Створення Національної ради кібербезпеки об’єднало федеральні та земельні структури, державний та приватний сектори. Федеральна академія безпекової політики стала майданчиком для вироблення спільних підходів між різними відомствами. Інноваційним є механізм «Мережева політика безпеки», що передбачає систематичну співпрацю між урядом, бізнесом, наукою та громадянським суспільством. Центр протидії гібридним загрозам при Федеральній розвідці аналізує комплексні загрози.

Іспанський досвід демонструє важливість адаптації безпекових структур до внутрішніх викликів. Створення Департаменту національної безпеки при Кабінеті прем’єр-міністра забезпечило координацію всіх безпекових відомств. Інтегрована система національної безпеки об’єднує 12 сфер – від тероризму до міграції. Інноваційним є механізм ситуаційної обізнаності, що інтегрує

інформацію від усіх джерел в єдину картину. Досвід протидії сепаратизму в Каталонії продемонстрував важливість невійськових інструментів у протидії гібридним загрозам [176].

Італійські інновації включають створення Міжвідомчого комітету з кібербезпеки, що координує зусилля 11 міністерств та агенцій. Національна агенція кібербезпеки, створена у 2021 році, консолідувала розпорошені функції. Особливістю є механізм «золотих повноважень», що дозволяє уряду блокувати іноземні інвестиції в стратегічні сектори. Досвід протидії організованій злочинності адаптується для боротьби з гібридними загрозами через механізми фінансового моніторингу та антикорупційні заходи.

Нідерландські інституційні інновації відображають акцент на соціальній стійкості. Національний координатор безпеки та протидії тероризму інтегрує всі аспекти національної безпеки. Інноваційним є підхід «всього суспільства» – систематичне залучення громадян, бізнесу, місцевої влади до забезпечення безпеки. Програма «Міцне суспільство» розвиває стійкість громад до різних загроз. Досвід розслідування збиття MH17 продемонстрував важливість міжнародної співпраці та інноваційних методів розслідування [179].

Бельгійські інновації зосереджені на координації складної федеральної системи. Створення Центру кризового управління забезпечило єдину точку координації під час надзвичайних ситуацій. Інтегрований механізм оцінки загроз об’єднує розвідувальні служби, поліцію, митницю. Особливістю є розвинена система раннього попередження про радикалізацію на місцевому рівні. Досвід протидії тероризму після атак 2016 року призвів до створення нових механізмів обміну інформацією.

Данські інновації включають створення Центру протидії гібридним загрозам при Міністерстві оборони, що аналізує та координує реагування на комплексні виклики. Інноваційним є механізм «безпекового діалогу» між урядом та критичною інфраструктурою. Данія розвинула унікальну систему психологічної стійкості через освітні програми та громадські ініціативи. Досвід протидії російському впливу в Арктиці демонструє важливість

превентивних заходів.

Шведські інституційні інновації відображають повернення до концепції «тотальної оборони» після десятиліть нейтралітету. Агентство психологічної оборони, створене у 2022 році, стало першою у світі державною установою, спеціально призначеною для протидії дезінформації та психологічним операціям. Відновлення цивільної оборони включає навчання всього населення діям в умовах кризи. Інноваційним є механізм співпраці з технологічними компаніями для виявлення та протидії інформаційним атакам.

Фінські інновації базуються на унікальній моделі «комплексної безпеки», що поєднує військову оборону, цивільну готовність та психологічну стійкість. Комітет безпеки при уряді координує всі аспекти національної безпеки. Інноваційним є обов'язкове навчання топ-менеджерів критичної інфраструктури з питань безпеки. Система «72 години» забезпечує готовність кожного домогосподарства до автономного виживання. Досвід протидії російському впливу включає унікальні медіаосвітні програми.

Австрійські інновації, незважаючи на нейтральний статус, включають створення Ради національної безпеки з широкими координаційними повноваженнями. Інтегрована система кризового менеджменту об'єднує федеральні та земельні структури. Особливістю є механізм «безпекового партнерства» між державою та приватним сектором. Досвід протидії російському впливу через енергетичні проекти демонструє важливість економічної безпеки.

Якщо узагальнити, то можна зазначити, що спільні тенденції інституційних інновацій країн ЄС включають: створення координаційних органів високого рівня; інтеграцію різних вимірів безпеки; систематичне залучення недержавних акторів; розвиток механізмів стійкості; акцент на превентивних заходах; використання технологічних рішень. Ці інновації відображають усвідомлення, що гібридні загрози вимагають гібридних відповідей – поєднання традиційних та нових підходів, державних та недержавних зусиль, національних та наднаціональних механізмів.

Азійські моделі забезпечення національної безпеки також представляють унікальний досвід організації безпекових систем, що поєднують тисячолітні традиції стратегічного мислення з сучасними технологічними інноваціями, колективістські цінності з прагматичним підходом до міжнародних відносин. Для України, що шукає оптимальні шляхи протидії гібридним загрозам, вивчення азійського досвіду відкриває альтернативні перспективи, які можуть доповнити євроатлантичні підходи та збагатити інструментарій національної безпеки.

Так, китайська модель забезпечення національної безпеки демонструє унікальне поєднання партійного керівництва, технологічного контролю та концепції «комплексної національної безпеки». Центральна комісія національної безпеки при ЦК Компартії Китаю, очолювана Генеральним секретарем, координує всі аспекти безпеки – від традиційної оборони до кібербезпеки та ідеологічного контролю. Концепція «активної оборони» передбачає превентивні дії для захисту національних інтересів, включаючи економічну експансію та технологічне домінування. Система «соціального кредиту» використовує великі дані та штучний інтелект для моніторингу та управління поведінкою громадян, що розглядається як інструмент забезпечення внутрішньої стабільності [206].

Технологічний вимір китайської моделі включає масштабні інвестиції в штучний інтелект, квантові обчислення, 5G мережі як інструменти забезпечення безпеки. «Великий китайський файрвол» демонструє можливості контролю інформаційного простору в масштабах країни. Концепція «військово-цивільного злиття» стирає межі між оборонними та цивільними технологіями, мобілізуючи всі ресурси для безпекових цілей. Досвід Китаю показує як потенціал, так і ризики тотального технологічного контролю для забезпечення безпеки.

Японська модель відображає унікальне поєднання пацифістської конституції з прагматичною безпековою політикою в умовах регіональних загроз. Рада національної безпеки Японії координує безпекову політику,

інтегруючи дипломатичні, економічні та оборонні аспекти. Концепція «проактивного пацифізму» дозволяє розширювати безпекові можливості в рамках конституційних обмежень. Сили самооборони, формально не будучи армією, розвинули високотехнологічні спроможності, особливо в сферах ПРО, кіберзахисту, морської безпеки. Альянс з США забезпечує «парасольку безпеки», дозволяючи Японії фокусуватися на нішевих спроможностях [169].

Інноваційні підходи Японії включають концепцію «людської безпеки», що ставить добробут громадян у центр безпекової політики. Система реагування на природні катастрофи, відпрацьована через численні землетруси та цунамі, демонструє важливість стійкості суспільства. Технологічне лідерство в робототехніці, матеріалознавстві, електроніці конвертується в безпекові спроможності. Досвід протидії північнокорейській загрозі через поєднання дипломатії, санкцій, оборонних заходів може бути корисним для України.

Південнокорейська модель сформувалася в унікальних умовах постійної загрози з боку КНДР та демонструє ефективність поєднання військової готовності з економічним розвитком. Рада національної безпеки при Президенті координує всі аспекти безпеки. Концепція «всебічної безпеки» інтегрує військові, економічні, соціальні виміри. Обов'язкова військова служба забезпечує високий рівень мобілізаційної готовності. Інвестиції в оборонну промисловість перетворили Південну Корею на глобального експортера озброєнь. Досвід кіберзахисту, розвинений у протистоянні з високотехнологічним противником, є особливо цінним [142].

Сінгапурська модель «тотальної оборони» демонструє, як мала держава може забезпечити безпеку через комплексний підхід. П'ять стовпів – військова, цивільна, економічна, соціальна та психологічна оборона – інтегруються в цілісну систему. Міністерство оборони координує не лише військові, а й цивільні аспекти безпеки. Обов'язкова військова служба поєднується з регулярними резервними тренуваннями. Концепція «отруйної креветки» – створення таких оборонних спроможностей, що агресія стане

занадто costly – ефективна стратегія для малої держави. Технологічні інновації, включаючи широке використання ШІ для безпеки, компенсують брак людських ресурсів.

Ізраїльська модель, хоча географічно не азійська, але культурно пов'язана з регіоном, демонструє унікальний досвід забезпечення безпеки в умовах постійної загрози. Концепція «нації в уніформі» передбачає тотальну мобілізацію суспільства. ЦАГАЛ інтегрує регулярні сили з резервом, забезпечуючи швидке нарощування. Технологічне лідерство в кібербезпеці, системах ППО (Iron Dome), розвідувальних технологіях створює асиметричні переваги. Досвід превентивних ударів, доктрина «кампанії між війнами» демонструють проактивний підхід до безпеки. Інтеграція безпекового сектору з високотехнологічною економікою створює синергію [120].

Індійська модель відображає виклики забезпечення безпеки великої, різноманітної держави з кількома активними конфліктами. Рада національної безпеки при прем'єр-міністрі координує безпекову політику. Інтегрований штаб оборони забезпечує міжвидову координацію. Доктрина «холодного старту» передбачає швидке розгортання для відповіді на провокації. Розвиток ядерної тріади забезпечує стратегічне стримування. Досвід протидії тероризму, повстанським рухам, гібридним тактикам Пакистану в Кашмірі є релевантним. Програма Make in India в оборонній сфері демонструє шлях до самозабезпечення.

В'єтнамська модель «всенародної оборони» базується на історичному досвіді партизанської війни та адаптується до сучасних викликів. Центральна військова комісія координує всі аспекти оборони. Концепція «народної війни в морі» адаптує традиційні підходи до морської безпеки. Мобілізація всього суспільства через мережу міліції та самооборони створює глибину оборони. Балансування між великими державами демонструє мистецтво стратегічної гнучкості. Досвід протидії «сірим зонним» тактикам Китаю в Південно-Китайському морі є особливо актуальним.

Тайванська модель формувалася в унікальних умовах постійної загрози

вторгнення з материка. Концепція «дикобразної оборони» передбачає створення таких спроможностей, що зроблять вторгнення надто costly. Асиметричні спроможності – протикорабельні ракети, мобільні ППО, кіберзахист – компенсують кількісну перевагу противника. Резервна система забезпечує швидку мобілізацію. Технологічне лідерство в напівпровідниках конвертується в безпекові переваги. Досвід протидії інформаційним атакам та політичному тиску є безпосередньо релевантним для України.

У цілому, спільні риси азійських моделей включають: акцент на соціальній мобілізації та єдності; поєднання традиційних цінностей з технологічними інноваціями; прагматичний підхід до балансування між великими державами; розвиток асиметричних спроможностей; інтеграція економічного розвитку з безпековими цілями; довгострокове стратегічне планування. Ці підходи відрізняються від західних моделей більшою готовністю обмежувати індивідуальні свободи заради колективної безпеки.

Отже, уроки для України з азійського досвіду включають: важливість мобілізації всього суспільства для забезпечення безпеки; потенціал асиметричних стратегій для компенсації кількісної переваги противника; критичну роль технологічних інновацій; необхідність довгострокового стратегічного мислення; можливості конвертації економічного потенціалу в безпекові спроможності. Водночас важливо враховувати культурні та політичні відмінності – не всі азійські підходи сумісні з європейськими цінностями та демократичними принципами України. Крім того, критичний аналіз показує, що азійські моделі мають як сильні, так і слабкі сторони. Висока ефективність часто досягається ціною обмеження свобод. Технологічний контроль створює ризики авторитаризму. Акцент на стабільності може гальмувати інновації. Тому для України важливо селективно адаптувати корисні елементи, зберігаючи демократичний характер держави.

Взагалі, адаптація кращих міжнародних практик забезпечення національної безпеки до українських реалій становить складне завдання, що

вимагає глибокого розуміння як самих практик та контексту їх успішного функціонування, так і специфіки української ситуації з її унікальними викликами, можливостями та обмеженнями. Механічне копіювання навіть найуспішніших моделей без урахування національного контексту приречене на провал, тому критично важливим є творчий синтез міжнародного досвіду з українськими традиціями, ресурсами та потребами.

Контекстуальні фактори, що визначають специфіку української ситуації, включають насамперед реальність триваючої гібридної війни з ядерною державою, що має значну перевагу в ресурсах та не обмежена міжнародним правом у виборі методів агресії. На відміну від країн НАТО, що можуть розраховувати на колективну оборону, або нейтральних країн, що уникають прямої конфронтації, Україна змушена самостійно протистояти екзистенційній загрозі. Це вимагає пріоритизації оборонних спроможностей та готовності до тривалого протистояння, що не характерно для більшості європейських країн. Водночас обмежені ресурси не дозволяють просто нарощувати кількісні показники, вимагаючи інноваційних асиметричних рішень.

Інституційна спадщина України створює як можливості, так і обмеження для адаптації кращих практик. Пострадянська традиція сильних силових структур може бути трансформована в ефективну систему національної безпеки, але вимагає подолання корупції, непотизму, закритості. Досвід державного будівництва в умовах зовнішньої агресії створив унікальну стійкість та адаптивність, але також призвів до певної мілітаризації суспільної свідомості. Традиції самоорганізації та волонтерства, яскраво проявлені під час Революції Гідності та війни, створюють потужний ресурс, але вимагають інституціоналізації для довгострокової ефективності.

Ресурсні обмеження диктують необхідність вибірковості в адаптації міжнародних практик. Україна не може дозволити собі розкіш утримувати всі елементи комплексних систем безпеки розвинених країн. Необхідна жорстка пріоритизація – концентрація на критично важливих спроможностях при

мінімізації витрат на престижні, але неефективні проекти. Досвід показує, що креативність та інновації можуть частково компенсувати брак ресурсів – українські розробки дронів, систем РЕБ, ІТ-рішень часто перевершують дорогі закордонні аналоги.

Адаптація натовських стандартів управління обороною стала одним з найуспішніших прикладів трансформації міжнародного досвіду. Впровадження циклу оборонного планування NDPP, системи J-структури штабів, процедур оперативного планування підвищило ефективність управління. Але механічне копіювання натовських структур без урахування реалій війни призводило до проблем – надмірна бюрократизація, повільність прийняття рішень. Успішною стала гібридна модель, що поєднує натовські стандарти з українською оперативністю та гнучкістю.

Досвід країн Балтії у протидії російському впливу виявився особливо релевантним, але вимагав масштабування. Естонські підходи до кібербезпеки успішно адаптовані через створення власних кіберпідрозділів та CERT-UA. Латвійський досвід стратегічних комунікацій трансформувався в український Центр протидії дезінформації. Литовська модель енергетичної незалежності надихнула на диверсифікацію енергопостачання. Але масштаб України вимагав не просто копіювання, а створення розподілених систем з регіональними вузлами.

Ізраїльський досвід виявився цінним у специфічних сферах – організації територіальної оборони, розвитку оборонних технологій, інтеграції резервістів. Концепція «нації в уніформі» резонувала з українським досвідом масової мобілізації. Але пряме копіювання ізраїльської моделі загальної військової повинності виявилося неможливим через масштаб країни та специфіку конфлікту. Натомість розвинулася унікальна українська модель поєднання професійної армії, територіальної оборони та добровольчого руху.

Технологічні інновації з різних країн адаптувалися через призму української ІТ-експертизи. Естонська X-Road трансформувалася в українську «Дію» – більш масштабну та функціональну. Південнокорейські підходи до

кібербезпеки поєднувалися з українськими розробками. Китайський досвід використання дронів переосмислювався через українські інновації. Результатом стала не імітація, а оригінальні рішення, що часто перевершували прототипи.

Організаційні інновації вимагали особливо делікатної адаптації через інституційний опір. Спроби впровадити скандинавську модель прозорості наштовхувалися на традиції секретності. Німецька модель федералізму в безпеці конфліктувала з українською централізацією. Успішними були поступові зміни – створення нових структур (кіберкомандування, ССО) за міжнародними стандартами при збереженні традиційних. Критичним фактором успіху була наявність «агентів змін» – реформаторів з досвідом роботи в міжнародному середовищі.

Правова адаптація виявилася одним з найскладніших аспектів. Європейські правові стандарти часто конфліктували з потребами воєнного часу. Спроби впровадити повну транспарентність оборонних закупівель створювали ризики для безпеки. Механізми громадського контролю, ефективні в мирний час, могли паралізувати прийняття рішень у кризових ситуаціях. Розв’язанням стала диференційована модель – повне дотримання стандартів у некритичних сферах при збереженні гнучкості в оперативних питаннях.

Культурна адаптація часто недооцінювалася, але виявлялася критичною для успіху реформ. Західна культура планування конфліктувала з українською імпровізацією. Натовська формальність процедур суперечила українській неформальності відносин. Азійський колективізм не відповідав українському індивідуалізму. Успішні адаптації враховували ці культурні особливості – формальні процедури доповнювалися неформальними каналами, жорстке планування поєднувалося з гнучкістю виконання.

Фінансові механізми адаптації включали творче поєднання різних джерел фінансування. Американська модель оборонних контрактів адаптувалася до українських реалій через ProZorro. Європейські грантові

механізми використовувалися для фінансування реформ. Краудфандинг доповнював державне фінансування. Результатом стала унікальна модель «гібридного фінансування», що поєднує державні, міжнародні та громадські ресурси.

Слід зазначити, що загальна оцінка ефективності адаптації показує нерівномірність успіхів. Так, найкраще адаптувалися технологічні та організаційні інновації у сферах, де був сильний внутрішній попит та наявні компетенції, а найгірше – це системні реформи, що вимагали зміни ментальності та подолання корупційних інтересів. Причому війна, з одного боку, стала каталізатором успішних адаптацій, але також створювала виправдання для опору змінам «не на часі».

Підсумовуючи, можна визначити такі уроки процесу адаптації: необхідність глибокого розуміння не лише форми, а й сутності практик, що адаптуються; важливість поступовості та експериментування замість революційних змін; критичну роль лідерства та «агентів змін»; необхідність балансу між збереженням національної специфіки та впровадженням міжнародних стандартів; важливість комунікації цілей та очікуваних результатів реформ.

Перспективи подальшої адаптації пов’язані з післявоєнною трансформацією, коли з’явиться можливість системних реформ без обмежень воєнного часу. При цьому критичними напрямками можна вважати: інтеграцію ветеранів у мирне життя з використанням досвіду країн НАТО; трансформацію оборонної промисловості за південнокорейською моделлю; розвиток системи національної стійкості за фінським зразком; створення регіональної безпекової архітектури з Україною як лідером. І успіх тут залежатиме від здатності зберегти енергію змін, накопичену під час війни, та спрямувати її на системну трансформацію країни.

Висновки до другого розділу

1. Нормативно-правова база функціонування системи національної безпеки України зазнала фундаментальної трансформації під впливом гібридної агресії, що виявилося у прийнятті нового базового законодавства (Закон «Про національну безпеку України» 2018 року, Закон «Про розвідку» 2020 року), оновленні стратегічних документів (Стратегія національної безпеки 2020 року, Воєнна доктрина 2015 року) та запровадженні нових правових інструментів протидії гібридним загрозам (законодавство про санкції, кібербезпеку, правовий режим воєнного стану). Разом з тим, аналіз виявив залишкові прогалини у правовому регулюванні інформаційної безпеки, координації діяльності різних суб'єктів, механізмів швидкого правового реагування на нові типи загроз, що створює виклики для ефективної протидії динамічним гібридним загрозам та вимагає подальшого вдосконалення законодавчої бази.

2. Організаційна структура суб'єктів забезпечення національної безпеки України еволюціонувала від пострадянської моделі до більш інтегрованої системи, адаптованої до викликів гібридної війни. Створення нових інституцій (Державний центр кіберзахисту, Центр протидії дезінформації, Сили територіальної оборони) та трансформація існуючих структур (РНБО, Міністерство оборони, СБУ) демонструють здатність системи до інституційних інновацій. Водночас, дослідження виявило проблеми дублювання функцій між різними відомствами, недостатньої горизонтальної координації, існування «сірих зон» компетенції у протидії гібридним загрозам, що знижує загальну ефективність системи та потребує подальшої оптимізації організаційної архітектури з акцентом на функціональну інтеграцію при збереженні спеціалізації. При цьому функціональний розподіл повноважень у сфері безпекового управління характеризується поступовим переходом від жорсткого відомчого розмежування до більш гнучких механізмів міжвідомчої взаємодії, що відповідає природі гібридних загроз. Проте залишаються

проблемні аспекти, пов’язані з неповною чіткістю розмежування повноважень на стиках компетенцій, особливо у нових сферах (кібербезпека, протидія дезінформації, захист критичної інфраструктури), що вимагає подальшого уточнення та формалізації функціонального розподілу.

3. Проблеми координації та взаємодії безпекових інституцій залишаються одним з найслабших місць системи національної безпеки України, незважаючи на значні зусилля з їх подолання. Структурні бар’єри координації коріняться у пострадянській спадщині відомчої фрагментації, конкуренції за ресурси та вплив, технічній несумісності інформаційних систем, культурно-психологічних відмінностях між силовими структурами. Хоча створено механізми вертикальної та горизонтальної координації (ситуаційні центри, міжвідомчі робочі групи, системи обміну інформацією), їх ефективність часто обмежується відомчими інтересами, формальним характером взаємодії, відсутністю загальної доктрини міжвідомчої співпраці. Подальше вдосконалення координації вимагає не лише організаційних та технологічних рішень, а й глибинної зміни організаційної культури з формування довіри, спільної ідентичності, готовності ставити загальні цілі вище відомчих.

4. Оцінювання ефективності механізмів публічного управління національною безпекою в умовах гібридної агресії продемонструвало значну позитивну динаміку порівняно з початковим етапом 2014 року. Десятирічний період протистояння став безпрецедентним випробуванням, що стимулювало інституційну адаптацію - від початкового колапсу та хаотичного реагування до формування більш структурованої системи з елементами превентивного планування, розвиненою координацією, міжнародною інтеграцією. Еволюція реагування включала чотири основні етапи: початковий колапс 2014 року з виявленням критичних вразливостей; адаптацію 2015-2016 років зі стабілізацією фронту та початком реформ; системні реформи 2017-2021 років з оновленням правової бази та професіоналізацією; період повномасштабної війни 2022-2024 років з демонстрацією якісно вищого рівня готовності.

Ключовими факторами успішної трансформації стали здатність до швидкого навчання на помилках, мобілізація громадянського суспільства, ефективне використання міжнародної підтримки, розвиток інноваційних підходів при збереженні демократичного характеру держави.

5. Реформування сектору безпеки і оборони України в період 2014-2024 років стало найбільш масштабною та глибокою трансформацією безпекових інституцій в історії незалежної України, що відбувалася в унікальних умовах одночасного ведення бойових дій та системних перетворень. Ключовими досягненнями реформ стали: розмежування функцій політичного керівництва та військового управління в Міноборони; перехід від радянської чотирьохвидової до тривидової структури Збройних Сил; створення нових високомобільних формувань (ССО, ДШВ, територіальна оборона); професіоналізація особового складу з підвищенням частки контрактників до 60%; реформа військової освіти відповідно до стандартів НАТО; часткова модернізація озброєння через власне виробництво та міжнародну допомогу; трансформація СБУ від економічних функцій до контррозвідувальних пріоритетів; розбудова розвідувальної спільноти з посиленням ГУР та СЗР. Попри значний прогрес, реформи залишаються незавершеними, особливо у сферах повної трансформації СБУ до стандартів демократичних служб безпеки, подолання корупційних ризиків, досягнення повної сумісності з НАТО.

6. Компаративний аналіз міжнародного досвіду інституціалізації управління національною безпекою в умовах гібридних конфліктів виявив спільні тенденції та кращі практики, релевантні для України. Моделі країн НАТО демонструють різноманітність організаційних рішень при спільних принципах демократичного цивільного контролю, інтегрованого підходу, розвинених координаційних механізмів. Особливо цінним є досвід країн Балтії (Естонії, Латвії, Литви), що першими зіткнулися з російською гібридною агресією та розробили ефективні механізми протидії: концепція комплексної оборони з залученням всього суспільства (Естонія); світове лідерство в

кібербезпеці з використанням блокчейн та X-Road (Естонія); активна протидія інформаційній агресії через Центр стратегічних комунікацій НАТО (Латвія); досягнення енергетичної незалежності через диверсифікацію та LNG термінал; програми соціальної інтеграції для зменшення вразливості до експлуатації етнічних розбіжностей. Інституційні інновації країн ЄС включають створення спеціалізованих центрів протидії гібридним загрозам, розвиток публічно-приватного партнерства в безпековій сфері, механізми швидкого впровадження технологічних інновацій. Адаптація цього досвіду до українського контексту з врахуванням специфіки триваючої війни може суттєво підвищити ефективність національної системи безпеки.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ ІНСТИТУЦІАЛІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

3.1. Концептуальна модель інституціалізації публічного управління національною безпекою в умовах гібридної війни

Побудова інтегрованої системи управління національною безпекою в умовах гібридної війни вимагає фундаментального переосмислення базових принципів організації безпекових інституцій, механізмів координації та процесів прийняття рішень. Досвід десятиліття протистояння гібридній агресії продемонстрував, що традиційні підходи до організації безпекового управління, засновані на жорсткому розмежуванні компетенцій та секторальній спеціалізації, виявляються недостатньо ефективними проти комплексних загроз, які одночасно діють у різних вимірах та експлуатують міжвідомчі розриви. Тому пропонується нова концептуальна модель інституціалізації публічного управління національною безпекою в умовах гібридної війни (рис. 3.1).

Рисунок 3.1 демонструє багаторівневу концептуальну модель інтегрованої системи управління національною безпекою, що складається з центрального ядра (інтегрована система управління), внутрішнього кільця базових принципів (системна цілісність, адаптивна архітектура, мережецентричність, інформаційна інтеграція, проактивність, розподілена стійкість, інклюзивність, континуальність), зовнішнього кільця архітектурних елементів (стратегічний, оперативний, регіональний рівні, аналітична платформа, інформаційно-аналітична підсистема, механізми прийняття рішень, ресурсне забезпечення, кадрова підсистема, мережевий компонент), а також чотирьох функціональних блоків: механізмів координації (вертикальна та горизонтальна координація, інформаційний, процедурний та ресурсний

механізми), системи моніторингу та оцінювання (збалансована система показників, автоматизований збір даних, системи обробки даних, оцінювання спроможностей, механізм зворотного зв'язку), механізмів адаптації до еволюції гібридних загроз (раннє виявлення слабких сигналів, сценарне прогнозування, організаційна та технологічна гнучкість, когнітивна адаптивність, механізм навчання) та контекстуального середовища гібридної війни.

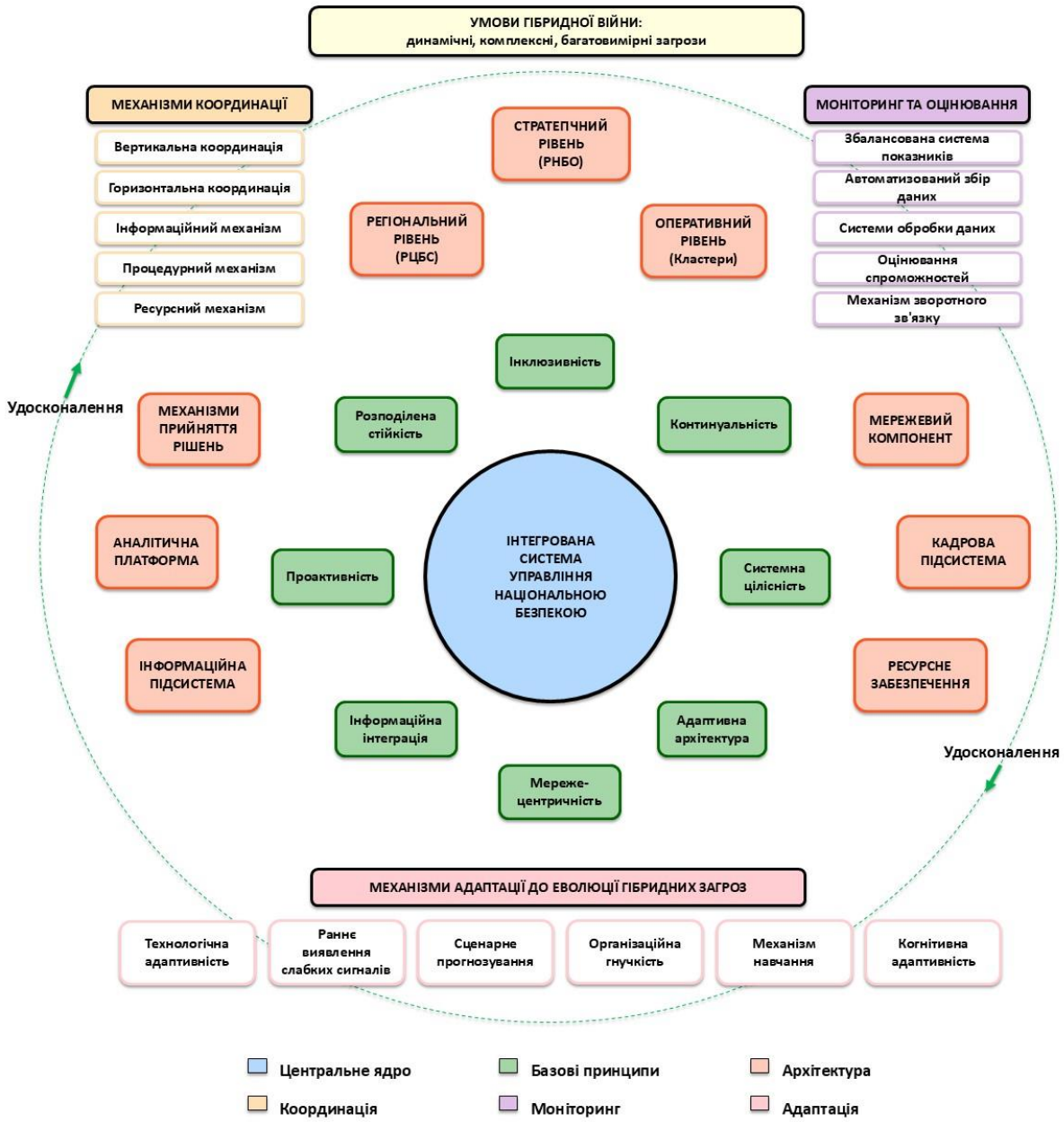

Рис. 3.1. Концептуальна модель інституціалізації публічного управління національною безпекою в умовах гібридної війни

Зелена пунктирна стрілка на рисунку символізує безперервне вдосконалення системи. Розглянемо докладніше складові та елементи даної моделі, починаючи з її **базових принципів**, кожен з яких має фундаментальне значення для формування цілісної системи управління національною безпекою в умовах гібридної війни.

Принцип системної цілісності постає наріжним каменем інтегрованої системи управління національною безпекою. На відміну від застарілого механістичного підходу, який примітивно розглядає безпекову систему як просту суму окремих компонентів, системна цілісність передбачає розуміння емерджентних властивостей, котрі виникають із взаємодії елементів і не можуть бути зведені до властивостей цих елементів окремо. Це означає, що ефективність системи визначається не лише якістю окремих інституцій, а насамперед характером зв'язків між ними, швидкістю обміну інформацією, синхронізацією дій, спільністю розуміння загроз та цілей. Практична реалізація цього принципу вимагає створення інституційних механізмів, котрі забезпечують не просту координацію паралельних дій різних відомств, а справді глибоку інтеграцію всіх зусиль на основі єдиного стратегічного бачення.

Принцип адаптивної архітектури відображає необхідність поєднання структурної стабільності з операційною гнучкістю. Інтегрована система має бути достатньо стійкою для забезпечення передбачуваності та надійності функціонування, але водночас здатною до швидкої реконфігурації відповідно до змін характеру загроз. Це досягається через модульну побудову системи, де базові функціональні модулі можуть об'єднуватися в різні конфігурації залежно від конкретних завдань. Створення постійного інституційного ядра, доповненого гнучкими тимчасовими структурами, дозволяє балансувати між стабільністю та адаптивністю без руйнування організаційної цілісності.

Мережецентричність як принцип організації передбачає перехід від ієрархічної піраміди до розподіленої мережі взаємопов'язаних вузлів. У контексті гібридних загроз, котрі часто мають децентралізований мережевий

характер, традиційні ієрархічні структури виявляються занадто повільними та ригідними через необхідність проходження інформації через численні бюрократичні інстанції. Мережева організація дозволяє забезпечити прямі зв'язки між елементами системи без непотрібних посередників, при цьому мережецентричність не означає повної відмови від ієрархії – вертикальні зв'язки зберігаються для стратегічного управління, але доповнюються горизонтальними для оперативної координації.

Принцип інформаційної інтеграції є критичним для ефективності управління в умовах інформаційної насиченості гібридної війни. Традиційна модель, за якої кожне відомство має власні закриті інформаційні системи, створює небезпечні «інформаційні силоси» та унеможливлює формування цілісної картини безпекової ситуації. Інформаційна інтеграція передбачає створення єдиного інформаційного простору з диференційованим доступом, де всі учасники системи можуть оперативно отримувати необхідну інформацію в реальному часі. Реалізація цього принципу вимагає не лише технічної сумісності інформаційних систем різних відомств, а й подолання глибоко вкоріненої відомчої монополії на інформацію через культурні та організаційні зміни.

Проактивність як принцип управління означає перехід від пасивного реагування на вже реалізовані загрози до їх завчасного виявлення та превенції. В умовах гібридної війни, де противник часто діє приховано та використовує тривалі підготовчі фази для створення сприятливих умов, реактивна модель управління неминуче призводить до постійного відставання від подій. Проактивність вимагає розвитку потужних прогностичних спроможностей, створення систем раннього попередження, формування механізмів виявлення слабких сигналів про зароджувані загрози. Це також означає готовність приймати рішення та діяти на основі неповної інформації та ймовірнісних оцінок, для чого необхідна висока толерантність керівництва до фундаментальної невизначеності.

Принцип розподіленої стійкості передбачає, що здатність системи

витримувати удари та швидко відновлюватися не концентрується в одному центральному вузлі, а розподіляється по всій системі через множину автономних елементів. Кожен елемент має власний запас міцності, альтернативні канали функціонування, внутрішні механізми самовідновлення після ушкоджень. Така архітектура набуває особливого значення в умовах гібридних атак, часто спрямованих саме на критичні централізовані вузли системи для її паралічу. Розподілена стійкість досягається через свідоме дублювання критичних функцій у різних елементах системи, створення резервних каналів управління, розвиток значних автономних спроможностей регіональних та галузевих компонентів, здатних ефективно функціонувати навіть за тимчасової втрати зв'язку з центром [23].

Інклюзивність як принцип передбачає залучення до системи управління національною безпекою не лише традиційних силових структур, а й широкого кола інших державних органів, приватного сектору, організацій громадянського суспільства. Оскільки гібридні загрози спрямовані на все суспільство в цілому та атакують одночасно в різних сферах від економіки до культури, відповідь також має бути загальносуспільною з мобілізацією всіх доступних ресурсів. Це вимагає створення ефективних механізмів партнерства, котрі дозволяють використовувати унікальні ресурси та компетенції недержавних акторів при обов'язковому збереженні державного контролю над критичними функціями застосування сили. Особливо важливим є залучення технологічного сектору з його інноваційним потенціалом, медіа як каналів стратегічних комунікацій, освітніх інституцій для формування суспільної стійкості.

Принцип континуальності управління відображає розуміння того фундаментального факту, що в умовах тривалої гібридної війни не існує чіткої фіксованої межі між станом миру та війни, між нормальним повсякденним та кризовим надзвичайним станом функціонування держави. Система управління має ефективно функціонувати в усьому широкому спектрі станів – від відносного спокою до гострої екзистенційної кризи – без необхідності

фундаментальної перебудови при кожному переході. Це досягається через створення масштабованих механізмів управління, котрі можуть плавно нарощувати інтенсивність діяльності та обсяг залучених ресурсів без структурної трансформації. Наявність «сплячих» резервних елементів системи, які можуть бути швидко активовані за потреби, дозволяє підтримувати постійну готовність без надмірного виснаження обмежених людських та фінансових ресурсів у спокійні періоди.

Технологічна інноваційність як принцип визнає критичну роль передових технологій у забезпеченні конкурентних переваг над противником у довгостроковій перспективі. Штучний інтелект для аналізу величезних масивів даних, аналітика великих даних для виявлення прихованих патернів, квантові технології для захищених комунікацій, блокчейн для забезпечення цілісності критичної інформації – всі ці та інші технології створюють принципово нові можливості для інтеграції управління, прогнозування еволюції загроз, надійного захисту інформації, ефективної координації розподілених дій. При цьому технології розглядаються не як самоціль або данина моді, а виключно як практичні інструменти реалізації інших фундаментальних принципів системи – інтеграції, проактивності, стійкості. Створення ефективних механізмів швидкого впровадження перевірених інновацій, безпечного експериментування з новими підходами, масштабування успішних пілотних рішень на всю систему стає критичним фактором довгострокової ефективності в технологічній гонці з противником.

Принцип стратегічної комунікації передбачає розуміння того, що управління національною безпекою в сучасних умовах включає не лише традиційні фізичні дії силових структур, а й цілеспрямоване формування сприятливого інформаційного середовища, переконливих наративів, широкої суспільної підтримки безпекової політики держави. В умовах гібридної війни, де боротьба за уми та серця населення є не менш, а часом навіть більш важливою за власне військові дії на полі бою, стратегічні комунікації перетворюються з допоміжної функції на інтегральну невід’ємну частину

всього процесу управління національною безпекою. Це вимагає тісної синхронізації публічних меседжів різних безпекових відомств для уникнення суперечностей, проактивного формування інформаційного порядку денного замість пасивного реагування, максимально швидкого спростування ворожої дезінформації до її масового поширення [54].

Правова легітимність як принцип підкреслює критично важливий факт, що навіть в екстремальних умовах екзистенційних загроз самому існуванню держави система управління національною безпекою має неухильно діяти в межах правового поля та конституційних норм. Це створює складний практичний баланс між операційною ефективністю, яка часом вимагає швидких нестандартних рішень, та безумовною законністю всіх дій, між гострою необхідністю швидких рішень у динамічних кризових ситуаціях та обов'язковим дотриманням встановлених демократичних процедур. Розробка спеціальних правових механізмів, максимально адекватних специфіці гібридних загроз, включаючи гнучкі режими підвищеної готовності з розширеними повноваженнями, спрощені прискорені процедури прийняття рішень для справді кризових ситуацій, механізми пост-фактум легалізації екстрених рішень через парламентський контроль, дозволяє зберегти фундаментальний правовий характер демократичної держави без критичної втрати оперативної ефективності в протидії загрозам.

Принцип безперервного навчання визнає об'єктивний факт, що в надзвичайно динамічному середовищі гібридної війни з постійною еволюцією тактик та технологій жодна система управління не може бути ідеально досконалою з першого разу та назавжди. Механізми систематичного вивчення практичних уроків з реальних операцій, глибокого аналізу помилок та невдач, активного поширення виявлених кращих практик між різними підрозділами, планомірної адаптації застарілих процедур на основі накопиченого досвіду мають бути органічно вбудовані в саму структуру системи як невід'ємний елемент повсякденного функціонування. Це включає проведення регулярних всебічних оглядів ефективності діяльності всієї системи, організацію

незалежних зовнішніх аудитів для об’єктивної оцінки, створення ефективних механізмів зворотного зв’язку від операційного рівня безпосередніх виконавців до стратегічного рівня вищого керівництва. При цьому формування прогресивної організаційної культури, яка щиро заохочує відповідальне експериментування з новими підходами та конструктивно визнає неминучі помилки як цінне джерело організаційного навчання замість їх приховування, стає критично важливою передумовою довгострокової ефективності системи через її здатність до самовдосконалення.

Економічна ефективність як принцип визнає об’єктивну обмеженість доступних державних ресурсів навіть в умовах війни та гостру необхідність їх максимально оптимального використання для досягнення безпекових цілей. Глибока інтеграція управління об’єктивно дозволяє уникнути марнотратного дублювання однакових функцій у різних відомствах, досягти суттєвої економії масштабу через консолідацію закупівель та сервісів, значно оптимізувати використання дефіцитних специфічних ресурсів через їх спільне використання. Практичні механізми спільного стратегічного планування потреб, консолідованих централізованих закупівель для всього сектору безпеки, створення розподілених спільних сервісів для забезпечуючих допоміжних функцій можуть радикально підвищити загальну ефективність безпекових видатків бюджету. При цьому критично важливо розуміти, що економія державних коштів ніколи не повинна досягатися за рахунок деградації критичних оперативних спроможностей системи – принцип достатності наявних спроможностей для виконання місії має безумовно превалювати над абстрактною мінімізацією поточних витрат.

Таким чином, як переконливо демонструє наведене вище, архітектура інституційної моделі безпекового управління в специфічних умовах гібридної війни об’єктивно представляє собою надзвичайно складну багаторівневу та багатовимірну конструкцію, котра має органічно забезпечувати ефективну інтеграцію принципово різнорідних компонентів всієї системи національної безпеки при обов’язковому збереженні їх функціональної спеціалізації в

конкретних доменах та необхідної операційної автономії в повсякденній діяльності. Проектування такої складної архітектури неминуче вимагає ретельного урахування специфічних особливостей гібридних загроз з їх багатовимірністю, унікальних національних особливостей України з її історією та культурою, реально наявних обмежених ресурсів та існуючих інституційних обмежень, а також адаптації кращих міжнародних практик розвинених демократичних країн до специфічного українського контексту.

Стратегічний рівень запропонованої архітектури логічно формується навколо Ради національної безпеки і оборони України як центрального координаційного органу. Нова модель передбачає створення при РНБО постійно діючого Стратегічного комітету з планування та координації безпекової політики, до складу якого входять керівники всіх ключових безпекових відомств, котрий забезпечує життєво необхідну безперервність стратегічного управління між періодичними засіданнями повного складу Ради. Паралельно з цим Інтегрований аналітичний центр при РНБО має системно консолідувати розвідувальну, аналітичну та прогностичну інформацію з усіх можливих джерел незалежно від їх відомчої приналежності для формування єдиної несуперечливої картини безпекового середовища, необхідної для обґрунтованого прийняття стратегічних рішень вищим політичним керівництвом держави.

Оперативний рівень архітектури раціонально будується на інноваційному принципі функціональних кластерів, кожен з яких організаційно об’єднує відомства та структури зі спорідненими близькими функціями під єдиним оперативним керівництвом для максимальної координації та синергії. Військовий кластер під загальним керівництвом Міністерства оборони оперативно інтегрує Збройні Сили України, Національну гвардію, Державну прикордонну службу в частині їх безпосереднього бойового застосування проти зовнішнього противника. Кластер внутрішньої безпеки під координаційною егідою Міністерства внутрішніх справ об’єднує правоохоронні функції різних структур,

забезпечення громадського порядку, організацію цивільного захисту населення. Розвідувальний кластер системно об’єднує всі спеціалізовані розвідувальні служби держави під стратегічною координацією Головного управління розвідки для уникнення дублювання зусиль. Кібербезпековий кластер консолідує розпорошені зусилля Держспецзв’язку, кіберпідрозділів різних силових відомств під єдиним оперативним командуванням. Така кластерна організація дозволяє оптимально зберегти необхідну функціональну спеціалізацію різних структур при одночасному забезпеченні їх ефективної координації в рамках кластерів.

Інноваційним елементом запропонованої архітектури є створення принципово нового Національного центру стійкості як міжвідомчої координаційної структури, безпосередньо відповідальної за забезпечення безперебійного функціонування об’єктів критичної інфраструктури держави, ефективну координацію різноманітних заходів цивільного захисту населення, професійне управління кризовими ситуаціями невоєнного характеру від природних катастроф до техногенних аварій. Центр має організаційно інтегрувати координовані зусилля профільних міністерств з вузькою спеціалізацією (енергетики, транспортної інфраструктури, охорони здоров’я населення), регіональних державних адміністрацій з їх знанням місцевої специфіки, приватних операторів критичної інфраструктури з їх технічною експертизою. Його ключовим завданням є не пряме оперативне управління всіма об’єктами, а саме стратегічна координація зусиль різних акторів, систематичний моніторинг критичних вразливостей системи, професійна розробка детальних планів забезпечення безперервності функціонування, регулярне проведення практичних навчань та реалістичних симуляцій кризових сценаріїв.

Регіональний рівень архітектури передбачає створення мережі Регіональних центрів безпеки та стійкості як інтегрованих міжвідомчих структур на обласному рівні, котрі об’єднують постійних представників усіх ключових безпекових відомств для координації на місцях. Ці центри

функціонують як регіональні координаційні хаби всієї системи, практично забезпечуючи оперативну координацію дій різних структур на місцях, систематичний моніторинг специфічних регіональних загроз, професійне управління територіальною обороною області, ефективну взаємодію з обласною владою та місцевою громадськістю. Важливою особливістю їх організації є подвійне підпорядкування – вертикальне центральним органам влади в Києві для забезпечення єдності політики та горизонтальне обласним адміністраціям для врахування регіональної специфіки, що дозволяє оптимально балансувати між необхідним централізованим стратегічним управлінням та доцільною регіональною автономією в оперативних питаннях.

Критично важливий **мережевий компонент** архітектури представлений розгалуженою системою множинних горизонтальних зв'язків між різними елементами системи на різних рівнях ієрархії та у різних функціональних кластерах для подолання відомчої роз'єднаності. Створення Єдиної захищеної телекомунікаційної мережі сектору безпеки і оборони з сучасним шифруванням забезпечує надійну технічну основу для безперешкодного обміну критичною інформацією між усіма учасниками. Паралельно численні міжвідомчі робочі групи з конкретних актуальних питань (протидія організованій дезінформації, комплексний захист критичної інфраструктури, координована протидія гібридним загрозам) формують гнучкі неформальні механізми оперативної координації без зайвої бюрократії. Нарешті, інноваційна система постійних взаємних представників між ключовими безпековими структурами забезпечує швидку неформальну координацію повсякденних питань без бюрократичних затримок на офіційні запити.

Інформаційна підсистема архітектури базується на прогресивній концепції «єдиного інформаційного простору» всього безпекового сектору з диференційованим рольовим доступом залежно від функціональних потреб. Національна платформа безпекових даних технологічно інтегрує розпорошені інформаційні системи всіх безпекових відомств через уніфіковані інтерфейси, практично забезпечуючи технічну можливість комплексного міжвідомчого

аналізу даних з різних джерел. Паралельно система розподілених ситуаційних центрів, надійно пов’язаних в єдину координовану мережу, забезпечує якісну візуалізацію актуальної оперативної обстановки на всіх рівнях управління від національного до регіонального. Нарешті, широке використання передових технологій штучного інтелекту для автоматизованої обробки величезних масивів даних, своєчасного виявлення статистичних аномалій, імовірнісного прогнозування можливого розвитку ситуації суттєво підвищує загальну якість інформаційно-аналітичного забезпечення процесу прийняття управлінських рішень на всіх рівнях [40].

Складний **механізм прийняття рішень** в новій архітектурі раціонально базується на комбінованому принципі «розподіленого консенсусу» для стратегічних питань довгострокового характеру та «делегованої автономії» для поточних оперативних питань. Стратегічні рішення з довгостроковими наслідками обов’язково приймаються колегіально в рамках засідань РНБО або спеціалізованих профільних комітетів з попереднім ретельним аналізом можливих альтернатив та комплексною оцінкою пов’язаних ризиків. Натомість поточні оперативні рішення тактичного характеру свідомо делегуються на найнижчий компетентний рівень управління з наступним обов’язковим інформуванням вищих інстанцій для контролю. При цьому чітка система «червоних ліній» однозначно визначає критерії, за яких рішення обов’язково потребують попереднього узгодження на вищому рівні, а які можуть прийматися автономно нижчими рівнями в межах їх компетенції.

Ресурсне забезпечення в рамках нової архітектури передбачає стратегічний перехід від традиційного відомчого принципу виділення коштів до програмно-цільового фінансування за пріоритетами. Консолідований бюджет всього сектору безпеки і оборони має розподілятися не за формальною відомчою належністю структур-отримувачів, а за цільовими міжвідомчими програмами розвитку конкретних спроможностей незалежно від того, які відомства їх реалізують. Створення спеціалізованої Агенції оборонних закупівель як єдиного професійного закупівельного центру для всього сектору

дозволяє досягти суттєвої економії масштабу та надійно уникнути дублювання аналогічних закупівель різними відомствами. Нарешті, механізм гнучкого оперативного перерозподілу бюджетних ресурсів між програмами залежно від зміни стратегічних пріоритетів та актуальних загроз значно підвищує адаптивність всієї системи до непередбачуваних змін.

Кадрова підсистема архітектури передбачає створення єдиного кадрового резерву всього сектору безпеки і оборони з практичною можливістю як горизонтальної мобільності персоналу між різними відомствами на одному рівні, так і вертикальної мобільності між рівнями управління. Уніфікація базової загальної підготовки для співробітників всіх безпекових структур незалежно від відомчої приналежності з подальшою обов'язковою вузькою спеціалізацією за профілем діяльності цілеспрямовано створює єдину професійну корпоративну культуру безпекового співтовариства. Паралельно запроваджувана система обов'язкової періодичної ротації керівних кадрів між різними відомствами розвиває цінне міжвідомче розуміння специфіки роботи партнерів та формує неформальні міжособистісні зв'язки між керівниками. Нарешті, створення міжвідомчого навчального центру вищого рівня забезпечує систематичну підготовку нової генерації безпекових менеджерів з необхідним системним стратегічним мисленням замість вузького відомчого підходу.

Важливі **механізми контролю та підзвітності** органічно вбудовані в архітектуру на абсолютно всіх рівнях для запобігання зловживанням та забезпечення ефективності. Парламентський демократичний контроль професійно здійснюється через спеціалізований профільний комітет Верховної Ради з істотно розширеними порівняно з нинішніми повноваженнями доступу до секретної інформації для обізнаного контролю. Громадський контроль з боку активного суспільства практично реалізується через створену Громадську раду при РНБО на національному рівні та мережу регіональних громадських рад безпеки в областях. Система внутрішнього професійного аудиту з централізованою Службою інспекції всього сектору

безпеки систематично забезпечує дотримання встановлених процедур та ефективність використання виділених ресурсів. Нарешті, механізм періодичної незалежної зовнішньої оцінки ефективності системи із обов'язковим залученням авторитетних міжнародних експертів з багатим досвідом об'єктивно забезпечує неупередженість оцінок.

Сучасна технологічна платформа архітектури базується на прогресивних принципах хмарних розподілених обчислень, котрі дозволяють гнучке масштабування потужностей та надійне географічне резервування критичних даних. Використання інноваційних блокчейн-технологій для зберігання найбільш критичних даних гарантує їх повну незмінність та прозору відстежуваність всіх операцій. Системи штучного інтелекту різного призначення органічно інтегровані на всіх рівнях управління для ефективної підтримки прийняття обґрунтованих рішень. Квантово-захищені канали зв'язку з теоретично недосяжним рівнем безпеки гарантують абсолютну конфіденційність найбільш чутливих стратегічних комунікацій. Нарешті, цифрові двійники всіх об'єктів критичної інфраструктури дозволяють безпечно моделювати наслідки різноманітних атак та систематично відпрацьовувати ефективні контрзаходи без ризику для реальних об'єктів.

Динамічна природа гібридних загроз, їх постійна еволюція та здатність до швидкої трансформації вимагають від системи національної безпеки не просто ефективних механізмів протидії існуючим викликам, а розвинених **адаптаційних механізмів**, що забезпечують випереджувальне пристосування до майбутніх, ще не проявлених форм агресії. Створення таких механізмів передбачає фундаментальний перехід від реактивної до проактивної парадигми безпекового управління, де система не лише реагує на зміни, а активно формує умови, що ускладнюють реалізацію гібридних стратегій противника.

Концептуальною основою адаптаційних механізмів є розуміння коеволюційної динаміки між системою національної безпеки та гібридними загрозами. Кожна дія захисту породжує контрдію нападу, кожне

вдосконалення оборонних механізмів стимулює пошук нових вразливостей. Ця діалектика вимагає від системи не просто високої швидкості реакції, а здатності до антиципації – передбачення напрямків еволюції загроз та завчасної підготовки контрзаходів. Модель «адаптивного циклу» включає фази моніторингу змін, аналізу трендів, прогнозування сценаріїв, розробки превентивних заходів, тестування та впровадження [218].

Система раннього виявлення слабких сигналів про еволюцію загроз базується на концепції «периферійного зору» організації. Традиційні системи моніторингу фокусуються на відомих типах загроз та встановлених індикаторах, натомість адаптивна система шукає аномалії, незвичайні патерни, слабкі сигнали, що можуть вказувати на формування нових типів загроз. При цьому використання методів аналітики великих даних дозволяє обробляти величезні масиви неструктурованої інформації з відкритих джерел - соціальних мереж, форумів, наукових публікацій - для виявлення ранніх ознак нових гібридних тактик. У свою чергу, механізм сценарного прогнозування еволюції загроз поєднує експертні методи з комп'ютерним моделюванням. Регулярні стратегічні форсайт-сесії залучають не лише безпекових експертів, а й футурологів, технологів, соціологів для вироблення альтернативних сценаріїв розвитку гібридних загроз, що дозволяє симулювати поведінку противника в різних умовах та тестувати його можливі адаптації до наших контрзаходів.

Організаційна гнучкість як ключовий адаптаційний механізм реалізується через модульну архітектуру безпекових структур, коли замість жорстких організаційних форм створюються адаптивні модулі, що можуть швидко переконфігуруватися для протидії новим типам загроз. В рамках цього механізм «швидкого прототипування» організаційних рішень дозволяє тестувати нові структури та процеси в обмеженому масштабі перед повномасштабним впровадженням, а «інноваційні лабораторії» в рамках безпекових структур мають мандат на експериментування з новими підходами без обмежень традиційних бюрократичних процедур.

Технологічна адаптивність забезпечується через створення «технологічного радару» – системи постійного моніторингу нових технологій, що можуть бути використані як для створення нових загроз, так і для протидії їм. Впроваджуваний при цьому механізм «швидкого впровадження» дозволяє тестувати та інтегрувати нові технології в операційну діяльність за тижні, а не роки, а створення власних дослідницьких центрів з фокусом на технології подвійного призначення забезпечує технологічну автономію.

Когнітивна адаптивність системи реалізується через механізми подолання ментальних моделей та когнітивних упереджень, що заважають розпізнавати нові типи загроз. Так, програми «когнітивної різноманітності» забезпечують залучення людей з різним бекграундом, досвідом, способом мислення до аналізу загроз, «ігри з альтернативними реальностями» тренують здатність мислити поза усталеними рамками та уявляти неочікувані сценарії. Важливим тут є також впровадження механізму навчання та еволюції системи, що перетворює кожен інцидент та кризу на джерело вдосконалення, створюючи «адаптивні цикли навчання», які включають не лише аналіз минулого досвіду, а й екстраполяцію уроків на майбутні сценарії.

Нарешті, метаадаптивність, тобто здатність адаптувати самі механізми адаптації, забезпечує стійкість системи в довгостроковій перспективі, що передбачає регулярний перегляд адаптаційних механізмів на предмет їх ефективності; моніторинг швидкості та якості адаптацій; бенчмаркінг з іншими адаптивними системами, не обов’язково безпековими; експерименти з новими формами адаптивності. Таким чином, система може не лише адаптуватися до загроз, а й постійно вдосконалювати свою здатність до адаптації, створюючи позитивну спіраль еволюції.

У цілому, фундаментальна еволюційність архітектури свідомо закладена через спеціальні механізми регулярного критичного перегляду та планомірної адаптації до змін. Щорічні всебічні стратегічні огляди системно оцінюють адекватність існуючої архітектури новим викликам та загрозам. Обмежені пілотні проекти дозволяють безпечно тестувати перспективні інноваційні

організаційні рішення перед ризикованим повномасштабним впровадженням на всю систему. Продуманий механізм «сплячих елементів» дозволяє швидко активувати додаткові резервні компоненти системи в гострих кризових ситуаціях без попередньої підготовки. Нарешті, послідовна модульність всієї архітектури технічно забезпечує практичну можливість органічного додавання принципово нових елементів у майбутньому без руйнування та перебудови вже існуючої працюючої структури, що критично важливо для еволюційного розвитку.

3.2. Правові механізми удосконалення системи публічного управління національною безпекою

Модернізація законодавчої бази у сфері національної безпеки України в умовах гібридної війни становить фундаментальне завдання, від вирішення якого залежить правова легітимність та ефективність всіх інших реформ безпекового сектору, оскільки саме законодавство створює юридичний каркас, в межах якого функціонують інституції, реалізуються повноваження та здійснюється координація зусиль різних суб’єктів забезпечення національної безпеки. Досвід десятиліття протистояння гібридній агресії переконливо виявив численні прогалини, суперечності та неузгодженості в чинному законодавстві, що створюють системні перешкоди для адекватного, своєчасного реагування на комплексні, багатовекторні загрози, ефективної координації діяльності різноманітних безпекових інституцій та забезпечення необхідного, але складного балансу між безпековими імперативами захисту держави та фундаментальними демократичними цінностями прав людини і верховенства права. Отже, комплексна модернізація законодавчої бази вимагає не просто точкових, косметичних змін до окремих законодавчих актів, що не усувають системних проблем, а глибокого системного переосмислення всієї багаторівневої архітектури безпекового законодавства, здатної адекватно

відповідати динамічним викликам сучасного турбулентного безпекового середовища та забезпечувати міцні правові основи для ефективної, координованої протидії багатовимірним гібридним загрозам, що постійно еволюціонують та набувають нових форм.

Концептуальною основою такої глибокої модернізації має стати парадигмальний перехід від фрагментарного, мозаїчного до принципово інтегрованого, системного підходу в правовому регулюванні національної безпеки, що передбачає послідовне подолання мозаїчності, безсистемності та внутрішньої суперечливості чинної нормативної бази, яка формувалася десятиліттями без достатньої координації. Чинне законодавство у сфері національної безпеки об'єктивно формувалося протягом десятиліть незалежності як строката, неоднорідна сукупність окремих, часто слабко узгоджених між собою законів, що регулюють діяльність конкретних відомств або вузькі сфери безпекової діяльності, без достатньої уваги законодавця до забезпечення узгодженості між різними правовими актами, термінологічної єдності понятійного апарату та цілісності правового поля.

Така еволюційна логіка розвитку законодавства неминуче призвела до численних змістовних неузгодженостей між різними законами, непродуктивного дублювання компетенцій різних органів, критичних прогалин на стиках відповідальності різних суб'єктів безпеки, а також термінологічної неоднорідності, коли одні й ті самі базові поняття трактуються по-різному, іноді навіть суперечливо в різних законодавчих актах, що створює правову невизначеність. Новий, принципово інтегрований підхід, що має замінити фрагментарний, передбачає цілеспрямоване, послідовне створення внутрішньо узгодженої, несуперечливої цілісної правової системи, де базовий рамковий закон про національну безпеку чітко визначає загальні принципи функціонування всієї системи, єдиний понятійний апарат з вичерпними дефініціями ключових термінів, інституційну архітектуру сектору безпеки та фундаментальні механізми його функціонування, а численні галузеві, спеціалізовані закони систематично

деталізують ці рамкові положення для конкретних сфер безпекової діяльності з їх специфікою, забезпечуючи при цьому сувору узгодженість термінології, процедур та механізмів координації на всіх рівнях правового регулювання [1].

Практична реалізація такого інтегрованого підходу може бути найефективніше досягнута через масштабну кодифікацію всього безпекового законодавства шляхом розробки, громадського обговорення та прийняття комплексного Кодексу національної безпеки України, який стане системним, концептуальним рішенням накопиченої проблеми правової фрагментації та забезпечить вичерпне комплексне регулювання практично всіх істотних аспектів забезпечення національної безпеки держави і суспільства.

Такий кодифікований акт має органічно консолідувати, систематизувати та узгодити численні норми, що наразі розпорошені в десятках законів та сотнях підзаконних актів і регулюють всі ключові аспекти забезпечення національної безпеки від стратегічного довгострокового планування до оперативної повсякденної діяльності безпекових органів, від функціонування системи в умовах мирного часу до застосування різноманітних особливих правових режимів в умовах криз, від внутрішніх механізмів координації до багатогранного міжнародного співробітництва в безпековій сфері. Внутрішня структура такого кодексу має бути побудована за класичним принципом від загального до конкретного, від абстрактного до конкретного та логічно включатиме наступні основні змістовні розділи:

загальні положення, що визначають фундаментальні принципи забезпечення національної безпеки як діяльності держави і суспільства, основні дефініції всіх ключових понять для забезпечення термінологічної єдності, вичерпний перелік суб’єктів та об’єктів національної безпеки з їх характеристиками;

система забезпечення національної безпеки, що деталізує інституційну архітектуру сектору безпеки, функціональний розподіл повноважень між різними державними органами, механізми їх взаємодії та координації;

процедурні механізми, що детально регламентують ключові процеси

стратегічного та оперативного планування, координації діяльності різних суб'єктів, прийняття управлінських рішень на різних рівнях, звітування про результати діяльності та багаторівневого контролю за діяльністю безпекових структур;

особливі правові режими, включаючи вичерпне детальне регулювання воєнного стану, надзвичайного стану, режиму підвищеної готовності з чіткими правовими підставами їх введення, процедурами прийняття рішень, межами можливих обмежень прав людини та гарантіями дотримання базових прав навіть в екстремальних умовах;

міжнародне співробітництво у сфері безпеки з урахуванням міжнародних зобов'язань України в рамках євроатлантичної інтеграції та участі в міжнародних організаціях;

юридична відповідальність за порушення законодавства про національну безпеку з диференціацією санкцій залежно від характеру та тяжкості порушень.

Водночас сама по собі кодифікація як суто технічна систематизація існуючих норм не вирішить всіх глибинних проблем без змістовної адаптації самого законодавства до якісно нової специфіки гібридних загроз, що вимагає введення в правове поле принципово нових правових концепцій, інститутів та механізмів, здатних адекватно, без спотворень відображати складні реалії сучасного безпекового середовища з його специфікою. Передусім поняття «гібридна агресія» як центральна категорія має отримати чітке, юридично точне правове визначення з максимально вичерпним, але водночас достатньо гнучким для адаптації до нових форм загроз переліком конкретних дій, які кваліфікуються законом як прояви гібридної агресії, що має охоплювати весь широкий спектр від руйнівних кібератак на критичну державну та комерційну інфраструктуру до багатоформного економічного тиску через торговельні обмеження, санкції, блокування транзиту, від масштабних інформаційних операцій з метою дестабілізації суспільства та підриву довіри до влади до прихованого використання проксі-сил, іррегулярних збройних формувань та

найманців.

Не менш важливим є законодавче введення якісно нового правового режиму «гібридної оборони» як проміжного стану між звичайним мирним часом та повноцінним воєнним станом, що дозволить застосовувати розширені, посилені безпекові заходи, об'єктивно необхідні для ефективної протидії багатовекторним гібридним загрозам, без формального введення повноцінного воєнного стану з його масштабними обмеженнями конституційних прав громадян та серйозними економічними наслідками для функціонування держави.

Сучасна концепція «критичної інформаційної інфраструктури» має законодавчо розширити традиційну сферу правового захисту далеко за межі звичних фізичних матеріальних об'єктів, охоплюючи віртуальні інформаційні системи, критично важливі бази даних, телекомунікаційні мережі та цифрові сервіси, від безперебійного функціонування яких об'єктивно залежить нормальна життєдіяльність сучасної держави та суспільства. Процедурний механізм «швидкого правового реагування» повинен на законодавчому рівні дозволити компетентним органам виконавчої влади оперативно адаптувати детальні правові норми до раптово виникаючих нових типів загроз через спрощені процедури внесення змін до підзаконних нормативних актів при обов'язковому збереженні парламентського демократичного контролю над принципово важливими, фундаментальними питаннями безпекової політики.

Особливо важливим, можливо найбільш проблемним аспектом модернізації законодавства є створення дійсно ефективного, а не декларативного правового забезпечення міжвідомчої координації, оскільки саме хронічна відсутність дієвих, обов'язкових для виконання механізмів координації об'єктивно залишається однією з найбільших, найболючіших структурних вад всієї чинної системи управління національною безпекою України. Правове забезпечення координації має системно подолати глибоко вкорінену традиційну відомчу замкненість, егоїзм через чітке законодавче закріплення обов'язкового, імперативного характеру рішень спеціально

створених координаційних органів для всіх без винятку суб'єктів сектору безпеки з чітким, недвозначним визначенням юридичних наслідків їх невиконання або ігнорування, що має остаточно усунути поширену нині ситуацію, коли координаційні рішення залишаються суто рекомендаційними за своєю природою та систематично ігноруються окремими відомствами, що керуються вузьковідомчими інтересами.

Законодавче встановлення персональної дисциплінарної та адміністративної відповідальності вищих керівників безпекових структур за систематичне невиконання обов'язкових координаційних рішень або неналежну, формальну взаємодію з іншими суб'єктами безпеки має створити потужні правові стимули для конструктивної міжвідомчої кооперації замість деструктивної конкуренції. А процедури ефективного, швидкого вирішення неминучих міжвідомчих конфліктів, суперечок через обов'язковий арбітраж Ради національної безпеки і оборони України з імперативним характером її арбітражних рішень для сторін конфлікту мають стати цивілізованою, правовою альтернативою затяжним, виснажливим бюрократичним суперечкам між відомствами.

У свою чергу, створення міцної правової бази для ефективного функціонування тимчасових міжвідомчих оперативних груп, створюваних ad hoc для вирішення конкретних завдань, з особливим юридичним статусом, що дозволяє їм діяти поза звичайними жорсткими відомчими ієрархіями, та спеціальними повноваженнями, включаючи прямий доступ до необхідних ресурсів усіх залучених до операції відомств, дозволить оперативно формувати високоефективні ad hoc структури для вирішення нестандартних конкретних завдань без довготривалих бюрократичних процедур.

Паралельно з удосконаленням правових координаційних механізмів об'єктивно необхідна глибока, всебічна модернізація законодавства про розвідувальну діяльність, яке має максимально повно врахувати якісно нові реалії інформаційної епохи та специфічні особливості гібридних загроз, що фундаментально трансформували як об'єкти розвідувальної зацікавленості,

так і методи, засоби ведення розвідувальної роботи порівняно з традиційними уявленнями. Законодавче розширення предмету, об’єктів розвідувальної діяльності на принципово нові сфери, що набули критичного значення для забезпечення національної безпеки в сучасних умовах, зокрема кіберпростір з його специфічними віртуальними загрозами, інформаційне середовище з його могутніми маніпулятивними впливами на масову свідомість, глобальні та регіональні економічні процеси з їх все частішим використанням як інструментів гібридної агресії, має отримати чітке, недвозначне правове закріплення з одночасним визначенням розумних меж дозволеного втручання розвідувальних органів для збереження балансу з правами людини.

Повна легалізація широкого використання даних з відкритих публічних джерел, так звана розвідка за відкритими джерелами (OSINT - Open Source Intelligence) як повноцінного, рівноправного виду розвідувальної діяльності поряд з традиційною агентурною та технічною розвідкою з відповідними процедурами систематичного збору, професійної обробки та відповідального використання таких даних адекватно відповідає сучасним технологічним реаліям, коли величезні обсяги стратегічно цінної інформації об’єктивно доступні публічно в інтернеті і потребують лише професійного аналітичного опрацювання кваліфікованими фахівцями. Надійні процедурні механізми ефективного захисту конфіденційних джерел інформації та секретних методів розвідувальної діяльності при вимушеному використанні розвідувальної інформації в публічних судових процесах або відкритому політичному дискурсі повинні забезпечувати складний баланс між потребою в доказовій базі для правосуддя та критичною необхідністю збереження операційної ефективності розвідувальних служб через захист їх джерел та методів від розкриття [55].

Не менш важливим стратегічним напрямом правової модернізації є комплексне законодавче забезпечення кібербезпеки держави і суспільства, де фрагментарність, неповнота чинного розпорошеного регулювання створює критичні, небезпечні вразливості в умовах, коли віртуальний кіберпростір

об’єктивно перетворився на повноцінний, дуже активний театр гібридної війни з щоденними атаками. Комплексний, всеосяжний базовий закон про кібербезпеку має системно визначити не лише суто технічні аспекти технологічного захисту інформаційних систем, комп’ютерних мереж та даних від несанкціонованого доступу, а й надзвичайно важливі організаційні механізми ефективної координації дій різноманітних суб’єктів забезпечення кібербезпеки, абсолютно чіткий функціональний розподіл відповідальності між численними державними органами різної підпорядкованості, приватним бізнес-сектором як власником більшості критичної інфраструктури та кінцевими користувачами систем, детальні процедури своєчасного виявлення кіберінцидентів, ефективного реагування на них та професійного розслідування з визначенням конкретних термінів виконання дій та персональних обов’язків різних учасників процесу.

Своєчасна криміналізація нових, раніше невідомих типів кіберзлочинів, що масово з’явилися в останні роки і становлять серйозну загрозу, включаючи ransomware-атаки (атаки програм-вимагачів, шифрувальників) з шифруванням критично важливих даних та вимаганням викупу за розшифрування, створення та масове поширення deepfake-контенту (синтетичних реалістичних медіафайлів) з метою масштабної дезінформації населення або витонченого шахрайства, цілеспрямовані руйнівні атаки на стратегічні об’єкти критичної інфраструктури через вразливості промислових систем управління, має встановити адекватну масштабам загрози кримінальну відповідальність з урахуванням потенційної величезної шкоди суспільству.

Правові механізми оперативного, майже миттєвого блокування виявленого шкідливого контенту в мережі інтернет, включаючи фішингові шахрайські сайти, джерела активного поширення зловмисного програмного забезпечення, платформи координації кібератак на українські цілі, мають забезпечувати необхідний для безпеки баланс між ефективним захистом національної кібербезпеки та фундаментальним збереженням свободи інтернету, старанно уникаючи надмірної цензури та необґрунтованих

блокувань. Поряд з цим, встановлення обов'язкових, юридично закріплених вимог кібергігієни (базових практик забезпечення кібербезпеки) для всіх без винятку об'єктів критичної інфраструктури держави з встановленням конкретних, технічно обґрунтованих стандартів технічного захисту, обов'язкового регулярного незалежного аудиту стану захищеності, термінової звітності про всі значні інциденти та персональної відповідальності вищих керівників організацій за систематичне недотримання стандартів створять потужні правові стимули для проактивного, превентивного захисту замість реактивного реагування.

Паралельно з регулюванням кібербезпеки об'єктивно необхідно врегулювати тісно пов'язане, але якісно окреме правове регулювання інформаційної безпеки в широкому сенсі, яке об'єктивно залишається найбільш контроверсійною, дискусійною сферою через фундаментальну об'єктивну необхідність надзвичайно делікатного балансування між нагальною потребою ефективної протидії масованій дезінформації як ключовому елементу гібридної агресії проти свідомості громадян та абсолютною непорушністю фундаментальної конституційної свободи слова, свободи медіа як наріжного каменя будь-якої демократії.

Визначення максимально юридично точних, однозначних критеріїв розмежування «дезінформації» (навмисно, свідомо неправдивої інформації, що цілеспрямовано поширюється зловмисниками з конкретною метою завдання шкоди державі, суспільству або окремим особам) та «маніпулятивної інформації» (витончених психологічних технік впливу на масову свідомість та підсвідомість без прямої фактичної брехні через упередження, контекст, емоції) має бути здійснене максимально обережно, виважено юристами та психологами, з встановленням чітких, недвозначних правових рамок застосування відповідальності та без створення небезпечних потенційних інструментів державної цензури, які можуть бути легко зловжиті авторитарною владою.

Ефективні механізми швидкого, майже миттєвого офіційного

публічного спростування виявлених, підтверджених фейків з боку компетентних державних органів з гарантованим правом на публічну відповідь, спростування для постраждалих від дезінформації осіб або організацій, чия репутація постраждала, мають стати цивілізованою правовою альтернативою примусовим заборонам та технічним блокуванням як єдиним засобам боротьби. Встановлення юридичної відповідальності великих онлайн-платформ, соціальних мереж за активне, недбале поширення завідомо неправдивої, шкідливої інформації після отримання обґрунтованої, документованої скарги від постраждалих з доказами має стимулювати відповідальне саморегулювання платформ без перетворення їх в цензорів контенту.

У свою чергу, законодавча вимога максимальної прозорості, публічності джерел фінансування медіа-організацій та громадських організацій, особливо тих, що активно працюють в чутливій інформаційній сфері та можуть впливати на суспільну думку, дозволить громадськості та правоохоронним органам своєчасно виявляти приховане ворожє іноземне втручання та небезпечні конфлікти інтересів. Поряд з цим посилений правовий захист сміливих журналістів-розслідувачів та громадських активістів, що професійно займаються викриттям дезінформації, спростуванням ворожої пропаганди, від можливого переслідування, тиску, залякування та насильства має бути законодавчо гарантований через встановлення підвищеної кримінальної відповідальності за такі дії.

Модернізація застарілого законодавства про державну таємницю також є невідкладним пріоритетним завданням, оскільки воно має забезпечити надзвичайно складний, делікатний баланс між об’єктивною необхідністю секретності для надійного захисту критично важливої інформації, розголошення якої дійсно може завдати істотної шкоди національній безпеці, та не менш важливими вимогами максимальної прозорості, відкритості, які демократичне громадянське суспільство цілком обґрунтовано висуває до діяльності всіх державних органів, особливо тих могутніх силових структур,

що наділені величезними повноваженнями та можуть зловживати ними.

Механізми автоматичного, за замовчуванням розсекречення документів після закінчення науково обґрунтованих встановлених строків секретності, якщо компетентним органом не прийнято спеціального обґрунтованого рішення про продовження режиму секретності на новий термін з поясненням причин, ефективно запобігатимуть безстроковому, необґрунтованому приховуванню історично важливої для суспільства інформації про минуле. А чіткі, прозорі процедури судового оскарження громадянами та організаціями необґрунтованого, свавільного засекречення суспільно значущої інформації, яка об’єктивно становить законний суспільний інтерес і не загрожує безпеці, мають забезпечити реальний, дієвий механізм судового контролю за можливими зловживаннями секретністю з боку бюрократії. Досягнення завдяки цьому розумного, суспільно прийнятного балансу між конституційним обов’язком держави захищати державну таємницю та фундаментальним правом громадськості знати правду про діяльність безпекових органів, принаймні в узагальненому, статистичному вигляді без деталей, суттєво зміцнить демократичний громадський контроль без реальної шкоди для безпеки держави [37].

Окремим надзвичайно важливим, інноваційним напрямом правової модернізації є комплексне законодавче забезпечення широкої участі активного громадянського суспільства в забезпеченні національної безпеки, що відкриває принципово нові, раніше недоступні можливості для ефективної мобілізації значного суспільного потенціалу патріотизму, ініціативності, креативності, який український народ неодноразово переконливо продемонстрував під час героїчного протистояння російській агресії. Законодавче чітке визначення правового статусу численних волонтерських організацій у безпековій сфері з конкретними, юридично закріпленими правами на доступ до несекретної інформації про діяльність безпекових структур, участь у офіційних консультаціях з виробленням політики, моніторинг діяльності та водночас чіткими обов’язками щодо збереження

конфіденційності отриманої інформації, неухильного дотримання безпекових вимог та координації своїх дій з офіційними державними органами створить необхідну правову визначеність для легітимної діяльності волонтерів.

Створення прозорих механізмів цільової державної фінансової та матеріальної підтримки найбільш ефективних громадських ініціатив у сфері національної безпеки, включаючи надання грантів на конкретні проекти, податкові пільги для донорів, доступ до державної інфраструктури для проведення заходів, мають раціонально стимулювати динамічний розвиток громадянського сектору безпеки без створення повної залежності від держави. При цьому підвищити професійну якість державних рішень та їх демократичну легітимність в очах суспільства можна через законодавче закріплення процедур обов'язкового, а не добровільного залучення незалежних громадських експертів до професійної розробки проектів нормативних актів, стратегічних документів та державних програм у сфері безпекової політики через обов'язкові громадські обговорення проектів, незалежні експертні висновки фахівців, паритетне представництво в консультативних дорадчих органах.

Встановлення спеціального посиленого правового захисту громадських активістів, незалежних експертів, волонтерів, що патріотично займаються протидією гібридним загрозам, включаючи небезпечне викривання агентів впливу ворога, системне спростування дезінформації, громадський моніторинг діяльності підозрілих організацій, від можливого переслідування, тиску, залякування та фізичного насильства може бути забезпеченим через встановлення підвищеної кримінальної відповідальності за незаконне перешкоджання такій суспільно корисній діяльності. Це має супроводжуватись створенням сприятливих правових рамок для вільного функціонування недержавних незалежних аналітичних центрів, «мозкових центрів», що професійно спеціалізуються на глибокому дослідженні безпекової тематики, включаючи спрощену можливість отримання міжнародних та національних грантів на дослідження, законодавчо

гарантований доступ до несекретної урядової інформації для аналізу, обов'язкову участь в експертних консультаціях з питань безпеки, сприятиме необхідному розвитку незалежної, критичної експертизи у стратегічно важливій сфері національної безпеки.

Водночас модернізація національного законодавства об'єктивно не може і не повинна відбуватися ізольовано від ширшого міжнародного правового контексту, в якому існує Україна, тому послідовна, системна гармонізація з міжнародним правом та стандартами НАТО і Європейського Союзу є абсолютно критичною для забезпечення стратегічно важливої міжнародної політичної та військової підтримки України в протистоянні агресії, її успішної поступової євроатлантичної інтеграції та ефективної практичної міжнародної безпекової кооперації з партнерами. Повноцінна, всебічна імплементація в національне законодавство сучасних стандартів НАТО щодо демократичного цивільного контролю над всіма силовими структурами, включаючи фундаментальні принципи повної підзвітності парламенту як представницькому органу, максимальної прозорості бюджетування оборонних витрат, обов'язкового незалежного зовнішнього аудиту використання коштів, має стати невід'ємною, органічною частиною національного законодавства, а не формальною вимогою.

Послідовна адаптація величезного правового доробку Європейського Союзу (acquis communautaire ЄС) у багатогранній сфері безпеки та оборони, включаючи детальне регулювання прозорих оборонних закупівель, жорсткого контролю над експортом озброєнь та технологій подвійного призначення, всеосяжної кібербезпеки, надійного захисту критичної інфраструктури, забезпечить поступове реальне наближення України до високих європейських стандартів у всіх аспектах. А уважне, серйозне врахування численних професійних рекомендацій авторитетної Венеціанської комісії Ради Європи щодо конкретних українських законопроектів у сфері національної безпеки, яка неодноразово надавала детальні експертні висновки на запит українських органів, дозволить завчасно уникнути включення в закони положень, що

суперечать глибоким європейським конституційним традиціям та стандартам прав людини.

Практичну щоденну взаємодію на оперативному рівні суттєво полегшить забезпечення максимальної процедурної сумісності, інтероперабельності українських правових механізмів з аналогічними механізмами країн-партнерів для ефективної, безперешкодної міжнародної співпраці в розслідуванні транснаціональних злочинів, оперативному обміні розвідувальною інформацією, проведенні координованих спільних операцій. Водночас у складному процесі міжнародної гармонізації надзвичайно важливо розумно зберегти національну правову специфіку, унікальні елементи регулювання там, де вона об'єктивно виправдана специфічними українськими умовами, обов'язково враховуючи унікальний та безцінний для всього світу практичний досвід України у тривалій, складній протидії повномасштабній багатовимірній гібридній агресії, який може істотно збагатити міжнародну правову практику та теорію новими підходами.

Для надійного забезпечення постійної актуальності законодавства в умовах надзвичайно швидкої, безперервної еволюції загроз та технологій об'єктивно необхідне впровадження інноваційних механізмів швидкої, гнучкої адаптації законодавства до раптово виникаючих нових викликів, які мають бути вбудовані безпосередньо в саму архітектуру правової системи як її органічна, невід'ємна складова, а не зовнішнє доповнення. Так, законодавче введення так званих «сонячних норм» (sunset clauses) з автоматичним припиненням юридичної дії після заздалегідь чітко встановленого розумного строку для експериментальних, інноваційних правових інститутів, механізмів дозволить відповідально тестувати принципово нові підходи до регулювання без серйозного ризику їх небажаної консервації, закостеніння в законодавстві на десятиліття в разі виявленої практичної неефективності, адже прогресивний законодавець завжди може свідомо продовжити дію норми спеціальним актом, якщо вона переконливо виправдала себе на практиці.

Поряд з цим, виважене розширення усталеної практики делегованого

законодавства, що надає уряду як виконавчому органу спеціальні повноваження оперативно, без довгих парламентських процедур деталізувати загальні рамкові норми законів, конкретизувати їх положення в межах чітко визначених парламентом меж делегування та за певних, законом встановлених умов, дозволить гнучко, швидко реагувати на раптові нові виклики без затяжних, багатомісячних парламентських процедур прийняття законів при обов'язковому збереженні фундаментального парламентського демократичного контролю над усіма принципово важливими, стратегічними питаннями безпекової політики держави.

Доцільним також видається і створення спеціальних експериментальних правових режимів, так званих «регуляторних пісочниць» (regulatory sandboxes) для відповідального апробування радикально інноваційних регуляторних рішень, особливо в технологічно складних, швидко змінюваних сферах типу динамічної кібербезпеки чи революційного застосування штучного інтелекту в безпековій діяльності, де застаріле традиційне негнучке регулювання може серйозно гальмувати необхідні інновації. Тимчасова можливість контрольованого відхилення від загальних правил у спеціально створених обмежених контрольованих умовах пісочниці дозволить експериментально знаходити оптимальні, збалансовані регуляторні підходи методом спроб та помилок.

Запровадження обов'язкового періодичного регулярного (наприклад, раз на три-п'ять років) інституціоналізованого перегляду всіх ключових елементів безпекового законодавства спеціально створеними експертними комісіями з обов'язковим проведенням ґрунтовного аналізу їх реальної практичної ефективності в досягненні цілей, актуальності в світлі нових загроз та відповідності новим технологічним та соціальним реаліям забезпечить системне, передбачуване оновлення правової бази замість хаотичних змін під тиском кризи. Також своєчасно виявляти накопичувані проблеми на ранніх стадіях до їх загострення та критичного накопичення дозволить створення дієвих, реально працюючих механізмів систематичного громадського

моніторингу практичного застосування безпекового законодавства через обов'язкову публікацію детальних публічних звітів про практичне застосування окремих норм з статистикою та аналізом, відкриті громадські слухання щодо виявлених системних проблем правозастосування, законодавчу можливість подання обґрунтованих громадських ініціатив про внесення конкретних змін до законів.

Проте найбільш складним концептуально, найдовшим за часом, але водночас абсолютно найважливішим за довгостроковим впливом аспектом успішної правової модернізації об'єктивно є глибинна, фундаментальна трансформація правової культури, правосвідомості в традиційно закритій безпековій сфері, яка має еволюціонувати від глибоко вкоріненого в пострадянській бюрократичній традиції примітивного формалістичного дотримання сухої букви закону як самоцілі, часто цинічно поєднаного з активним пошуком способів формально легально його обійти, до якісно нового глибокого, зрілого розуміння духу, сенсу, цілей та фундаментальних цінностей, які закон має втілювати та захищати в житті.

Тому створення та реалізація систематичних, обов'язкових програм всебічної правової освіти для всіх без винятку співробітників безпекових структур на всіх організаційних рівнях ієрархії від рядових виконавців до вищого керівництва, з принциповим акцентом не просто на механічне заучування текстів юридичних норм, а на глибоке критичне розуміння фундаментальних правових принципів, універсальних прав людини, розумних меж допустимого втручання держави в приватне життя, мають стати абсолютно обов'язковим, невід'ємним елементом базової професійної підготовки кожного фахівця. Додатковим, але надзвичайно важливим рівнем професійного саморегулювання поведінки може бути розробка за участю фахівців з етики та впровадження в практику детальних професійних етичних кодексів поведінки, що органічно доповнюють формальні правові норми неформальними, але обов'язковими моральними стандартами поведінки, включаючи делікатні питання конфліктів інтересів, етичних відносин з

громадськістю та медіа, меж професійної солідарності та корпоративної лояльності.

Узагальнюючи викладене, можна систематизувати десять ключових напрямів модернізації законодавства про національну безпеку, їх змістові компоненти та очікувані практичні результати (табл. 3.1).

Таблиця 3.1

Напрями модернізації законодавства про національну безпеку

Напрям модернізації	Ключові елементи	Очікувані результати
Кодифікація безпекового законодавства	Розробка Кодексу національної безпеки; усунення суперечностей; єдиний понятійний апарат	Системність правового регулювання; ліквідація прогалин і дублювань
Правове регулювання гібридних загроз	Визначення гібридної агресії; режим гібридної оборони; критична інформаційна інфраструктура	Адекватна правова основа для протидії новим загрозам
Міжвідомча координація	Обов’язковий характер координаційних рішень; персональна відповідальність керівників; арбітраж РНБО	Подолання відомчої роз’єднаності; ефективна взаємодія
Розвідувальна діяльність	Розширення предмету розвідки; легалізація OSINT; захист джерел і методів	Адаптація до інформаційної епохи; нові розвідувальні спроможності
Кібербезпека	Комплексний закон про кібербезпеку; криміналізація нових кіберзлочинів; обов’язкові стандарти кібергігієни	Правовий захист кіберпростору; підвищення стійкості до кібератак
Інформаційна безпека	Критерії дезінформації; механізми спростування фейків; відповідальність онлайн-платформ	Протидія дезінформації при збереженні свободи слова
Державна таємниця	Автоматичне розсекречення; судове оскарження засекречення	Баланс між секретністю і прозорістю; демократичний контроль

Закінчення табл. 3.1

Участь громадянського суспільства	Правовий статус волонтерів; фінансова підтримка ініціатив; залучення експертів	Мобілізація суспільного потенціалу; легітимність рішень
Міжнародна гармонізація	Імплементація стандартів НАТО; адаптація acquis ЄС; процедурна сумісність	Євроатлантична інтеграція; ефективна міжнародна співпраця
Механізми адаптації	«Сонячні норми»; делеговане законодавство; регуляторні пісочниці; періодичний перегляд	Гнучкість і актуальність законодавства; швидке реагування на нові виклики

Завдяки цьому модернізація законодавчої бази має остаточно, незворотно усвідомлюватися всіма залученими акторами не як одноразовий формальний акт урочистого прийняття кількох нових красивих законів з подальшим забуттям, а як постійний, безперервний, систематичний процес цілеспрямованої адаптації всієї правової системи до об'єктивно динамічних, безперервно змінюваних безпекових реалій, що принципово вимагає створення відповідної потужної інституційної інфраструктури підтримки та послідовного формування сучасної культури постійного правового розвитку в безпековій сфері.

3.3. Трансформація організаційної архітектури сектору безпеки на засадах інтегрованого підходу

Органічно переходячи від правових аспектів модернізації до організаційних питань, необхідно підкреслити, що оптимізація організаційної структури численних суб'єктів сектору безпеки України в специфічних, надзвичайно складних умовах триваючої гібридної війни об'єктивно представляє собою не менш комплексне, багатогранне завдання фундаментальної трансформації всієї інституційної архітектури сектору від застарілої, неефективної пострадянської моделі з її характерною, вкрай шкідливою надмірною централізацією всіх рішень на верхівці, масштабним

непродуктивним дублюванням однакових функцій між різними відомствами та глибоко деструктивною міжвідомчою конкуренцією за ресурси до сучасної, ефективної інтегрованої системи, об'єктивно здатної ефективно, координовано, синхронізовано та результативно протидіяти багатовимірним, постійно еволюціонуючим загрозам складного гібридного характеру, що атакують одночасно в різних сферах.

Багаторічний практичний досвід десятиліття інституційних реформ в Україні переконливо демонструє незаперечний факт, що поверхневі косметичні організаційні зміни, обмежені формальним перейменуванням структурних підрозділів або черговими кадровими перестановками керівників без змін сутності, а також наївне механічне копіювання західних організаційних моделей, структур без належного, критичного урахування принципово іншого національного контексту, історичного досвіду та глибоких особливостей вкоріненої інституційної культури категорично не дають бажаних стійких результатів і дуже часто навіть значно поглиблюють, загострюють існуючі хронічні системні проблеми замість їх вирішення.

Отже, об'єктивно необхідна глибинна, всеосяжна системна трансформація організаційних структур, що має органічно, збалансовано поєднувати структурні зміни на рівні формальних організаційних схем, штатних розписів з паралельною культурною еволюцією на глибшому рівні неформальних цінностей, поведінкових моделей та організаційної ідентичності, всебічною технологічною модернізацією на рівні інструментів, систем, процесів, а також послідовним впровадженням принципово нових, сучасних принципів та методів управління складними організаціями, максимально адаптованих до специфічних реалій затяжних гібридних конфліктів з їх невизначеністю.

Концептуальною теоретичною основою такої комплексної, всеосяжної оптимізації організаційних структур має стати парадигмальний, фундаментальний перехід від застарілого традиційного функціонально-галузевого до принципово інноваційного процесно-орієнтованого принципу

логічної побудови організаційних структур безпекових відомств, що передбачає глибоке фундаментальне переосмислення базової логіки організації всієї діяльності установ.

Традиційна, звична бюрократична модель організації діяльності, за якою практично кожне окреме відомство організаційно прагне мати власний повний, автономний, самодостатній набір абсолютно всіх функцій від аналітичної роботи та стратегічного планування до матеріально-технічного забезпечення і медичного обслуговування персоналу, створюючи паралельні структури, об'єктивно неминуче призводить до величезного масштабного дублювання однакових зусиль різними відомствами, вкрай неефективного марнотратного використання хронічно обмежених цінних ресурсів, непродуктивного створення численних паралельних дублюючих структур, які фактично виконують абсолютно ідентичні функції в різних відомствах.

Натомість нова процесно-орієнтована модель організації принципово передбачає системне виділення, ідентифікацію наскрізних, міжвідомчих за своєю природою бізнес-процесів, таких як повний розвідувальний цикл від визначення інформаційних потреб споживачів до розповсюдження готової аналітичної продукції, комплексний процес оперативного реагування на різноманітні інциденти від раннього виявлення загрози до повної ліквідації наслідків, багатоетапний процес стратегічного планування від глибокого аналізу безпекового середовища до детальної розробки конкретних програм дій, та наступне організаційне створення спеціальних інтегрованих, міжвідомчих за складом структур для максимально ефективної реалізації цих складних процесів з активною участю, внеском всіх релевантних, компетентних суб'єктів безпеки (рис. 3.2).

Така процесна логіка організації об'єктивно дозволяє досягти потужного синергетичного ефекту від координованих, узгоджених зусиль різних відомств, кожне з яких вносить свою унікальну, незамінну експертизу, спеціальні знання та досвід, при одночасному обов'язковому збереженні їх профільної функціональної спеціалізації в конкретних вузьких предметних

доменах, сферах діяльності, де саме вони об’єктивно мають найбільші, найглибші компетенції, досвід та ресурси.

Рис. 3.2. Трансформація організаційної архітектури сектору безпеки на засадах інтегрованого підходу

Ключовим практичним організаційним втіленням, реалізацією цього прогресивного концептуального підходу на практиці має закономірно стати створення принципово нового Інтегрованого командування сил безпеки та оборони як єдиного, централізованого органу повноцінного оперативного управління абсолютно всіма силовими компонентами української держави в кризових та активних конфліктних ситуаціях, що об’єктивно стане революційним, проривним елементом якісно нової інституційної архітектури системи безпеки. На принципову відміну від існуючих нині координаційних механізмів, які організаційно мають переважно дорадчі, консультативні та

узгоджувальні функції без юридичного права прямого командування силами та засобами, принципово нове Інтегроване командування законодавчо матиме реальні, юридично закріплені повноваження віддавати прямі, обов'язкові для виконання накази та розпорядження абсолютно всім залученим до конкретної операції силам та засобам незалежно від їх постійної відомчої підпорядкованості в мирний час. Це остаточно, радикально усуне традиційні хронічні проблеми розпорошеності, фрагментації командування між різними відомствами в критичні моменти.

Внутрішня організаційна структура такого Командування має бути побудована за сучасним матричним принципом організації та обов'язково включатиме постійних, штатних представників абсолютно всіх ключових, профільних силових відомств держави (Збройні Сили України, Служба безпеки, Національна поліція, Національна гвардія, розвідувальні служби, Державна прикордонна служба), які працюватимуть організаційно не як формальні відомчі представники з власними інструкціями та вказівками від свого керівництва, а як справді єдина, злагоджена, інтегрована команда професіоналів зі спільними цілями, єдиним баченням ситуації та колективною відповідальністю за результат операції перед керівництвом держави.

Функціональна логіка роботи Командування чітко передбачає, що в мирний, спокійний час воно функціонує переважно в підготовчому режимі стратегічного та детального оперативного планування можливих операцій, розробки альтернативних сценаріїв дій, систематичного проведення штабних навчань, тренувань та командно-штабних ігор для відпрацювання взаємодії. Але в разі раптового виникнення реальних кризових ситуацій, збройних конфліктів або масштабних надзвичайних ситуацій, що загрожують безпеці, оперативно, майже миттєво переходить до принципово іншого режиму безпосереднього, централізованого, повноцінного оперативного управління абсолютно всіма задіяними в операції силами та засобами через єдиний центр прийняття стратегічних та оперативних рішень, що дозволяє максимальну координацію та синхронізацію дій.

Не менш критично важливою для ефективності системи національної безпеки є кардинальна, глибока реорганізація української розвідувальної спільноти. Дана реорганізація як стратегічну мету повинна мати послідовне подолання глибоко деструктивної, шкідливої відомчої роз'єднаності служб, непродуктивної конкуренції за бюджетні ресурси та політичні пріоритети, масштабного дублювання однакових аналітичних зусиль паралельно в різних службах та організаційне створення справді інтегрованої, синергетично ефективної системи національної розвідки, що працює як єдиний організм.

Ключовим інституційним механізмом професійного синтезу, об'єднання розвідувальної інформації з різних джерел в єдину картину може стати організаційне створення принципово нового Національного розвідувального агентства як єдиного потужного аналітично-координаційного центру всієї розвідувальної діяльності, що має організаційно об'єднати, інтегрувати всі потужні аналітичні підрозділи, експертів абсолютно всіх розвідувальних служб держави (Головного управління розвідки Міністерства оборони України, Служби зовнішньої розвідки України, розвідувальних аналітичних підрозділів Служби безпеки України).

При цьому функціональна спеціалізація різних розвідувальних служб за профілями абсолютно обов'язково повністю зберігається на критично важливому рівні первинного збору інформації з різних джерел, де кожна спеціалізована служба професійно фокусується на своїй профільній, унікальній сфері відповідальності згідно компетенції:

військова розвідка ГУР концентрує зусилля на воєнних аспектах діяльності потенційних противників, озброєннях, військовій техніці та стратегічних військових планах ймовірного противника;

зовнішня розвідка СЗР професійно працює з політичними, економічними, дипломатичними аспектами діяльності іноземних держав та міжнародних організацій;

Служба безпеки зосереджується на контррозвідувальній діяльності проти іноземних спецслужб та внутрішніх загрозах національній безпеці.

Але весь подальший глибокий аналіз вже отриманих різними шляхами даних, професійний синтез різнорідної інформації з численних джерел, підготовка узагальнених, цілісних розвідувальних оцінок ситуації та організоване розповсюдження готової аналітичної продукції кінцевим споживачам здійснюється вже централізовано через єдине Національне агентство. Така раціональна модель організації радикально, повністю усуває вкрай контрпродуктивне дублювання аналітичних зусиль, коли різні розвідувальні служби повністю незалежно, паралельно аналізують абсолютно ті самі події, дуже часто закономірно приходячи при цьому до суперечливих, взаємовиключних висновків, що дезорієнтує керівництво, та об'єктивно забезпечує формування єдиної, цілісної, внутрішньо несуперечливої розвідувальної картини для інформованого прийняття рішень керівництвом держави на всіх рівнях.

Паралельно з інтеграцією розвідки об'єктивно необхідна глибока трансформація територіальної організації всіх безпекових структур від застарілої, негнучкої моделі абсолютно жорсткої прив'язки всіх підрозділів та їх зон відповідальності до формального адміністративно-територіального устрою держави, що склався історично, до принципово гнучкої мережевої моделі організації, що максимально адекватно відповідає об'єктивним реаліям сучасних гібридних загроз, які за своєю природою принципово не визнають ніяких адміністративних кордонів між областями чи районами і вимагають функціональної, а не бюрократичної територіальної логіки організації сил.

Організаційне створення принципово нових міжрегіональних оперативних командувань, кожне з яких функціонально охоплює одразу кілька адміністративних областей зі схожим, подібним профілем безпекових загроз, географічними фізичними особливостями театру та стратегічним військовим значенням для оборони, дозволить концентрувати обмежені ресурси більш раціонально, ефективно без розпилення. Формування високомобільних оперативних груп швидкого реагування з гнучкою модульною організаційною структурою, які принципово не прив'язані жорстко до конкретних

адміністративних територій на постійній основі, а можуть та повинні оперативно, швидко перекидатися між різними регіонами країни в залежності від динамічної, постійно змінюваної актуальної загрозової ситуації, забезпечить необхідну стратегічну гнучкість, маневреність оперативного реагування на загрози. А створення розгалуженої мережі універсальних, багатофункціональних опорних пунктів з максимально уніфікованою модульною інфраструктурою, об'єктивно придатною для гнучкого, швидкого тимчасового розміщення принципово різних за профілем діяльності силових компонентів (військових підрозділів, поліцейських сил, рятувальних служб), замість утримання численних дорогих спеціалізованих відомчих баз, казарм дозволить суттєво оптимізувати ефективне використання дорогої інфраструктури.

Така гнучка територіальна організація сил об'єктивно дозволяє оперативно, швидко концентрувати значні сили, створювати перевагу в критичних, найбільш загрозливих напрямках без економічної необхідності постійного утримання надмірної, економічно неефективної військової присутності абсолютно рівномірно по всій величезній території країни незалежно від реальних загроз.

Важливим стратегічним напрямком структурної оптимізації безпекового сектору є кардинальне удосконалення організаційної внутрішньої будови Міністерства оборони України, де об'єктивно необхідне значно чіткіше, ніж існує зараз в практиці, функціональне організаційне розмежування між власне політичним керівництвом міністерства, що стратегічно формує оборонну політику держави та представляє інтереси держави в міжнародних відносинах, та адміністративно-забезпечувальними допоміжними структурами міністерства, що технічно створюють необхідні матеріальні, фінансові, кадрові умови для безпосередньо ефективної бойової діяльності військ на фронті. Вище політичне керівництво міністерства, що організаційно включає цивільного міністра оборони та його заступників з ключових стратегічних напрямків державної політики в оборонній сфері, має

професійно концентруватися виключно на найвищих стратегічних функціях держави. Натомість Генеральний штаб Збройних Сил України як вищий орган військового управління має законодавчо отримати повну, гарантовану на рівні закону автономію, незалежність в усіх питаннях чисто оперативного, тактичного управління військами в полі, детального професійного планування та безпосереднього проведення військових операцій на театрі, оперативно-тактичного використання наявних сил та засобів, ведення розвідувальної діяльності в інтересах забезпечення оборони, абсолютно без втручання політичного керівництва в суто оперативні, тактичні військові питання, де воно об'єктивно не має необхідної професійної компетенції та може завдати шкоди непрофесійними рішеннями.

При цьому спеціалізована Агенція оборонних закупівель має бути організаційно повністю виведена з безпосереднього адміністративного підпорядкування Міністерству оборони як замовнику та підпорядкована безпосередньо уряду з єдиною стратегічною метою забезпечення максимальної можливої прозорості процедур, надійного запобігання небезпечним конфліктам інтересів замовника та постачальника, мінімізації корупційних ризиків [75]. Додатково до цього мають бути організаційно створені повністю автономні спеціалізовані виконавчі агенції з окремих ключових функцій матеріально-технічного забезпечення:

кадрова агенція для централізованого, професійного управління абсолютно всіма аспектами складної роботи з військовим персоналом від рекрутингу до звільнення;

інфраструктурна агенція для професійної експлуатації та планомірного розвитку величезних військових об'єктів нерухомості;

науково-технічна агенція для стратегічної координації оборонних досліджень та розробок перспективних технологій, які професійно надаватимуть високоякісні спеціалізовані сервіси абсолютно всім різноманітним компонентам величезного оборонного сектору на єдиних стандартах якості без дублювання.

Окремої пильної уваги, можливо найбільш складної політично, заслуговує питання фундаментального, глибокого реформування Служби безпеки України з амбітною стратегічною метою її послідовної трансформації з громіздкої багатофункціональної спадкової структури радянського тоталітарного типу з надмірно широкими повноваженнями в спеціалізовану, професійну контррозвідувальну службу сучасного європейського демократичного типу з чітко визначеними, обмеженими функціями. Це принципово вимагає не просто поверхневого механічного скорочення окремих другорядних функцій для звітності, а справді глибокої, всеосяжної реорганізації всієї корпоративної філософії діяльності організації, організаційної культури поведінки та інституційної ідентичності, самосприйняття співробітників.

Повне, безповоротне законодавче виведення з широкої компетенції СБУ абсолютно невластивих для спеціальної спецслужби, нетипових функцій активної боротьби з економічними злочинами в господарській сфері, викриття корупції чиновників, протидії організованій злочинності з обов'язковою передачею всіх цих важливих, але непрофільних функцій спеціалізованим правоохоронним органам загальної компетенції, які мають відповідні професійні компетенції, досвід та значно більшу підзвітність суспільству, об'єктивно дозволить СБУ максимально зосередитися виключно на своїх профільних, унікальних завданнях контррозвідки.

Критично важливою для безпеки в цифрову епоху є послідовна структурна інтеграція та координація розпорошених кіберсил держави, які наразі безсистемно розпорошені між численними різними відомствами без належної ефективної координації дій. З цією метою видається доцільним створення об'єднаного Кіберкомандування як єдиного потужного органу централізованого стратегічного планування кібероперації, оперативної координації всіх дій та безпосереднього професійного проведення як складних наступальних кібероперації проти ворожих інформаційних систем та мереж, так і оборонних операцій із захисту національного суверенного кіберпростору

від атак, з прямим оперативним підпорядкуванням йому абсолютно всіх військових спеціалізованих кіберпідрозділів різних силових відомств. Створення такої організаційної структури забезпечить критично необхідну єдність оперативного командування в специфічному віртуальному кіберпросторі як театрі воєнних дій.

При цьому Державний центр кіберзахисту зберігає за собою важливі функції загальної стратегічної координації захисту об'єктів критичної державної та комерційної інфраструктури від кібератак, розробки обов'язкових стандартів кібербезпеки та формування державної політики в цифровій сфері, але принципово не дублює оперативні функції прямого управління силами. А кіберполіція в організаційній структурі Національної поліції України концентрується виключно на специфічних правоохоронних функціях кримінальної юстиції: професійне розслідування різноманітних кіберзлочинів, активне переслідування кіберзлочинців через суди, ретельне збирання процесуальних доказів для судових кримінальних процесів, а не на військових операціях.

Такий чіткий, недвозначний функціональний розподіл сфер відповідальності, компетенцій з одночасним запровадженням ефективних, реально працюючих механізмів оперативної щоденної взаємодії, швидкого обміну критично важливою тактичною інформацією про загрози, координованого спільного реагування на масштабні інциденти через єдині затверджені протоколи та стандартні процедури об'єктивно усуває небезпечне непродуктивне дублювання обмежених зусиль різних структур та критичні прогалини в національній кібероборoні, коли загроза випадає з поля зору всіх. Додатково до постійних структур об'єктивно необхідне цілеспрямоване формування резервного кібер-резерву з висококваліфікованих професійних ІТ-фахівців, програмістів приватного комерційного сектору, які в звичайний мирний час професійно працюють у своїх приватних ІТ-компаніях на комерційних проектах, але можуть та повинні бути законно, швидко мобілізовані державою для термінового нарощування обмежених державних

кіберспроможностей у разі виникнення масштабних, затяжних кіберконфліктів високої інтенсивності або надзвичайних кризових ситуацій в кіберпросторі, що загрожують безпеці.

Величезний потенціал суттєвого підвищення загальної ефективності діяльності та економії хронічно обмежених бюджетних ресурсів об'єктивно закладений в послідовній оптимізації громіздких структур матеріально-технічного, інформаційно-комунікаційного та іншого допоміжного забезпечення основної діяльності через стратегічний перехід від традиційної малоефективної централізованої відомчої моделі дублюючого забезпечення (за якої практично кожне окреме відомство неефективно має власні, повністю паралельні, дублюючі системи всіх видів забезпечення) до принципово інтегрованої економічної моделі спільних міжвідомчих сервісів забезпечення, професійно доступних абсолютно всім різноманітним суб'єктам сектору безпеки на рівних умовах без дискримінації.

Суттєвого підвищення ефективності використання обмежених ресурсів можна досягти через організаційне створення єдиної консолідованої логістичної системи постачання для всього сектору безпеки і оборони. На противагу численним паралельним відомчим структурам тилового забезпечення, централізована система з автоматизованими складами, спільним транспортним парком та інтегрованими системами управління запасами забезпечує значну економію масштабу. Більше того, така консолідація радикально підвищує оперативність критичного постачання, що особливо важливо в умовах динамічних гібридних загроз.

Аналогічна логіка має застосовуватися і до сфери урядового зв'язку та інформаційних технологій. Формування консолідованої системи з єдиними технічними стандартами обладнання, спільною телекомунікаційною інфраструктурою та централізованою кіберзахищеністю забезпечить надійну міжвідомчу комунікацію в критичні моменти. Це принципово перевершує утримання безлічі технічно несумісних відомчих інформаційних систем, які створюють «інформаційні силоси» та унеможливлюють ефективну

координацію.

Подібний підхід доцільно застосувати і до сфери професійної підготовки персоналу. Створення мережі спільних міжвідомчих навчальних центрів для уніфікованої базової підготовки всіх категорій співробітників безпекових структур суттєво оптимізує використання дорогої навчальної інфраструктури, полігонів та тренажерів. При цьому після базової підготовки за єдиними стандартами співробітники проходитимуть спеціалізовану поглиблену підготовку у профільних відомчих закладах за конкретними професійними профілями, що дозволяє поєднати переваги уніфікації та спеціалізації.

Таким чином, масштабна консолідація допоміжних функцій у всіх описаних сферах дозволяє досягти значної економії бюджетних коштів завдяки ефекту економії масштабу та вивільнити ресурси для посилення основної оперативної діяльності безпекових структур. Водночас важливим доповненням до традиційних постійних організаційних форм має стати широке використання гнучких тимчасових проектних структур для вирішення специфічних нестандартних завдань. Такі завдання принципово не вписуються в рутинну діяльність постійних підрозділів з їх бюрократією, тому потребують інших організаційних рішень.

Передусім йдеться про оперативне формування спеціалізованих міжвідомчих цільових груп (task force) для протидії конкретним загрозам. Це можуть бути операції проти певної терористичної організації, конкретного кіберугруповання або складної схеми контрабанди зброї. Учасників таких груп тимчасово повністю виводять з їх постійних структур та максимально зосереджують виключно на пріоритетному завданні до його успішного виконання або ліквідації загрози, що забезпечує максимальне фокусування зусиль на пріоритеті.

Іншим важливим елементом гнучкої організаційної архітектури є створення спеціалізованих інноваційних лабораторій. Вони дозволяють творчо розробляти принципово нові підходи до вирішення проблем, вільно експериментувати з передовими технологіями та апробувати нетрадиційні

методи роботи. Звільнення від жорсткого обтяження традиційною бюрократією, усталеними процедурами та організаційною інерцією створює сприятливе середовище для генерування проривних інновацій без страху покарання за невдалі експерименти.

Для мінімізації ризиків масштабних реформ доцільним є формування спеціальних експериментальних пілотних підрозділів. Вони дозволяють практично тестувати принципово нові організаційні форми, інноваційні управлінські методи та революційні технологічні рішення в реальних, хоча й контрольованих умовах. Лише після успішного пілотування та ретельного аналізу результатів приймається стратегічне рішення про масштабування нововведень на всю систему, що суттєво знижує ризики та витрати невдалих реформ.

Особливе місце серед тимчасових структур займають «червоні команди» (red team) – професійні групи досвідчених фахівців, які систематично намагаються виявити критичні вразливості власної системи безпеки. Через реалістичну імітацію можливих дій противника, систематичне критичне мислення та альтернативний незалежний аналіз такі команди підвищують загальну стійкість системи. Вони виявляють слабкі місця до того, як їх експлуатує реальний противник в бойових умовах, що дозволяє завчасно вжити необхідних контрзаходів.

Така гнучка динамічна проектна надбудова над стабільною базовою постійною структурою забезпечує життєво необхідну адаптивність та постійну інноваційність всієї організаційної системи. При цьому зберігається критично важлива стабільність та передбачуваність її фундаментальних постійних елементів, які забезпечують наступність діяльності та організаційну пам’ять.

Абсолютно критично важливими для подолання глибоко вкорінених відомчих бюрократичних бар’єрів є різноманітні механізми цілеспрямованого стимулювання горизонтальної міжвідомчої інтеграції на всіх організаційних рівнях. Відомча роз’єднаність об’єктивно залишається однією з найбільших

системних проблем української системи безпеки, тому її подолання вимагає комплексного підходу.

Одним з найефективніших інструментів є організаційне створення постійно діючих спільних ситуаційних та оперативних координаційних центрів. У таких центрах професійні представники принципово різних безпекових структур працюють не у відокремлених кімнатах свого відомства, а в єдиному спільному фізичному просторі. Вони бачать одночасно ті самі оперативні інформаційні екрани, активно обговорюють ситуацію в режимі реального часу та спільно приймають координовані рішення без бюрократичних затримок на міжвідомче узгодження, що радикально підвищує практичну ефективність оперативної координації.

Паралельно з цим послідовна розбудова інтегрованих міжвідомчих інформаційних систем усуває хронічні інформаційні бар'єри між структурами. Технічна можливість безпечного крос-відомчого електронного доступу до релевантної інформації з баз даних іншого відомства (з дотриманням рівнів секретності та принципу необхідності знати) дозволяє оперативному працівнику одного відомства отримати критично необхідні дані в режимі реального часу. Це радикально скорочує час, який раніше витрачався на довгі бюрократичні запити через систему паперового документообігу.

Не менш важливою є цілеспрямована розробка та впровадження уніфікованих стандартизованих процедур та протоколів спільної діяльності. Єдина несуперечлива професійна термінологія, повністю сумісні технічні стандарти обладнання та спільні уніфіковані формати службових документів для всіх відомств забезпечують критично важливу інтероперабельність на базовому процедурному рівні повсякденної роботи. Без такої уніфікації навіть найкраща координаційна архітектура залишатиметься малоефективною через технічну несумісність.

Нарешті, запровадження конкретних фінансових стимулів та публічних заохочень за продемонстровану успішну міжвідомчу співпрацю на індивідуальному рівні окремих співробітників та груповому рівні цілих

підрозділів робить активну кооперацію не просто абстрактним обов’язком, а особисто вигідною та привабливою для безпосередніх виконавців. Грошові премії та нагороди за результати спільних операцій створюють матеріальну зацікавленість у ефективній координації.

У цілому, стратегічною метою всієї організаційної оптимізації структур має бути послідовний перехід від екстенсивної радянської моделі нарощування потужності до інтенсивної сучасної моделі підвищення якості. Традиційний підхід «більше завжди краще», де єдиним способом досягнення ефективності вважалося механічне збільшення чисельності персоналу та кількості підрозділів без уваги до їх якості, має поступитися місцем принципово іншому розумінню: «якість категорично важливіша за кількість». Абсолютним пріоритетом стає високий професіоналізм, сучасна технічна оснащеність та якісна підготовка кожного окремого співробітника, а не валова чисельність.

Реалізація цього переходу передбачає кілька взаємопов’язаних напрямів. По-перше, послідовне систематичне скорочення численних надлишкових дублюючих управлінських ланок бюрократичної ієрархії через професійний організаційний аудит та детальний функціональний аналіз процесів. Скорочення малокваліфікованого обслуговуючого персоналу, який не бере безпосередньої участі в оперативній діяльності, а лише обслуговує саму бюрократію, цілеспрямовано вивільняє значні ресурси для більш продуктивного використання.

По-друге, масштабна технологічна автоматизація рутинних повторюваних функцій дозволяє радикально вивільнити людські ресурси для переведення на критично важливі оперативні напрямки. Паперовий документообіг, бухгалтерський облік, статистична звітність, первинний технічний моніторинг – всі ці функції можуть бути ефективно автоматизовані через впровадження сучасних інформаційних систем управління, технологій штучного інтелекту та роботизації бізнес-процесів.

По-третє, активний широкий аутсорсинг непрофільних допоміжних

функцій спеціалізованим приватним компаніям дозволяє безпековим структурам максимально зосередитися виключно на своїй унікальній профільній діяльності. Фізична охорона об’єктів, прибирання приміщень, організація харчування, транспортні послуги, технічне обслуговування небойової цивільної техніки – всі ці функції приватні компанії можуть виконувати значно ефективніше та економічно дешевше завдяки спеціалізації.

Нарешті, цілеспрямоване стратегічне підвищення відносної частки висококваліфікованого оперативного складу, безпосередньо зайнятого виконанням основних профільних завдань, відносно загальної чисельності персоналу через продуманий перерозподіл людських ресурсів з допоміжних на основні функції суттєво підвищує загальну результативність діяльності організації.

Кінцевим бажаним результатом має стати створення відносно компактних за загальною чисельністю, але водночас високопрофесійних за кваліфікацією персоналу, відмінно технічно оснащених сучасним обладнанням та ефективно керованих сучасними методами менеджменту безпекових структур. Це принципово відрізняється від громіздких неповороткіших бюрократизованих утворень з надмірним персоналом низької середньої кваліфікації та застарілим обладнанням, які успадковані з радянської епохи.

Для надійного забезпечення не одноразового епізодичного характеру реорганізації, а справжньої безперервності процесу організаційного розвитку об’єктивно необхідне свідоме вбудовування безпосередньо в нові організаційні структури постійно діючих механізмів їх систематичного самовдосконалення та адаптації. Організація має еволюціонувати відповідно до об’єктивних змін зовнішнього безпекового середовища та цінного накопичення внутрішнього практичного досвіду діяльності.

Передусім йдеться про регулярні систематичні організаційні аудити ефективності діяльності, які обов’язково проводяться не самими підконтрольними структурами, а повністю незалежними зовнішніми

експертами-консультантами з багатим міжнародним досвідом. Використання найпередовіших методологій об’єктивної оцінки ефективності та обов’язкове порівняння з кращими світовими практиками демократичних країн своєчасно виявляють накопичувані проблемні зони та конкретні можливості системного покращення до виникнення кризи.

Не менш важливим інструментом є систематичний професійний бенчмаркінг – детальний порівняльний аналіз власних організаційних рішень, ключових показників ефективності та практик роботи з об’єктивно кращими світовими аналогами в розвинених демократичних країнах з передовими системами національної безпеки. Це дозволяє своєчасно виявляти критичне відставання від світових стандартів та усвідомлено запозичувати і адаптувати кращі перевірені практики без необхідності винаходити велосипед.

Створення спеціалізованої професійної системи управління організаційними змінами з обов’язковим залученням кваліфікованих фахівців з управління трансформаціями забезпечує максимальну м’якість та плавність болісних організаційних переходів без деструктивних конфліктів. Використання міжнародно перевірених методологій управління змінами, розробка детальних комунікаційних стратегій для роз’яснення необхідності змін персоналу та активне залучення самого персоналу до процесу спільної розробки трансформації мінімізує природний психологічний опір будь-яким змінам з боку співробітників.

Таким чином, організаційна оптимізація структур має остаточно усвідомлюватися всіма залученими акторами не як одноразова велика драматична реорганізація з болісною радикальною ломкою всіх усталених структур та травматичними масовими звільненнями з подальшим тривалим забуттям теми, а як постійний безперервний систематичний керований еволюційний процес. Це процес цілеспрямованого поступового вдосконалення, планомірної адаптації гнучких організаційних форм точно відповідно до об’єктивної еволюції загроз, регулярної появи проривних нових технологій та систематичного накопичення цінного операційного практичного

досвіду. Така зміна парадигми принципово вимагає формування відповідної прогресивної організаційної культури постійних позитивних змін та психологічної готовності всього персоналу до постійних організаційних трансформацій як нормального стану [111].

Завершуючи розгляд організаційних механізмів підсилення національної безпеки України, необхідно підкреслити їх фундаментальну взаємозалежність та необхідність комплексного впровадження. Жоден окремий механізм, навіть блискуче розроблений на папері, не може забезпечити трансформацію системи ізольовано від інших елементів реформи. Лише синергетична взаємодія інституційних перебудов, що змінюють структури, процедурних оптимізацій, що покращують процеси, технологічних інновацій, що надають інструменти, та культурних змін, що трансформують ментальність, може створити якісно нову систему національної безпеки. Така система буде здатна ефективно протидіяти сучасним гібридним загрозам та забезпечувати довгострокову стійкість української держави в умовах непередбачуваного майбутнього.

Висновки до третього розділу

1. Розроблено концептуальну модель інституціалізації публічного управління національною безпекою в умовах гібридної війни, яка ґрунтується на принципово новій парадигмі інтегрованого системного підходу замість традиційного фрагментарного. Модель структурована навколо чотирнадцяти базових принципів, серед яких системна цілісність, адаптивна архітектура, мережецентричність, інформаційна інтеграція, проактивність, розподілена стійкість, інклюзивність, континуальність управління, технологічна інноваційність, стратегічна комунікація, правова легітимність, безперервне навчання, економічна ефективність. Кожен принцип отримав детальне теоретичне обґрунтування та практичну інтерпретацію з урахуванням

специфіки гібридних загроз. При цьому принциповою особливістю моделі є її багаторівнева архітектура, що охоплює стратегічний, оперативний та регіональний рівні з інноваційними елементами у вигляді функціональних кластерів замість традиційних відомчих структур, Національного центру стійкості для забезпечення безперебійного функціонування критичної інфраструктури, Регіональних центрів безпеки та стійкості як інтегрованих міжвідомчих структур на обласному рівні. Модель передбачає створення потужної мережевої компоненти з горизонтальними зв'язками між елементами різних рівнів, інформаційної підсистеми на базі концепції єдиного інформаційного простору, а також вбудованих механізмів адаптації до еволюції гібридних загроз через раннє виявлення слабких сигналів, сценарне прогнозування, організаційну та технологічну гнучкість.

2. Обґрунтовано систему механізмів координації в інтегрованій моделі управління національною безпекою, яка поєднує вертикальну та горизонтальну координацію на всіх рівнях управління. Вертикальна координація реалізується через каскадну систему узгодженого цілепокладання від Національної стратегії безпеки до річних планів діяльності конкретних відомств з використанням інструменту «стратегічних контрактів» між РНБО та керівниками безпекових відомств, що юридично закріплюють конкретні вимірювані результати. Горизонтальна координація на стратегічному рівні забезпечується через систему спеціалізованих міжвідомчих комітетів при РНБО з конкретних напрямків діяльності, на оперативному рівні – через спільні ситуаційні центри та міжвідомчі оперативні групи, на регіональному рівні – через Регіональні центри безпеки та стійкості. Інформаційний механізм координації базується на створенні Національної платформи безпекових даних з технологічною інтеграцією інформаційних систем всіх відомств та можливістю крос-відомчого доступу до релевантної інформації з дотриманням принципу необхідності знати. Процедурний механізм передбачає уніфікацію стандартів, протоколів, термінології та форматів документів для забезпечення інтероперабельності. Ресурсний механізм включає перехід від відомчого до

програмно-цільового фінансування через консолідований бюджет сектору безпеки і оборони та створення Агенції оборонних закупівель як єдиного закупівельного центру. Запропонована система механізмів координації забезпечує синергетичну взаємодію різних суб'єктів безпеки при збереженні їх функціональної спеціалізації та необхідної операційної автономії.

3. Розроблено комплексну систему правових механізмів удосконалення публічного управління національною безпекою, концептуальною основою якої є парадигмальний перехід від фрагментарного до інтегрованого системного підходу в правовому регулюванні. Обґрунтовано необхідність масштабної кодифікації безпекового законодавства через розробку Кодексу національної безпеки України з логічною структурою, що включає загальні положення, систему забезпечення національної безпеки, процедурні механізми, особливі правові режими, міжнародне співробітництво та юридичну відповідальність. Систематизовано десять пріоритетних напрямів модернізації законодавства: кодифікація безпекового законодавства, правове регулювання гібридних загроз, міжвідомча координація, розвідувальна діяльність, кібербезпека, інформаційна безпека, державна таємниця, участь громадянського суспільства, міжнародна гармонізація, механізми адаптації. Для кожного напрямку визначено ключові елементи та очікувані результати впровадження. законодавства до швидкої еволюції загроз через «сонячні норми», делеговане законодавство, регуляторні пісочниці та періодичний інституціоналізований перегляд.

4. Виявлено критичну важливість послідовної гармонізації національного законодавства про національну безпеку з міжнародним правом та стандартами НАТО і Європейського Союзу для забезпечення міжнародної підтримки України, євроатлантичної інтеграції та ефективної міжнародної безпекової кооперації. Обґрунтовано необхідність повноцінної імплементації стандартів НАТО щодо демократичного цивільного контролю над силовими структурами, включаючи принципи підзвітності парламенту, прозорості бюджетування та незалежного зовнішнього аудиту. Визначено потребу

адаптації правового доробку ЄС у сфері безпеки та оборони, включаючи регулювання оборонних закупівель, контроль експорту озброєнь, кібербезпеку та захист критичної інфраструктури. Водночас обґрунтовано необхідність збереження національної правової специфіки там, де вона виправдана українськими умовами, з урахуванням унікального практичного досвіду протидії повномасштабній гібридній агресії. Виявлено, що найбільш складним та довгостроковим аспектом правової модернізації є фундаментальна трансформація правової культури та правосвідомості в безпековій сфері від формалістичного дотримання букви закону до глибокого розуміння його духу, цілей та цінностей.

5. Розроблено систему організаційних механізмів трансформації сектору безпеки на засадах інтегрованого підходу, концептуальною основою якої є парадигмальний перехід від традиційного функціонально-галузевого до процесно-орієнтованого принципу побудови організаційних структур. Обґрунтовано необхідність системного виділення наскрізних міжвідомчих бізнес-процесів та створення спеціалізованих інтегрованих структур для їх реалізації з участю всіх релевантних суб’єктів безпеки. Ключовим практичним втіленням цього підходу визначено створення Інтегрованого командування сил безпеки та оборони як єдиного органу оперативного управління всіма силовими компонентами в кризових ситуаціях з реальними повноваженнями віддавати обов’язкові для виконання накази незалежно від відомчої підпорядкованості. Запропоновано трансформацію територіальної організації безпекових структур від жорсткої прив’язки до адміністративно-територіального устрою до гнучкої мережевої моделі з міжрегіональними оперативними командуваннями та високомобільними групами швидкого реагування.

6. Виявлено потенціал підвищення ефективності та економії ресурсів через послідовну оптимізацію структур матеріально-технічного та інформаційно-комунікаційного забезпечення з переходом від централізованої відомчої моделі дублюючого забезпечення до інтегрованої моделі спільних

міжвідомчих сервісів. Обґрунтовано доцільність створення єдиної консолідованої логістичної системи постачання, консолідованої системи урядового зв'язку та інформаційних технологій з єдиними стандартами, мережі спільних міжвідомчих навчальних центрів та єдиної інтегрованої медичної служби для всіх категорій силовиків. Визначено важливість широкого використання гнучких тимчасових проектних структур для вирішення специфічних завдань через оперативне формування міжвідомчих цільових груп, створення інноваційних лабораторій для експериментування з новими підходами, формування експериментальних пілотних підрозділів для тестування організаційних інновацій та створення «червоних команд» для виявлення вразливостей системи. Визначено стратегічну мету організаційної оптимізації як перехід від екстенсивної моделі нарощування чисельності до інтенсивної моделі підвищення якості через скорочення надлишкових управлінських ланок, технологічну автоматизацію рутинних функцій, аутсорсинг непрофільних функцій та підвищення частки висококваліфікованого оперативного складу.

ВИСНОВКИ

1. Доведено, що в умовах гібридної війни традиційні моделі інституціалізації, орієнтовані на стабільне безпекове середовище та лінійну логіку розвитку, виявляються недостатньо ефективними, оскільки не враховують необхідність одночасної адаптації до багатовекторних загроз, що діють синхронізовано у військовій, політичній, економічній, інформаційній та соціальній сферах. При цьому встановлено діалектичний характер взаємозв'язку між формальною та неформальною інституціалізацією, де формальні правила створюють структурні рамки, а неформальні практики визначають реальну ефективність функціонування інститутів, особливо в екстремальних умовах, коли швидкість реагування та гнучкість адаптації стають критичними факторами виживання системи. Виходячи з цього було запропоновано модель публічного управління національною безпекою в умовах гібридної війни, що базується на принципах багатовимірності, адаптивності та інтегрованості, що відрізняє її від традиційних моделей, орієнтованих на ієрархічність, сталість та секторальність. Модель включає три взаємопов'язані компоненти: структурно-організаційний (створення гнучких мережевих форм координації замість жорстких ієрархічних структур, формування міжвідомчих платформ взаємодії, розвиток механізмів публічно-приватного партнерства), процесуально-функціональний (стандартизація процедур ситуаційного аналізу та швидкого реагування, впровадження систем раннього попередження, автоматизація обміну інформацією між суб'єктами безпеки) та ціннісно-культурний (формування культури міжвідомчої співпраці, розвиток професійних компетенцій для роботи в умовах невизначеності, виховання стратегічного мислення у керівників безпекових структур). Впровадження даної моделі дозволяє забезпечити здатність системи публічного управління національною безпекою не лише протистояти деструктивним впливам, а й абсорбувати шоки, швидко відновлюватися після кризових ситуацій та еволюційно адаптуватися до нових типів загроз через

організаційне навчання та акумуляцію досвіду.

2. Концептуалізація гібридної війни як детермінанти трансформації системи публічного управління національною безпекою виявила її принципову відмінність від традиційних безпекових викликів через множинність, синхронність та синергетичність деструктивних впливів, що одночасно спрямовуються на всі виміри життєдіяльності держави та суспільства. Встановлено, що гібридна війна генерує каскадний ефект інституційної дестабілізації, коли первинний удар по одному сегменту безпекової системи провокує ланцюгову реакцію порушень у суміжних сферах, експоненційно збільшуючи загальний деструктивний вплив та створюючи ситуацію системної кризи. Завдяки цьому виявлено специфічні характеристики гібридних загроз, що фундаментально змінюють вимоги до інституційної організації управління національною безпекою: розмивання меж між війною і миром вимагає здатності інститутів функціонувати в режимі перманентної готовності; амбівалентність статусу агресора створює правову невизначеність та потребу в адаптації нормативної бази; асиметричність конфлікту зумовлює необхідність розробки нетрадиційних стратегій протидії; темпоральна невизначеність конфлікту вимагає формування інститутів, здатних до тривалого функціонування під навантаженням без організаційного виснаження. Визначено, що через ці характеристики гібридна війна впливає на інституційну систему одночасно на декількох рівнях: макрорівень (трансформація стратегічних пріоритетів державної політики), мезорівень (реорганізація відомчих структур та механізмів координації), мікрорівень (зміна повсякденних управлінських практик та процедур прийняття рішень), що вимагає комплексної та узгодженої інституційної відповіді на всіх рівнях організації системи.

3. Розроблено систему критеріїв та індикаторів оцінювання інституційної зрілості системи публічного управління національною безпекою, яка інтегрує сім взаємопов’язаних вимірів, що комплексно характеризують спроможність безпекових інститутів ефективно

функціонувати в умовах гібридних загроз. Структурна зрілість відображає повноту інституційної архітектури та чіткість розподілу повноважень; функціональна зрілість характеризує ефективність виконання безпековими інститутами покладених функцій; нормативна зрілість визначає якість правового забезпечення діяльності; координаційна зрілість оцінює ефективність механізмів міжвідомчої взаємодії; адаптивна зрілість вимірює здатність до швидкого реагування на нові виклики; культурна зрілість характеризує розвиненість організаційної культури та професійної етики; інтеграційна зрілість відображає включеність національної системи в міжнародні безпекові механізми. Встановлено, що між окремими вимірами інституційної зрілості існують нелінійні взаємозв'язки, коли дефіцит розвитку одного виміру не може бути повністю компенсований надрозвиненістю інших, що обґрунтовує необхідність збалансованого підходу до інституційного розвитку. Доведено, що в умовах гібридної війни найбільшого значення набувають адаптивна та координаційна зрілість, оскільки саме здатність до швидкої адаптації та ефективної міжвідомчої координації визначають результативність протидії багатовекторним асиметричним загрозам. Обґрунтовано методологічний підхід до комплексного оцінювання інституційної зрілості, який поєднує кількісні індикатори (ресурсне забезпечення, кількість міжвідомчих угод, термін реагування на інциденти) та якісні експертні оцінки (ефективність координації, рівень довіри, організаційна культура), що дозволяє отримати об'єктивну картину стану інституційного розвитку та обґрунтувати пріоритети подальших реформ.

4. Аналіз нормативно-правового та організаційного забезпечення системи управління національною безпекою України виявив динамічну еволюцію інституційного середовища під впливом гібридної війни, що проявилося у поетапній трансформації правової архітектури від фрагментарної адаптації до формування комплексної системи регулювання протидії багатовекторним загрозам. Виявлено, що еволюція нормативної бази демонструє перехід від вузького мілітаристського розуміння безпеки до

широкої концепції, що охоплює воєнну, політичну, економічну, інформаційну, кібернетичну, екологічну сфери, відповідаючи багатовимірній природі гібридної агресії. Поряд з цим дослідження практики інституційного реагування України на гібридну агресію у період 2014-2024 років дозволило виявити чотири послідовні фази адаптації, кожна з яких характеризується специфічною логікою інституційних трансформацій та різним рівнем ефективності протидії загрозам. Перша фаза (2014-2015 роки) характеризувалася шоковим реагуванням на несподівану агресію в умовах глибокої інституційної кризи, коли система національної безпеки виявилася неготовою до протидії гібридним методам ведення війни, що проявилося у втраті Криму, інституційному колапсі на Донбасі, необхідності імпровізованого формування нових силових структур на волонтерських засадах. Друга фаза (2016-2018 роки) демонструвала структурну стабілізацію та початок системних реформ через прийняття нового базового законодавства, реорганізацію збройних сил, створення нових безпекових інституцій, налагодження міжнародної співпраці, хоча темпи перетворень залишалися повільними через інституційну інерцію та відомчий опір змінам. Третя фаза (2019-2021 роки) відзначалася поглибленням інституційної трансформації через впровадження євроатлантичних стандартів, посилення спроможностей кіберзахисту та стратегічних комунікацій, накопичення бойового досвіду, модернізацію озброєння, хоча повна імплементація реформ стримувалася політичною нестабільністю. Четверта фаза (з 2022 року) продемонструвала якісно вищий рівень інституційної зрілості через ефективне стримування повномасштабного вторгнення, збереження системи управління, організовану оборону, успішні контрнаступальні операції, що засвідчило результативність проведених реформ. Виявлено закономірність, що найбільш динамічні інституційні зміни відбувалися в періоди загострення конфлікту, коли екстремальні виклики долали організаційний опір і створювали політичне вікно можливостей для впровадження болючих, але необхідних реформ.

5. Компаративний аналіз зарубіжного досвіду інституціалізації

управління національною безпекою в умовах гібридних загроз виявив конвергенцію інституційних відповідей країн, що зіткнулися з російською агресією або перебувають під загрозою такої, при збереженні національної специфіки імплементації загальних принципів. Встановлено, що країни Балтії (Естонія, Латвія, Литва) розробили найбільш релевантні для України моделі протидії гібридним загрозам через схожість викликів, обмеженість ресурсів, необхідність компенсувати відсутність стратегічної глибини через високу готовність суспільства та інституційну гнучкість. Естонський досвід демонструє ефективність побудови системи кіберзахисту на основі публічно-приватного партнерства, створення резервних систем управління та даних, інтеграції цифрових технологій у всі аспекти національної безпеки. Латвійська модель стратегічних комунікацій і протидії дезінформації, що включає створення спеціалізованого центру StratCom НАТО, розвиток медіаграмотності населення, міжвідомчу координацію інформаційної політики, виявилася особливо цінною для протидії російській пропаганді. Литовський досвід розбудови територіальної оборони та концепції національного опору, що передбачає підготовку населення до дій в умовах окупації, інтеграцію добровольчих формувань у систему безпеки, соціальну згуртованість через спільне протистояння загрозам, має пряму релевантність для України. Фінська концепція всеосяжної безпеки (comprehensive security), що базується на залученні всіх секторів суспільства до забезпечення стійкості, створенні запасів критичних ресурсів, підготовці до автономного функціонування в умовах кризи, продемонструвала ефективність проактивного підходу. Польський досвід масштабного посилення збройних сил як стримуючого фактора в поєднанні з активною регіональною безпековою дипломатією показує важливість видимої військової потужності. Виявлено спільні елементи успішних моделей: створення координаційних центрів протидії гібридним загрозам на вищому державному рівні; розбудова спроможностей кіберзахисту критичної інфраструктури; системи стратегічних комунікацій та контрпропаганди; механізми залучення громадянського

суспільства до національної безпеки; міжнародна кооперація та обмін досвідом.

6. Розроблено концептуальну модель інституціалізації публічного управління національною безпекою в умовах гібридної війни, яка вперше об’єднує в органічну систему принципи функціонування, архітектурні елементи, механізми координації та адаптаційні спроможності, необхідні для ефективної протидії багатовимірним динамічним загрозам. Модель спирається на чотирнадцять взаємопов’язаних базових принципів, що формують самоузгоджену систему, де кожен принцип не лише виконує власну функцію, а й компенсує потенційні обмеження інших, забезпечуючи баланс між такими діалектичними протиріччями як стабільність та гнучкість, централізація та децентралізація, секретність та прозорість. Принциповою особливістю запропонованої архітектури є відмова від традиційного відомчого підходу на користь функціональної інтеграції через створення кластерів споріднених функцій, що дозволяє уникнути дублювання зусиль та забезпечити синергію. Запровадження нових інституційних елементів – Національного центру стійкості для захисту критичної інфраструктури та Регіональних центрів безпеки як інтегрованих міжвідомчих хабів – формує якісно нову конфігурацію взаємодії між центральним та регіональним рівнями управління. Мережева логіка з потужними горизонтальними зв’язками та єдиним інформаційним простором руйнує традиційні бюрократичні бар’єри між відомствами. Критичним досягненням є органічне вбудовування адаптаційних механізмів безпосередньо в архітектуру системи, що забезпечує її коеволюцію разом із загрозами через концепцію «периферійного зору» для виявлення слабких сигналів, сценарне прогнозування з використанням комп’ютерного моделювання, модульну організаційну гнучкість, технологічний радар для моніторингу подвійних технологій та когнітивну різноманітність для подолання упереджень. Метаадаптивність як здатність вдосконалювати самі адаптаційні механізми створює позитивну спіраль еволюції, що забезпечує довгострокову стійкість системи навіть до

принципово нових, ще невідомих форм гібридної агресії.

7. Розроблено комплексну систему правових та організаційних механізмів удосконалення публічного управління національною безпекою, практична реалізація яких забезпечить трансформацію сектору безпеки до якісно нового стану ефективності. Правові механізми базуються на парадигмальному переході від фрагментарного до інтегрованого системного підходу в правовому регулюванні через масштабну кодифікацію безпекового законодавства у формі Кодексу національної безпеки України, введення в правове поле нових концепцій гібридної агресії, гібридної оборони та критичної інформаційної інфраструктури, створення дійсно ефективного правового забезпечення міжвідомчої координації через імперативний характер координаційних рішень та персональну відповідальність керівників, комплексну модернізацію законодавства про розвідувальну діяльність, кібербезпеку та інформаційну безпеку з балансуванням між безпековими потребами та демократичними цінностями, послідовну гармонізацію з міжнародним правом та стандартами НАТО і ЄС, впровадження інноваційних механізмів адаптації законодавства через «сонячні норми», делеговане законодавство та регуляторні пісочниці. Організаційні механізми передбачають парадигмальний перехід від функціонально-галузевого до процесно-орієнтованого принципу побудови структур через створення Інтегрованого командування сил безпеки та оборони з реальними повноваженнями оперативного управління всіма силовими компонентами, глибоку реорганізацію розвідувальної спільноти через Національне розвідувальне агентство як єдиний аналітично-координаційний центр, трансформацію територіальної організації до гнучкої мережевої моделі з міжрегіональними командуваннями та мобільними групами, структурну інтеграцію кіберсил через об’єднане Кіберкомандування, послідовну консолідацію забезпечувальних функцій у формі спільних міжвідомчих сервісів, широке використання гнучких тимчасових проектних структур та систему механізмів стимулювання міжвідомчої інтеграції. Обґрунтовано, що

найбільш складним та довгостроковим аспектом модернізації є фундаментальна трансформація організаційної культури та правосвідомості в безпековій сфері від формалістичного дотримання букви закону до глибокого розуміння його духу та від відомчого егоїзму до системного бачення національної безпеки. Практична реалізація запропонованої системи механізмів забезпечить створення якісно нової інтегрованої системи управління національною безпекою, здатної ефективно протидіяти комплексним гібридним загрозам через синергетичну взаємодію всіх суб'єктів безпеки, випереджувальну адаптацію до еволюції загроз та безперервне самовдосконалення на основі накопиченого досвіду.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакумов В. М. Правове регулювання протидії інформаційним війнам в Україні : автореф. дис. ... канд. юрид. наук : 12.00.07 / Класич. приват. ун-т. Запоріжжя, 2011. 19 с.

2. Агаєв Н. А., Базарний В. Т., Мацагор О. Н. та ін. Україна в умовах воєнно-політичного конфлікту: історія та сучасність. К. : ФОП Маслаков, 2018. 47 с.

3. Агресія Росії проти України: історичні передумови та сучасні виклики / П. П. Гай-Нижник та ін. ; під заг. ред. П. П. Гай-Нижника. Київ : МП Леся, 2016. 586 с.

4. Бакуменко В. Д. Формування державно-управлінських рішень: проблеми теорії, методології, практики. Київ: УАДУ, 2000. 328 с.

5. Бегма В.М. Стратегічне управління експортом продукції військового призначення та подвійного використання в контексті економічної безпеки держави : дис… д-ра екон. наук : 21.04.01. К., 2004. 393 с.

6. Бєлай С. В. Підходи до оцінювання соціально-економічної безпеки регіонів України. *Державне управління та місцеве самоврядування* : тези XI Міжнар. наук. конгресу (Харків, 24 берез. 2011 р.). Харків : Магістр, 2011. С. 232–234.

7. Біла книга-2021: Оборонна політика України. Київ: Міністерство оборони України, 2022. 124 с.

8. Білоконь М. В. Ентропія як виклик інституційній стійкості публічного управління в умовах гібридних загроз. *Актуальні проблеми державного управління*. 2025. Vol.1, No 66. С. 179–195.

9. Білоконь М.В., Мирна Н.В. Інституційна синергія як чинник стійкості публічного управління у сфері обігу лікарських засобів: моделі взаємодії в умовах європейської інтеграції та безпекової турбулентності. *Актуальні питання у сучасній науці*. 2025. № 6(36). С. 110-122.

10. Богданович В.Ю., Прима А.М. Методичний підхід до визначення

необхідних спроможностей складових інтегрованого потенціалу протидії загрозам на виконавчому рівні. *Наука і техніка Повітряних сил Збройних Сил України*. 2017. № 2(27). С. 162-166.

11. Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. Теоретико-методологічні основи забезпечення національної безпеки України: моногр. у 7 т. Т. 1: Теоретичні основи, методи й технології забезпечення національної безпеки України. К.: Наук.-вид. відділ НА СБ України, 2012. 548 с.

12. Бондар З. К., Житник О. М., Шевченко М. М. Система критеріїв та показників оцінки ефективності стратегічного планування у сфері національної безпеки. *Інвестиції: практика та досвід*. 2017. № 17. С. 110–114.

13. Величко Л. Ю., Пупяліс Є.В. Особливості публічного управління в умовах гібридних війн. *Суспільство та національні інтереси*. 2025. № 6(14). С. 634-647.

14. Величко Л. Ю., Пупяліс Є.В. Стратегічна культура як чинник публічного управління національною безпекою в умовах гібридної війни. *Матеріали VIII Міжнародної науково-практичної конференції «Міжнародна та національна безпека: теоретичні і прикладні аспекти»*. С. 397-400.

15. Виклики і загрози національній безпеці в умовах гібридної війни : матеріали наук.-практ. семінару (Київ, 27 квіт. 2017 р.) / за ред. Л. М. Шипілової. Київ : НАДУ, 2017. 104 с.

16. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики. Київ: НІСД, 2016. 528 с.

17. Волянюк О., Притула Х. Гібридна війна у вимірі стратегічних комунікацій. *Науковий часопис УДУ ім. Михайла Драгоманова*. 2025. Вип. 37. С. 97-109.

18. Вплив глобальних політичних, енергоресурсних та екологічних змін на воєнну безпеку держави / В. В. Зубарєв та ін. Київ : Інтертехнологія, 2009. 256 с.

19. Галанюк Я. С. Теоретичні основи взаємодії органів публічної влади з Державною прикордонною службою України у сфері прикордонної безпеки.

Науково-інформаційний вісник Академії національної безпеки. 2015. № 3–4 (7–8). С. 104–115.

20. Гібадуллін О.В., Дунаєв І.В., Громов С.О. Складові системи промислового відновлення регіонів в умовах воєнного стану в Україні. *Вісник післядипломної освіти: Серія «Соціальні та поведінкові науки; Управління та адміністрування»*. 2024. Вип. 28 (57). С. 174-205.

21. Глобальна та національна безпека : підручник / В. І. Абрамов, Г. П. Ситник, М. М. Шевченко та ін. ; за заг. ред. Г. П. Ситника. Київ : НАДУ, 2016. 748 с.

22. Горбулін В. П. Як перемогти Росію у війні майбутнього. Київ: Брайт Букс, 2021. 248 с.

23. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки : монографія. Київ : НІСД, 2011. 288 с.

24. Горбулін В.П., Качинський А.Б. Системно-концептуальні засади стратегії національної безпеки України: монографія. К.: ДП «НВЦ «Євроатлантикінформ», 2007. 592 с.

25. Деякі питання здійснення оборонних та публічних закупівель товарів, робіт і послуг в умовах воєнного стану: Постанова Кабінету Міністрів України від 28 лютого 2022 р. № 169. URL: https://zakon.rada.gov.ua/laws/show/169-2022-%D0%BF/en/ed20220713#Text.

26. Дєгтяр А. О. Державно-управлінські рішення: інформаційно-аналітичне та організаційне забезпечення. Харків : Магістр, 2004. 224 с.

27. Дєгтяр О.А., Носков О.О., Мілевський К.В. Інформаційна безпека у сфері національної безпеки України в умовах сучасних викликів. *Національні інтереси України*. 2025. № 4(9). С. 117-129.

28. Дзьобань О. П. Інформаційна безпека України в умовах формування інформаційного суспільства: соціально-філософський аналіз. Харків : Майдан, 2011. 436 с.

29. Дзьобань О. П. Національна безпека в умовах соціальних

трансформацій (теоретико-методологічний аналіз) : автореф. дис. ... д-ра філос. наук : 21.03.01 / НІСД. Київ, 2005. 32 с.

30. Дзюндзюк В.Б. Цифрова трансформація публічного управління національною безпекою в умовах гібридної війни. *Актуальні проблеми державного управління*. 2025. № 2 (67). С. 60-74.

31. Дунаєв І. В., Соловйов Є. В. Публічне управління інтелектуальними ресурсами національної безпеки: які перспективи у ідеї регіональних хабів експертних ресурсів? *Державне будівництво*. 2024. № 2(36). С.219-253.

32. Дунаєв І.В. Залучення стейкхолдерів до технічного регулювання залізничного транспорту України: як балансувати суспільною безпекою, галузевими потребами та операційною ефективністю? *Національні інтереси України*. 2025. №4 (9). С. 749-767.

33. Дунаєв І.В., Кокорєв В.В. Інституційні механізми залучення малого та середнього підприємництва до забезпечення економічної стійкості в умовах триваючої та гібридної війни. *Актуальні питання у сучасній науці (Серія Публічне управління)*. 2026. №1/43. С. 349-361.

34. Завгородня С. П. Оцінювання ефективності системи державного управління у сфері економічної безпеки України. *Науково-інформаційний вісник Академії національної безпеки*. 2016. № 3–4 (11–12). С. 96–112.

35. Константинюк С. Державна культурна політика як елемент національної політики безпеки: досвід України (2014-2022 рр.). *Історико-політичні проблеми сучасного світу*. 2023. Т. 47. С. 219-227

36. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

37. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. Київ : Кондор, 2004. 384 с.

38. Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення : монографія. Львів : Сполом, 2020. 418 с.

39. Майстренко О. В. Взаємовплив можливостей військових

формувань щодо вогневого ураження противника. К. : НУОУ, 2017. 180 с.

40. Марутян Р. Р. Інтелектуальне забезпечення державного управління національною безпекою: вдосконалення та розвиток. *Науково-інформаційний вісник Академії національної безпеки*. 2014. № 1 (1). С. 120–126.

41. Мас-медіа. Демократія, Інформаційна війна : науково-практичне видання / за заг. ред. С. Ф. Джерджа. Київ : СПД Матвієнко, 2014. 78 с.

42. Мельниченко О.А., Макарова В.І., Старусева В.В. Екологічна безпека: значення та взаємозв'язок з іншими складовими національної безпеки. *Національні інтереси України*. 2025. № 5 (10). С. 1164–1173.

43. Мельниченко О.А., Стовбан М.П., Кравченко Ж.Д., Чернецький В.В. Протидія рейдерству як складова державної політики щодо забезпечення національної безпеки. *Національні інтереси України*. 2025. № 4 (9). С. 885–896.

44. Методологія стратегічного планування в умовах глобальних загроз національній безпеці та міжнародній стабільності : монографія / В. І. Абрамов, Т. В. Запорожець, Р. Р. Марутян та ін. ; за заг. ред. Л. М. Шипілової. Київ : НАДУ, 2018. 232 с.

45. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький. Київ, 2022. 552 с.

46. Нестеренко О.В., Савенков О.І., Фаловський О.О. Інтелектуальні системи підтримки прийняття рішень К: НАУ, 2016. 188 с.

47. Орел М. Г. Теоретичні основи державного управління у сфері політичної безпеки: монографія. Київ: Поліграф Плюс «Ц-СІ», 2019. 320 с.

48. Остапчук В.М., Дєгтяр О.А. Механізми публічного управління оборонною та безпековою політикою європейського союзу. *Національні інтереси України*. 2025. № 5(10). С. 1199-1211.

49. Парахонський Б. О., Яворська Г. М. Актуальні виклики та загрози регіональній безпеці: висновки для України : аналіт. доп. / за заг. ред. К. А.

Кононенка. Київ : НІСД, 2014. 48 с.

50. Пелих А. О., Шевченко М. М. Оцінка можливостей використання в Україні досвіду європейських країн щодо забезпечення національної безпеки: методологічний та практичний аспекти. *Реструктурізація глобального простору: історичні імперативи та виклики* : матеріали IV Міжнар. наук.-практ. конф. (Київ, 23 квіт. 2015 р.). Київ : ДАУ при МЗС України, 2015. С. 149–152.

51. Пилипчук В. Г. Проблеми дослідження новітньої історії органів безпеки та розвідки в контексті розвитку сектору безпеки України. *Стратегічні пріоритети*. 2012. № 3 (24). С. 114–119.

52. Пилипчук В.Г., Доронін І.М., Право національної безпеки та військове право: теоретичні та прикладні засади становлення і розвитку в Україні. Інформація і право. 2018. № 2(25). С. 62-72.

53. Поляков А. П. Сучасний стан та перспективи розвитку ЗС України: навчальний посібник. Вінниця: ВНТУ, 2016. 103 с.

54. Почепцов Г. Г. Смисли і війни: Україна і Росія в інформаційній і смислових війнах. Київ : Видавничий дім «Києво-Могилянська академія», 2016. 316 с.

55. Про внесення змін до деяких законодавчих актів України щодо розвідувальних органів України: Закон України, редакція від 01.01.2022. URL: https://zakon.rada.gov.ua/laws/show/3200-15#Text.

56. Про Кабінет Міністрів України: Закон України від 27.02.2014 № 794-VII. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text.

57. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

58. Про оборону України: Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

59. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

60. Про парламентський контроль у сфері національної безпеки і оборони: проект Закону України № 6543 від 28.12.2021. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=73515

61. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.

62. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text.

63. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

64. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України»: Указ Президента України від 25.03.2021 № 121/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/4860.html.

65. Про розвідку: Закон України від 17.09.2020 № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text.

66. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text.

67. Пупяліс Є.В. Адаптація системи національної безпеки до викликів гібридної агресії. *Матеріали XXV Міжнародного наукового конгресу «Публічне управління XXI століття: основні виклики післявоєнної відбудови»*. С. 218-222.

68. Пупяліс Є.В. Зарубіжний досвід інституціалізації управління національною безпекою в умовах гібридних загроз: можливості для України. *Національні інтереси України*. № 11(16), 2025. С. 1317-1328.

69. Пупяліс Є.В. Концептуальна модель інституціалізації публічного управління національною безпекою в умовах гібридної війни. *Актуальні проблеми державного управління*. 2025. № 2 (67). С. 285-302.

70. Пупяліс Є.В. Розвиток інституційної спроможності публічного управління у протидії гібридним загрозам національній безпеці. Наукові інновації та передові технології. 2025. № 6(46). С. 253-264.

71. Резнікова О. Національна стійкість в умовах мінливого безпекового середовища. Київ : НІСД, 2022. 456 с.

72. Романенко Є.О., Гурковський В.І., Дєгтяр О.А. Управління інформаційною безпекою оборони. *Національні інтереси України*. 2025. № 7(12). С. 227-235.

73. Саганюк Ф.В., Устименко О.В., Лобко М.М.та ін. Сектор безпеки і оборони України: теорія, стратегія, практика. К.: Академпрес, 2017. 182 с.

74. Сегеда С.П., Шевчук В.П. Гібридна війна Росії проти України: історичний вимір. Наука і оборона. 2019. № 1. С. 31-35.

75. Сектор безпеки і оборони України: стратегічне планування / Ф. В. Саганюк, М. М. Лобко, О. В. Устименко, А. К. Павліковський ; за ред. Р. І. Тимошенка. Київ : Майстер книг, 2016. 248 с.

76. Семенченко А. І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України. К.: НАДУ, 2008. 429 с

77. Семенченко А. І. Стратегічне планування у сфері державного управління національною безпекою : автореф. дис. ... док. наук з держ. упр. : 25.00.02 / НАДУ. Київ, 2008. 36 с.

78. Сенченко О. М. Інформаційно-мережеві війни: теорія, моделі, алгоритми : монографія. Київ : КВІЦ, 2017. 332 с.

79. Ситник Г. П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади). Київ: НАДУ, 2012. 544 с.

80. Сніцаренко П. М., Саричев Ю. О. Теоретичні підходи до визначення сутності інформаційного забезпечення в системі державного управління. *Науково-інформаційний вісник Академії національної безпеки*. 2016. № 1–2 (9–10). С. 7–19.

81. Соколов В. А. Роль класифікації аналітичної діяльності за

професором Ю. Сурміним в емпіричних узагальненнях у сфері національної безпеки. *Проблеми управління соціальним і гуманітарним розвитком* : матеріали X регіон. наук.-практ. конф. Дніпро : ДРІДУ НАДУ, 2016. С. 9–10.

82. Соколов В. А. Типова модель гібридної війни: сутність і сучасне підтвердження. *Виклики і загрози національній безпеці в умовах гібридної війни* : матеріали наук.-практ. семінару (Київ, 27 квіт. 2017 р.) / за заг. ред. Л. М. Шипілової. Київ : НАДУ, 2017. С. 92–94.

83. Стратегія громадської безпеки та цивільного захисту України. URL: https://mvs.gov.ua/ministry/normativna-baza-mvs/proekti-normativnix-aktiv/strategiya-gromadskoyi-bezpeki-ta-civilnogo-zaxistu-ukrayini-zatverdzeno-vid-29062021.

84. Теоретико-методологічні засади формування кадрової безпеки в системі публічного управління : кол. моногр. / С. О. Борисевич, В. І. Абрамов, В. Ф. Смолянюк, М. М. Шевченко ; за заг. ред. С. О. Борисевича. Київ : НАДУ, 2014. 248 с.

85. Ткач І. М. Концептуальні засади воєнно-економічної безпеки держави: монографія. Київ : НУОУ ім. І. Черняховського, 2018. 312 с.

86. Толубко В. Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія. Київ : НАОУ, 2003. 320 с.

87. Требін М. П. Армія та суспільство: соціально-філософський аналіз взаємодії в умовах трансформації. Харків : Видавничий дім «Інжек», 2004. 404 с.

88. Турченко Ф., Турченко Г. Проект «Новоросія» і новітня російсько-українська війна. К. : Інститут історії України, 2015.166 с.

89. Черненко Т.В. Пріоритети державної інформаційної політики в умовах гібридної війни. *Стратегічні пріоритети*. 2015. № 4 (37). С. 83–92.

90. Шевченко М. М. Система стратегічного планування у сфері національної безпеки: методологічні засади формування та розвитку. *Науково-інформаційний вісник Академії національної безпеки*. 2015. № 1-2. С. 34–45.

91. Ясюк О.М., Дєгтяр О.А. Методологія дослідження публічного

управління сферою оборони в Україні. *Суспільство та національні інтереси*. 2025. № 3(11). С. 1060-1068.

92. Abbott A. Time Matters: On Theory and Method. Chicago: University of Chicago Press, 2001. 296 p.

93. Allison G. T., Zelikow P. Essence of Decision: Explaining the Cuban Missile Crisis. 2nd ed. New York: Longman, 1999. 416 p.

94. Andreas P., Nadelmann E. Policing the Globe: Criminalization and Crime Control in International Relations. Oxford: Oxford University Press, 2008. 352 p.

95. Angrist J. D., Pischke J.-S. Mostly Harmless Econometrics: An Empiricist's Companion. Princeton: Princeton University Press, 2009. 392 p.

96. Arquilla J., Ronfeldt D. Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica: RAND Corporation, 2001. 377 p.

97. Arutunyan A. Hybrid Warriors: Proxies, Freelancers and Moscow's Struggle for Ukraine. London: Hurst, 2022. 306 p.

98. Ashby W. R. An Introduction to Cybernetics. London: Chapman & Hall, 1956. 295 p.

99. Avant D. D. Political Institutions and Military Change: Lessons from Peripheral Wars. Ithaca: Cornell University Press, 1994. 176 p.

100. Badrak V. Creation of the defense shield of Ukraine. Designers and managers. Kyiv: TsDAKR, 2018. 161 p.

101. Baldwin D. A. The concept of security. Review of International Studies. 1997. Vol. 23, No. 1. P. 5–26.

102. Bertalanffy L. von. General System Theory: Foundations, Development, Applications. New York: George Braziller, 2015. 295 p.

103. Blackwill R. D., Harris J. M. War by Other Means: Geoeconomics and Statecraft. Cambridge: Harvard University Press, 2016. 384 p.

104. Boot M. The Road Not Taken: Edward Lansdale and the American Tragedy in Vietnam. New York: Liveright, 2019. 768 p.

105. Born H., Caparini M., Fluri P. Security Sector Reform and Democracy

in Transitional Societies. Baden-Baden: Nomos, 2002. 248 p.

106. Boyd J. R. A Discourse on Winning and Losing. Maxwell: Air University Press, 2018. 400 p.

107. Bryden A., Hänggi H. Reform and Reconstruction of the Security Sector. Geneva: DCAF, 2004. 323 p.

108. Bryson J. M. Strategic Planning for Public and Nonprofit Organizations. 5th ed. San Francisco: Jossey-Bass, 2018. 576 p.

109. Buzan B., Hansen L. The Evolution of International Security Studies. Cambridge: Cambridge University Press, 2009. 400 p.

110. Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers, 1998. 239 p.

111. Caliskan M. Modern Political Warfare: Current Practices and Possible Responses. *The RUSI Journal*. 2019. Vol. 164(2). P. 84-86

112. Cederberg A., Eronen P. How Can Societies Be Defended against Hybrid Threats? Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2019. 15 p.

113. Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, *Democracy, and National Security. California Law Review.* 2019. Vol. 107. P. 1753–1820.

114. Cohen R.S. et al. The Future of Warfare in 2030. Santa Monica: RAND, 2020. 103 p.

115. Creswell J. W., Plano Clark V. L. Designing and Conducting Mixed Methods Research. 3rd ed. Los Angeles: SAGE Publications, 2018. 520 p.

116. Cullen P. J., Reichborn-Kjennerud E. Understanding Hybrid Warfare. MCDC Countering Hybrid Warfare Project. Norfolk: MCDC, 2017. 36 p.

117. Diegtiar A., Bilokon M. Institutional Resilience of Public Administration Under Hybrid Threats: Economic and Socio-Humanitarian Countermeasures. *Global Scientific Trends: Economics and Public Administration*. 2025. Vol. 4. URL: https://gst-journal.net.ua/index.php/gst/article/view/61.

118. DiMaggio P. J., Powell W. W. The Iron Cage Revisited: Isomorphism in

Organizational Fields. *American Sociological Review*. 2000. Vol. 48, No. 2. P. 147–160.

119. Drezner D. W. The Sanctions Paradox: Economic Statecraft and International Relations. Cambridge: Cambridge University Press, 1999. 364 p.

120. Eisenkot G., Siboni G. Guidelines for Israel's National Security Strategy. Tel Aviv: INSS, 2019. 78 p.

121. European Commission. A Strategic Compass for Security and Defence. Brussels: EEAS, 2022. 47 p.

122. Explaining Institutional Change: Ambiguity, Agency, and Power / ed. by J. Mahoney, K. Thelen. Cambridge: Cambridge University Press, 2010. 236 p.

123. France's Defence Strategy in the Indo-Pacific. Paris: MDA, 2019. 32 p.

124. Freedman L. Command: The Politics of Military Operations from Korea to Ukraine. London: Allen Lane, 2022. 608 p.

125. Fridman O. Russian «Hybrid Warfare»: Resurgence and Politicisation. London: Hurst & Company, 2018. 288 p.

126. Galeotti M. Russian Political War: Moving Beyond the Hybrid. London: Routledge, 2020. 136 p.

127. Galeotti M. The Weaponisation of Everything: A Field Guide to the New Way of War. New Haven: Yale University Press, 2023. 248 p.

128. Giles K. Moscow Rules: What Drives Russia to Confront the West. London: Royal Institute of International Affairs, 2019. 234 p.

129. Giles K. Russia's War on Everybody: And What it Means for You. London: Bloomsbury, 2023. 246 p.

130. Glenn R. W. Rethinking Western Approaches to Counterinsurgency. London: Routledge, 2015. 330 p.

131. Gray C. S. Modern Strategy. Oxford: Oxford University Press, 1999. 412 p.

132. Haken H. Synergetics: An Introduction. Berlin: Springer-Verlag, 1983. 355 p.

133. Hänggi H. Making Sense of Security Sector Governance. Geneva:

DCAF, 2003. P. 3–23.

134. HM Government. Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy. London: Cabinet Office, 2021. 114 p.

135. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 2007. 72 p.

136. Holling C. S. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*. 1973. Vol. 4. P. 1–23.

137. Hollnagel E., Woods D. D., Leveson N. Resilience Engineering: Concepts and Precepts. Aldershot: Ashgate, 2006. 397 p.

138. Human Development Report 1994: New Dimensions of Human Security. New York: Oxford University Press, 1994. 226 p.

139. Huntington S. P. The Soldier and the State: The Theory and Politics of Civil-Military Relations. Cambridge: Harvard University Press, 1957. 534 p.

140. Hybrid Threats: A Comprehensive Resilience Ecosystem. Helsinki: Hybrid CoE, 2023. 124 p.

141. Jackson R., Sørensen G. Introduction to International Relations: Theories and Approaches. 6th ed. Oxford: Oxford University Press, 2016. 384 p.

142. Jaekyu J. Quantum Technology and South Korea’s Defense Innovation 4.0. *Journal of Peace and Unification*. 2025. 15(1). P.43-69.

143. Jane’s Defence Weekly. Ukraine’s Defence Modernisation Programme 2021-2025. London: Janes, 2021. P. 14–19.

144. Jervis R. System Effects: Complexity in Political and Social Life. Princeton: Princeton University Press, 1997. 318 p.

145. Kaplan R. S., Norton D. P. Strategy Maps: Converting Intangible Assets into Tangible Outcomes. Boston: Harvard Business Review Press, 2004. 392 p.

146. Kaplan R. S., Norton D. P. The Balanced Scorecard: Translating Strategy into Action. Boston: Harvard Business Review Press, 1996. 336 p.

147. Kauffman S. A. The Origins of Order: Self-Organization and Selection in Evolution. Oxford: Oxford University Press, 1993. 734 p.

148. Kegan R., Lahey L. L. Immunity to Change: How to Overcome It and Unlock the Potential in Yourself and Your Organization. Boston: Harvard Business Review Press, 2009. 368 p.

149. Kello L. The Virtual Weapon and International Order. New Haven: Yale University Press, 2018. 336 p.

150. Kiel Institute for the World Economy. Ukraine Support Tracker. Kiel: IfW, 2023. URL: https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/

151. Kilcullen D. Out of the Mountains: The Coming Age of the Urban Guerrilla. Oxford: Oxford University Press, 2013. 352 p.

152. Kilcullen D. The Dragons and the Snakes: How the Rest Learned to Fight the West. Oxford: Oxford University Press, 2020. 336 p.

153. Krahmann E. States, Citizens and the Privatisation of Security. Cambridge: Cambridge University Press, 2010. 312 p.

154. Krieg A., Rickli J.-M. Surrogate Warfare: The Transformation of War in the Twenty-First Century. Washington: Georgetown University Press, 2019. 264 p.

155. Lasconjarias G., Larsen J.A. (Eds.) NATO's Response to Hybrid Threats. *NDC Forum Papers 24, December 2015*. 372 p.

156. Lazer D. et al. Computational Social Science. *Science*. 2009. Vol. 323, No. 5915. P. 721–723.

157. Lefebvre V. A., Lefebvre V. D. Reflexive Control: The Soviet Concept of Influencing an Adversary's Decision Making Process. London: Science Applications, Incorporated, 1984. 172 p.

158. Lin H., Zegart A. Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations. Washington: Brookings Institution Press, 2019. 438 p.

159. Lucas E. The New Cold War: Putin's Russia and the Threat to the West. London: Bloomsbury, 2014. 384 p.

160. Mahnken T. G. Cyber war and Cyber warfare. In America's Cyber Future Security and Prosperity in the Information Age volume II, K. M. Lord and T. Sharp, Eds. Washington D.C.: Center for New American Security, 2011 P. 57 - 64

161. Mahoney J., Thelen K. (Eds.) Explaining Institutional Change: Ambiguity, Agency, and Power. Cambridge: Cambridge University Press, 2010. 254 p.

162. Mandelbrot B. B. The Fractal Geometry of Nature. New York: W. H. Freeman and Company, 1982. 468 p.

163. March J. G., Olsen J. P. Rediscovering Institutions: The Organizational Basis of Politics. New York: Free Press, 1989. 227 p.

164. Matei F. C., Halladay C., Bruneau T. C., The Routledge Handbook of Civil-Military Relations. London: Routledge, 2021. 406 p.

165. Mazarr M. J. Understanding Deterrence. *NL ARMS Netherlands Annual Review of Military Studies*. 2020 . P. 13-28.

166. Mazarr M.J. Mastering the Gray Zone: Understanding a Changing Era of Conflict. Washington: Lulu Press, 2015. 154 p.

167. Ministère des Armées. Strategic Update 2021. Paris: DICoD, 2021. 48 p.

168. Ministry of Defence of Estonia. National Defence Development Plan 2022-2031. Tallinn: MoD Estonia, 2022. 36 p.

169. Ministry of Defense of Japan. Defense of Japan 2023. Tokyo: MoD Japan, 2023. 32 p.

170. Mintzberg H., Ahlstrand B., Lampel J. Strategy Safari: The Complete Guide Through the Wilds of Strategic Management. 2nd ed. Harlow: Prentice Hall, 2009. 416 p.

171. Mitchell M. Complexity: A Guided Tour. Oxford: Oxford University Press, 2009. 368 p.

172. Monaghan A. Dealing with the Russians. Cambridge & Medford, MA: Polity Press, 2019. 164 p.

173. Moore M. H. Creating Public Value: Strategic Management in Government. Cambridge: Harvard University Press, 1995. 402 p.

174. Moore M. H. Recognizing Public Value. Cambridge: Harvard University Press, 2013. 484 p.

175. Morgan P. The Concept of Capacity. Maastricht: ECDPM, 2006. 22 p.

176. National Security Strategy 2021. Madrid: Estugraf, 2021. 114 p.

177. NATO Strategic Communications Centre of Excellence. Russia's Footprint in the Nordic-Baltic Information Environment. Riga: NATO StratCom COE, 2020. 124 p.

178. NATO. NATO 2030: United for a New Era. Brussels: NATO Public Diplomacy Division, 2020. 68 p.

179. Netherlands Ministry of Defence. Defence White Paper 2022. The Hague: Ministry of Defence, 2022. 72 p.

180. Norheim-Martinsen P. M. The European Union and Military Force: Governance and Strategy. Cambridge: Cambridge University Press, 2013. 248 p.

181. North D. C. Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press, 1990. 152 p.

182. Ostrom E. Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge: Cambridge University Press, 1990. 280 p.

183. Parsons T. The Social System. London: Routledge, 1991. 575 p.

184. Paul C. Strategic Communication: Origins, Concepts, and Current Debates. Santa Barbara: Praeger, 2011. 256 p.

185. Peters B. G. Institutional Theory in Political Science: The New Institutionalism. 4th ed. Cheltenham: Edward Elgar Publishing, 2019. 296 p.

186. Polyakova A., Boyer S. P. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. Washington: Brookings Institution, 2018. 23 p.

187. Pomerantsev P. Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia. New York: PublicAffairs, 2014. 241 p.

188. Posen B. R. The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars. Ithaca: Cornell University Press, 1984. 283 p.

189. Prigogine I., Stengers I. Order Out of Chaos: Man's New Dialogue with Nature. London: Bantam Books, 1984. 349 p.

190. Puglerin J. The Role of Civil Society in Ukraine's Defence against Russian Aggression. Berlin: DGAP, 2022. 28 p.

191. Renz B. Russia’s Military Revival. Cambridge: Polity Press, 2018. 240 p.

192. Repko A. F., Szostak R. Interdisciplinary Research: Process and Theory. 3rd ed. Los Angeles: SAGE Publications, 2016. 464 p.

193. Resnik D. B. The Ethics of Science: An Introduction. London: Routledge, 1998. 221 p.

194. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020. 513 p.

195. Rid T., Buchanan B. Attributing Cyber Attacks. *Journal of Strategic Studies*. 2015. Vol. 35. No. 1. P. 4-37.

196. Rogulis, D. Understanding Lithuania’s total defence approach in the face of Russian threat through principal–agent theory. *Security and Defence Quarterly*. 2025. 49(1). P. 58–73

197. Rostoks T., Sprūds A. (eds.) The Different Faces of "Soft Power": the Baltic States and Eastern Neighbourhood between Russia and the EU. Latvian Institute of International Affairs, 2015. 256 p.

198. Russia’s Strategy in Cyberspace. Riga: NATO StratCom COE, 2021. 42 p.

199. Sagan S. D. The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton: Princeton University Press, 1993. 286 p.

200. Schein E. H. Organizational Culture and Leadership. 5th ed. San Francisco: Jossey-Bass, 2017. 416 p.

201. Schoemaker P. J. H. Scenario Planning: A Tool for Strategic Thinking. *Sloan Management Review*. 1995. Vol. 36, No. 2. P. 25–40.

202. Schwartz P. The Art of the Long View: Planning for the Future in an Uncertain World. New York: Currency Doubleday, 1996. 272 p.

203. Scott W. R. Institutions and Organizations: Ideas, Interests, and Identities. 4th ed. Thousand Oaks: SAGE Publications, 2013. 360 p.

204. Sedra M. The Future of Security Sector Reform. Waterloo: CIGI, 2010. 396 p.

205. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014. 320 p.

206. Singh A., Pandey F. China's Military Modernization and Its Implications for Regional and Global Security. *International Journal for Multidisciplinary Research*. 2025. Vol. 7, Issue 2. P. 1-14.

207. Stacey R. D. Strategic Management and Organisational Dynamics: The Challenge of Complexity. 7th ed. Harlow: Pearson, 2016. 516 p.

208. Stockholm International Peace Research Institute. SIPRI Military Expenditure Database. Stockholm: SIPRI, 2023. URL: https://www.sipri.org/databases/milex

209. Stoker D. Why America Loses Wars: Limited War and US Strategy from the Korean War to the Present. Cambridge: Cambridge University Press, 2019. 336 p.

210. Stronski P., Sokolsky R. The Return of Global Russia: An Analytical Framework. Washington: Carnegie Endowment for International Peace, 2017. 54 p.

211. Szanton D. L. The Politics of Knowledge: Area Studies and the Disciplines. Berkeley: University of California Press, 2004. 413 p.

212. Taleb N. N. Antifragile: Things That Gain from Disorder. New York: Random House, 2012. 519 p.

213. Taleb N. N. The Black Swan: The Impact of the Highly Improbable. 2nd ed. New York: Random House, 2010. 444 p.

214. The National Infrastructure Advisory Council. Critical Infrastructure Resilience: Final Report and Recommendations. Washington: NIAC, 2020. 54 p.

215. The World Bank. Ukraine Public Finance Review 2. Washington: World Bank Group, 2021. 146 p.

216. Theohary C. A. Defense Primer: Information Operations. Washington: CRS, 2024. 3 p.

217. Thornton P. H., Ocasio W., Lounsbury M. The Institutional Logics Perspective: A New Approach to Culture, Structure and Process. Oxford: Oxford University Press, 2012. 256 p.

218. Walker B., Salt D. Resilience Practice: Building Capacity to Absorb Disturbance and Maintain Function. Washington: Island Press, 2012. 248 p.

219. Weiss M., Vaux P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. New York: Institute of Modern Russia, 2014. 44 p.

220. Wirtz J. J. Understanding Intelligence Failure: Warning, Response and Deterrence. London: Routledge, 2017. 174 p.

221. Wolfers A. «National Security» as an Ambiguous Symbol. Political Science Quarterly. 1952. Vol. 67, No. 4. P. 481–502.

222. Yarger H. R. Strategic Theory for the 21st Century: The Little Book on Big Strategy. Carlisle: Strategic Studies Institute, 2006. 94 p.

223. Zabrodskyi M., Watling J., Danylyuk O., Reynolds N. Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022. *SIRIUS*. 2023. Vol. 7(1). P. 90–103.

224. Zegart A. Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton: Princeton University Press, 2022. 424 p.

ДОДАТОК А
ДОВІДКИ ПРО ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ

ДСНС України
ГУ ДСНС України у Харківській області
3 ДЕРЖАВНИЙ ПОЖЕЖНО-РЯТУВАЛЬНИЙ ЗАГІН
ГОЛОВНОГО УПРАВЛІННЯ ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ
З НАДЗВИЧАЙНИХ СИТУАЦІЙ У ХАРКІВСЬКІЙ ОБЛАСТІ
(3 ДПРЗ ГУ ДСНС України у Харківській області)
вул. Кандаурова, 47, м. Харків, 61093, тел. (063) 713-78-01
сайт: https://kh.dsns.gov.ua код згідно з ЄДРПОУ 38362671 E-mail: 3-dprz-kh@dsns.gov.ua

Харківський національний
університет імені В. Н. Каразіна.

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Пупяліса Єгора Вікторовича
за темою «Інституціалізація публічного управління національною безпекою в умовах гібридної війни в Україні»

У дисертаційній роботі визначено та систематизовано ключові виклики для системи управління національною безпекою в умовах гібридної війни, що включають необхідність забезпечення безперебійного функціонування критичної інфраструктури, координації дій різних суб'єктів забезпечення національної безпеки під час кризових ситуацій та підвищення адаптивності системи до швидкозмінних багатовекторних загроз. Для Державної служби України з надзвичайних ситуацій ці виклики набувають особливої актуальності в контексті необхідності забезпечення цивільного захисту населення в умовах воєнного стану та координації реагування на надзвичайні ситуації різного характеру.

Виходячи з цього, автор пропонує комплекс взаємопов'язаних заходів для підвищення координаційної та адаптивної зрілості системи цивільного захисту в умовах гібридної війни, які можна успішно використовувати у діяльності ДСНС України, а саме: заходи щодо посилення міжвідомчої координації під час реагування на надзвичайні ситуації, які передбачають створення спільних ситуаційних центрів із залученням представників ДСНС, правоохоронних органів, медичних служб та інших суб'єктів забезпечення безпеки для

оперативного обміну інформацією та узгодження дій; заходи щодо підвищення адаптивності системи реагування через впровадження механізмів сценарного прогнозування можливих кризових ситуацій, розробку гнучких планів реагування на різні типи надзвичайних ситуацій та створення резервних систем управління і комунікації; заходи щодо стандартизації процедур взаємодії, спрямовані на розробку уніфікованих протоколів обміну інформацією між ДСНС та іншими органами під час надзвичайних ситуацій, узгодження термінології та форматів звітності для підвищення оперативності координації; технологічні заходи, метою яких є інтеграція інформаційних систем ДСНС із системами інших суб'єктів забезпечення безпеки для створення єдиного інформаційного простору та впровадження систем раннього попередження про потенційні загрози критичній інфраструктурі.

Враховуючи значну практичну цінність запропоновані заходи, можуть бути впроваджені в практичній роботі під час ліквідації надзвичайних ситуацій.

Начальник загону Сергій ПАТЛАХ

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
КОМАНДУВАННЯ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ УКРАЇНИ
вул. Дегтярівська ,19, м. Київ,04119
call.ksv@post.mil.gov.ua код згідно з ЕРДРПОУ 22991037 ksv@mod.gov.ua

Харківський національний
університет імені В.Н. Каразіна

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Пупяліса Єгора Вікторовича
за темою «Інституціалізація публічного управління національною безпекою в умовах гібридної війни в Україні»

В умовах тривалої гібридної агресії Російської Федерації проти України, що з лютого 2022 року переросла у повномасштабну воєнну агресію, особливої актуальності набуває питання удосконалення механізмів міжвідомчої координації у секторі безпеки та оборони. Це обумовлено тим, що гібридна війна одночасно охоплює воєнну, інформаційну, економічну, кібернетичну та дипломатичну сфери, що вимагає синхронізованих дій різних складових сектору безпеки для ефективної протидії багатовекторним асиметричним загрозам.

У дисертаційному дослідженні автором було обґрунтовано систему критеріїв оцінювання інституційної зрілості безпекових структур, яка інтегрує сім взаємопов'язаних вимірів: структурна, функціональна, нормативна, координаційна, адаптивна, культурна та інтеграційна зрілість. При цьому доведено, що в умовах гібридної війни найбільшого значення набувають адаптивна та координаційна зрілість, оскільки саме здатність до швидкої адаптації та ефективної міжвідомчої координації визначають результативність протидії загрозам.

зрілості), що дозволяє студентам аналізувати динаміку інституційних змін у реальних кризових умовах;

компаративний аналіз зарубіжного досвіду інституціалізації управління національною безпекою (країни Балтії, Фінляндія, Польща) з виявленням релевантних для України практик протидії гібридним загрозам;

засвоєння механізмів координації в системі управління національною безпекою, що поєднують вертикальну координацію через каскадну систему цілепокладання та горизонтальну координацію через міжвідомчі комітети і спільні ситуаційні центри; розуміння необхідності трансформації організаційної архітектури сектору безпеки від функціонально-галузевого до процесно-орієнтованого принципу побудови структур.

Через значну теоретичну та практичну цінність результатів дисертаційного дослідження, а також їх актуальність для підготовки фахівців у сфері публічного управління, основні положення дисертації Пупяліса Є.В. впроваджено у навчальний процес кафедри права, національної безпеки та європейської інтеграції менеджменту ННІ «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна при викладанні дисциплін Гібридні загрози та комплексна безпека (Освітньо-професійна програма «Публічна політика і управління в умовах гібридних загроз» для другого (магістерського) рівня вищої освіти галузі знань D «Бізнес, адміністрування та право» за спеціальністю D4 «Публічне управління та адміністрування»), Європейська інтеграція та політика національної безпеки України (Освітньо-професійна програма «Публічне управління та адміністрування» для другого (магістерського) рівня вищої освіти галузі знань D «Бізнес, адміністрування та право» за спеціальністю D4 «Публічне управління та адміністрування»), Механізми забезпечення національної безпеки (Освітньо-наукова програма «Публічне управління та адміністрування» для третього (освітньо-наукового) рівня вищої освіти галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування»).

Комісія у складі:

Голова комісії – заступник директора ННІ «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна к.е.н., професор Золотарьов В.Ф.,

члени комісії – завідувач кафедри публічної політики д.держ.упр., професор В. Дзюндзюк, доцент кафедри права, національної безпеки та європейської інтеграції к.держ.упр., доцент Мирна Н.

Голова комісії,
Заступник директор, к.е.н., професор — В. Золотарьов

Члени комісії:

д.держ.упр., професор — В. Дзюндзюк

к.держ.упр., доцент — Н. Мирна

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
КОМАНДУВАННЯ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ УКРАЇНИ
вул. Дегтярівська ,19, м. Київ,04119
call.ksv@post.mil.gov.ua код згідно з ЕРДРПОУ 22991037 ksv@mod.gov.ua

Харківський національний
університет імені В.Н. Каразіна

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Пупяліса Єгора Вікторовича
за темою «Інституціалізація публічного управління національною безпекою в умовах гібридної війни в Україні»

В умовах тривалої гібридної агресії Російської Федерації проти України, що з лютого 2022 року переросла у повномасштабну воєнну агресію, особливої актуальності набуває питання удосконалення механізмів міжвідомчої координації у секторі безпеки та оборони. Це обумовлено тим, що гібридна війна одночасно охоплює воєнну, інформаційну, економічну, кібернетичну та дипломатичну сфери, що вимагає синхронізованих дій різних складових сектору безпеки для ефективної протидії багатовекторним асиметричним загрозам.

У дисертаційному дослідженні автором було обґрунтовано систему критеріїв оцінювання інституційної зрілості безпекових структур, яка інтегрує сім взаємопов'язаних вимірів: структурна, функціональна, нормативна, координаційна, адаптивна, культурна та інтеграційна зрілість. При цьому доведено, що в умовах гібридної війни найбільшого значення набувають адаптивна та координаційна зрілість, оскільки саме здатність до швидкої адаптації та ефективної міжвідомчої координації визначають результативність протидії загрозам.

Виходячи з цього, автором було запропоновано комплекс практичних механізмів підвищення координаційної та адаптивної зрілості, який передбачає: впровадження системи раннього виявлення слабких сигналів про еволюцію гібридних загроз через створення спеціалізованих аналітичних груп; використання інструменту сценарного прогнозування для передбачення можливих траєкторій розвитку безпекової ситуації та завчасної підготовки до них; створення спільних ситуаційних центрів для оперативного обміну інформацією між різними складовими сектору безпеки в режимі реального часу; стандартизацію процедур міжвідомчої взаємодії в типових кризових ситуаціях для підвищення швидкості та узгодженості реагування; розробку уніфікованих протоколів обміну даними між інформаційними системами різних відомств.

Враховуючи значну практичну цінність даного комплексу механізмів, його було прийнято для впровадження в практичній роботі.

Міністерство оборони України Військова частина А1105 * Код 22991037 *

Командувач Сухопутних військ Збройних Сил України
генерал-майор Геннадій ШАПОВАЛОВ

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 11:25:04 06.04.2026

Назва файлу з підписом: Дисертація_Пупяліс-12.02.26.docx.asice
Розмір файлу з підписом: 5.1 МБ

Назва файлу без підпису: Дисертація_Пупяліс-12.02.26.docx.zip
Розмір файлу без підпису: 5.6 МБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ПУПЯЛІС ЄГОР ВІКТОРОВИЧ
П.І.Б.: ПУПЯЛІС ЄГОР ВІКТОРОВИЧ
Країна: Україна
РНОКПП: 3082518591
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 11:21:04 06.04.2026
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F04000000986FCC0169B15406
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Серійний номер носія особистого ключа: 014
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований
Підписані файли: Дисертація_Пупяліс-12.02.26.docx

Версія від: 2026.02.19 13:00