ДЕРЖАВНА СЛУЖБИ УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Кваліфікаційна наукова праця на правах рукопису

УДК 351.86(477)

ОМЕЛЬЧЕНКО МИКОЛА МИКОЛАЙОВИЧ

МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ РЕФОРМУВАННЯМ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Спеціальність 25.00.02 – механізми державного управління

Подається на здобуття наукового ступеня
кандидата наук з державного управління

Науковий керівник – доктор наук з державного управління, професор, МАЙСТРО Сергій Вікторович

Черкаси – 2026

АНОТАЦІЯ

Омельченко М. М. Механізми державного управління реформуванням сектору безпеки і оборони України в умовах збройної агресії. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація присвячена дослідженню механізмів державного управління реформуванням сектору безпеки і оборони України в умовах збройної агресії рф, аналізу сучасного стану функціонування цих механізмів в Україні та за кордоном із використанням системного, індикативного та інституціонального підходів, а також розробленню науково обґрунтованих практичних рекомендацій щодо вдосконалення державного управління зазначеним сектором. Об'єктом дослідження є система державного управління реформуванням сектору безпеки і оборони України як складова системи національної безпеки держави, предметом – сукупність управлінських відносин, організаційно-правових та інституційних механізмів, методів, принципів, процедур і технологій державного управління процесами реформування сектору безпеки і оборони України.

Визначено теоретичні засади механізмів державного управління сектором безпеки і оборони України, зокрема уточнено понятійне наповнення термінів «механізм державного управління», «сектор безпеки і оборони», «реформування», «гібридна загроза». На основі аналізу зарубіжного досвіду провідних країн НАТО – США, Великої Британії, Франції, Німеччини та Польщі – встановлено, що ефективне управління сектором безпеки і оборони ґрунтується на принципах цивільного контролю, міжвідомчої координації, прозорості й підзвітності, стратегічного планування та управління ризиками. Зокрема, у США координація забезпечується Радою національної безпеки при Президентові, у Великій Британії – Комітетом з питань національної безпеки при Прем'єр-міністрові, а в Польщі реалізовано дворівневу систему цивільного контролю за участю Президента та Прем'єр-міністра.

Обґрунтовано доцільність застосування індикативного підходу до оцінки ризиків і загроз національній безпеці України, який поєднує кількісні та якісні методи оцінки за ключовими сферами безпеки – воєнною, кібернетичною, інформаційною, економічною, енергетичною та внутрішньополітичною. У цьому контексті вперше у вітчизняній науці державного управління застосовано деліберaційний метод ранжування ризиків, адаптований до українських реалій з урахуванням специфіки гібридної війни, що дозволило подолати обмеженість традиційних методів, які не враховують комплексного характеру гібридних загроз.

Аналіз сучасного стану державного управління сектором безпеки і оборони України дав змогу охарактеризувати його як недостатньо ефективний і визначити причини такої оцінки. Установлено, що ефективність існуючої системи координації не перевищує 60% від потенційно можливого рівня через фрагментованість управлінських структур, неузгодженість нормативно-правової бази з вимогами НАТО та недостатній рівень цивільного демократичного контролю. Виявлено, що сформована законодавча база загалом відповідає євроатлантичним підходам, проте її практична імплементація стримується інерційністю інституційної структури та дублюванням функцій органів управління.

Обґрунтовано необхідність запровадження нового елемента архітектури управління сектором. Вперше розроблено концептуальну модель оптимізації системи управління сектором безпеки і оборони, яка ґрунтується на принципах цілісності, адаптивності, демократичного цивільного контролю, міжвідомчої координації та прозорості й включає функціональні модулі ідентифікації загроз, оцінки ризиків, планування реагування, реалізації контрзаходів та відновлення. Доведено необхідність створення Національного координаційного центру безпеки (НКЦБ) як постійно діючого органу при РНБО, що виконуватиме функції стратегічної координації, моніторингу реформ та індикативної оцінки загроз, забезпечуючи цілодобову координацію діяльності всіх структур сектору.

Зважаючи на євроатлантичні прагнення України, визначено шляхи вдосконалення системи державного управління сектором безпеки і оборони. Систематизація зарубіжного досвіду провідних держав – членів НАТО дозволила обґрунтувати необхідність адаптації кращих практик до українських умов з урахуванням специфіки гібридної війни, зокрема щодо запровадження єдиних стандартів прийняття рішень, посилення міжвідомчої координації та підвищення прозорості й підзвітності управлінських процесів.

Обґрунтовано напрями розвитку механізмів парламентського та громадського контролю за діяльністю сектору безпеки і оборони з метою забезпечення демократичної підзвітності силових структур. Розроблено практичні рекомендації щодо вдосконалення нормативно-правового забезпечення реформування сектору, впровадження єдиної інформаційно-аналітичної системи національної безпеки та адаптації євроатлантичних стандартів управління до українських умов.

Розроблено методичні підходи до вдосконалення механізмів державного управління реформуванням сектору безпеки і оборони України, зокрема систему індикаторів та критеріїв оцінки ефективності реформ, систему моніторингу на основі збалансованих показників, що забезпечує прозорий контроль реалізації реформ, а також структуру єдиної інформаційно-аналітичної системи національної безпеки для задоволення інформаційних потреб сектору з метою прийняття ефективних державно-управлінських рішень.

Ключові слова: державне управління, сектор безпеки і оборони, національна безпека, гібридні загрози, координація, реформування, індикативний підхід, упереджувальне управління, євроатлантична інтеграція.

ABSTRACT

Omelchenko M.M. Mechanisms of State Management for Security and Defense Sector Reform in Ukraine under Armed Aggression. – Qualifying scientific work as a manuscript.

Dissertation for the degree of Candidate of Sciences in Public Administration, speciality 25.00.02 – Mechanisms of Public Administration. – National University of Civil Protection of Ukraine, Cherkasy, 2026.

The dissertation is devoted to the study of the mechanisms of state administration of the security and defence sector reform of Ukraine under conditions of armed Russian aggression, to the analysis of the current state of functioning of these mechanisms in Ukraine and abroad using systemic, indicative, and institutional approaches, and to the development of scientifically substantiated practical recommendations for improving state administration of the sector. The object of research is the state administration system of the security and defence sector reform of Ukraine, while the subject is the mechanisms of state administration of the reform processes aimed at increasing the effectiveness of countering contemporary threats to national security.

The theoretical foundations of state administration mechanisms of the security and defence sector of Ukraine are defined, in particular the conceptual content of the terms 'mechanism of state administration', 'security and defence sector', 'reform', and 'hybrid threat' is clarified. Based on the analysis of the experience of leading NATO countries – the United States, the United Kingdom, France, Germany, and Poland – it is established that effective management of the security and defence sector is grounded in the principles of civilian control, interagency coordination, transparency and accountability, strategic planning, and risk management. In particular, coordination in the United States is ensured by the National Security Council under the President, in the United Kingdom by the National Security Council under the Prime Minister, while Poland has

implemented a two-tier system of civilian control involving both the President and the Prime Minister.

The expediency of applying an indicative approach to assessing risks and threats to Ukraine's national security, combining quantitative and qualitative assessment methods across key security domains – military, cyber, informational, economic, energy, and domestic political – is substantiated. In this context, for the first time in Ukrainian public administration science, a deliberative risk-ranking method adapted to Ukrainian realities and the specifics of hybrid warfare is applied, overcoming the limitations of traditional methods that fail to account for the complex nature of hybrid threats.

The analysis of the current state of state administration of the security and defence sector of Ukraine made it possible to characterise it as insufficiently effective and to identify the reasons for this assessment. It is established that the effectiveness of the existing coordination system does not exceed 60% of its potential level due to the fragmentation of management structures, the inconsistency of the regulatory framework with NATO requirements, and an insufficient level of democratic civilian control. It is found that, although the established legislative framework generally corresponds to Euro-Atlantic approaches, its practical implementation is constrained by the inertia of the institutional structure and the duplication of management functions.

The necessity of introducing a new element of the sector's management architecture is substantiated. For the first time, a conceptual model for optimising the security and defence sector management system is developed, based on the principles of integrity, adaptability, democratic civilian control, interagency coordination, and transparency, and comprising functional modules for threat identification, risk assessment, response planning, countermeasure implementation, and recovery. The necessity of establishing a National Security Coordination Centre (NSCC) as a permanent body under the National Security and Defence Council is substantiated, tasked with strategic coordination, reform monitoring,

and indicative threat assessment, thereby ensuring round-the-clock coordination of all sector structures.

Given Ukraine's Euro-Atlantic aspirations, ways of improving the state administration system of the security and defence sector are identified. The systematisation of the experience of leading NATO member states made it possible to substantiate the need to adapt best practices to Ukrainian conditions, taking into account the specifics of hybrid warfare, in particular regarding the introduction of unified decision-making standards, strengthened interagency coordination, and increased transparency and accountability of management processes.

Directions for developing mechanisms of parliamentary and public control over the activities of the security and defence sector are substantiated with a view to ensuring the democratic accountability of security structures. Practical recommendations are developed for improving the regulatory framework for sector reform, implementing a unified national security information-analytical system, and adapting Euro-Atlantic management standards to Ukrainian conditions.

Methodological approaches to improving the mechanisms of state administration of the security and defence sector reform of Ukraine are developed, including a system of indicators and criteria for assessing reform effectiveness, a monitoring system based on balanced indicators ensuring transparent oversight of reform implementation, and the structure of a unified national security information-analytical system for meeting the informational needs of the sector in support of effective public administration decisions.

Keywords: public administration, security and defence sector, national security, hybrid threats, coordination, reform, indicative approach, anticipatory management, Euro-Atlantic integration.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові статті у фахових виданнях:

1. Омельченко М.М. Національний координаційний центр безпеки як ключовий елемент інтегрованого управління реформуванням сектору безпеки і оборони України. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2019. Вип. 1 (10). С. 461–468. https://repositsc.nuczu.edu.ua/bitstream/123456789/28954/1/Omelchenko.pdf

2. Омельченко М.М. Механізми державного управління реформуванням сектору безпеки і оборони України в період 2014–2021 років: досягнення та проблеми. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2021. Вип. 1 (14). С. 430–440. https://repositsc.nuczu.edu.ua/bitstream/123456789/25439/1/Omelchenko21.1.pdf

3. Омельченко М.М. Інституційні механізми державного управління реформуванням сектору безпеки і оборони України: регіональний вимір (2014–2021 роки). Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2021. Вип. 2 (15). С. 462–469. https://vdu-nuczu.net/ua/11-ukr/storinkaavtora/518-omelchenko-m-m-institutsijni-mekhanizmi-derzhavnogo-upravlinnya-reformuvannyam-sektoru-bezpeki-i-oboroni-ukrajini-regionalnij-vimir-2014-2021-roki

4. Omelchenko M.M., Paliukh V.V. Methodological Foundations for Diagnosing the Effectiveness of Public Administration in the Security and Defense Sector under Russian Aggression: Ukrainian Experience. Public administration and state security aspects. 2025. Vol. 2. P. 43–54. https://passa.nuczu.edu.ua/en/archive/252-paliukh-v-omelchenko-m-methodological-foundations-for-diagnosing-the-effectiveness-of-public-administration-in-the-security-and-defense-sector-under-russian-aggression-ukrainian-experience

Особистий внесок: розроблено методичні засади діагностики ефективності державного управління у сфері безпеки та оборони в умовах збройної агресії.

5. Палюх В.В., Омельченко М.М. Управлінська синергія та виклики при міжвідомчому комплектуванні керівного складу ЗВО зі специфічними умовами навчання: аналіз адаптаційних механізмів. Успіхи і досягнення у науці. Серія: Управління та адміністрування. 2025. № 17. DOI:10.52058/3041-1254-2025-11(21)-905-914

Особистий внесок: проаналізовано адаптаційні механізми міжвідомчого комплектування керівного складу закладів вищої освіти зі специфічними умовами навчання.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Омельченко М.М. Еволюція стратегічних підходів до забезпечення енергетичної безпеки України в умовах повномасштабної війни: уроки 2022–2025 років. Матеріали IX Міжнародної науково-практичної конференції 11 листопада 2025 року Київ, 2025. С. 290-293.

7. Омельченко М.М., Тарасов С.С. Трансформація механізмів державного управління сектором безпеки і оборони: адаптація до гібридних загроз на основі зарубіжного досвіду. Матеріали І-ї Міжнародної науково-практичної конференції «Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення», 27 листопада 2025 року. Івано-Франківськ, 2025. С. 495-498.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АТО – антитерористична операція

ВСУ / ЗСУ – Збройні Сили України

ДПС – Державна прикордонна служба України

МВС – Міністерство внутрішніх справ України

МО – Міністерство оборони України

НАТО – Організація Північноатлантичного договору

НУЦЗ – Національний університет цивільного захисту України

РНБО – Рада національної безпеки і оборони України

СБУ – Служба безпеки України

СБО – сектор безпеки і оборони

ДКІБ – державне керування і безпека

ВСТУП

Актуальність теми дослідження. Збройна агресія рф проти України, розпочата ще у 2014 році, докорінно змінила безпекове середовище не лише для нашої держави, а й для всієї Європи. Сектор безпеки і оборони України опинився перед безпрецедентними викликами: необхідністю одночасного ведення бойових дій та проведення системних реформ, інтеграції в євроатлантичну архітектуру безпеки, адаптації управлінських структур до умов гібридної війни. У цих обставинах ефективність механізмів державного управління реформуванням сектору безпеки і оборони набуває стратегічного значення для виживання та розвитку держави [86].

Трансформація сектору безпеки і оборони України розпочалася після 2014 року у відповідь на анексію Криму та збройний конфлікт на Сході країни. Проте досвід повномасштабної агресії виявив як здобутки здійснених реформ, так і системні недоліки механізмів координації, планування та управління у сфері національної безпеки. Фрагментованість управлінських рішень, відсутність єдиних стандартів оцінки ризиків і загроз, недостатня узгодженість діяльності суб'єктів сектору безпеки і оборони — ці проблеми набули особливої гостроти в умовах збройного протистояння [86].

Прагнення України до членства в НАТО та ЄС визначає додатковий вектор трансформації: запровадження євроатлантичних стандартів управління у сфері безпеки і оборони стає не лише бажаним орієнтиром, а й обов'язковою умовою інтеграційного процесу. Водночас адаптація зарубіжного досвіду до українських реалій потребує врахування специфіки гібридної війни, обмеженості ресурсів в умовах воєнного стану та необхідності збереження управлінської спроможності в надзвичайних умовах [86].

Незважаючи на значний обсяг наукових праць із проблематики державного управління у сфері національної безпеки, механізми державного управління реформуванням сектору безпеки і оборони саме в умовах збройної агресії залишаються недостатньо дослідженими. Відсутні

комплексні підходи до оцінки ефективності реформ із використанням індикативних методів, не сформована цілісна концептуальна модель інтегрованого управління реформами в умовах активних бойових дій. Це й зумовило вибір теми дисертаційної роботи, її мету і завдання [84].

Теоретичними та практичними аспектами державного управління у сфері національної безпеки і оборони займалися такі вчені, як: Г. Ситник, В. Горбулін, О. Литвиненко, М. Требін, В. Богданович, С. Пирожков, В. Шемаєв, Г. Перепелиця, Б. Парахонський та інші. Питаннями реформування сектору безпеки і оборони та механізмів його державного управління займалися: О. Резнікова, С. Дяченко, В. Телелим, А. Сиротенко, В. Павленко, О. Косевцов та інші. Серед зарубіжних учених вагомий внесок у розвиток теорії управління сектором безпеки і оборони зробили: Т. Флурі, Р. Хакалехто, Д. Борн, Х.-Й. Гізманн та інші [26; 91; 92; 181–209].

Необхідно відзначити, що ступінь наукової розробленості теми є достатньо високим з позицій загальних підстав реформування сектору безпеки і оборони в мирних умовах та недостатнім з точки зору дослідження механізмів державного управління цими процесами в умовах активної збройної агресії, що й зумовлює наукову актуальність обраної теми [84].

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана в науково-дослідному центрі Національного університету цивільного захисту України в межах науково-дослідної роботи «Розробка механізмів державного управління соціально-економічною сферою та її галузями в контексті забезпечення безпеки українського суспільства» (ДР № 0118U001007). Внесок здобувача полягає в обґрунтуванні підходів та визначенні напрямів удосконалення механізмів державного управління реформуванням сектору безпеки і оборони України [85].

Мета і завдання роботи. Метою дисертаційної роботи є розробка теоретичних засад та науково обґрунтованих практичних рекомендацій щодо удосконалення механізмів державного управління реформуванням сектору

безпеки і оборони України на основі комплексного аналізу сучасного стану системи національної безпеки, узагальнення зарубіжного досвіду та застосування інноваційних підходів до оцінки ризиків і загроз для забезпечення ефективної протидії сучасним викликам та успішної євроатлантичної інтеграції.

Досягнення визначеної мети зумовило необхідність вирішення таких завдань:

– узагальнити та систематизувати теоретичні засади механізмів державного управління у сфері національної безпеки та оборони;

– дослідити зарубіжний досвід формування систем управління сектором безпеки і оборони та виявити кращі практики, які можуть бути адаптовані до українських умов;

– розробити методичні засади застосування індикативного підходу до оцінки ризиків і загроз національній безпеці України;

– провести комплексний аналіз сучасного стану системи державного управління сектором безпеки і оборони України та оцінити ефективність чинної нормативно-правової бази та інституційної структури управління;

– розробити концептуальну модель удосконалення механізмів державного управління реформуванням сектору безпеки і оборони;

– обґрунтувати систему механізмів координації, контролю та моніторингу реформ у сфері безпеки і оборони та розробити практичні рекомендації щодо вдосконалення державного управління реформуванням сектору безпеки і оборони України.

Об'єктом дослідження є система державного управління реформуванням сектору безпеки і оборони України як складова системи національної безпеки держави.

Предметом дослідження сукупність управлінських відносин, організаційно-правових та інституційних механізмів, методів, принципів, процедур і технологій державного управління процесами реформування

сектору безпеки і оборони України, спрямованих на підвищення ефективності протидії сучасним загрозам національній безпеці

Методи дослідження. Теоретичну та методичну основу дисертаційного дослідження становлять фундаментальні положення теорії державного управління, теорії національної безпеки, інституціональної теорії, теорії ризиків, а також сучасні концепції реформування сектору безпеки і оборони. Дисертаційне дослідження ґрунтується на використанні системного підходу, який полягає в комплексному дослідженні механізмів державного управління у сфері національної безпеки як цілісної системи взаємопов'язаних елементів. Крім того, у роботі застосовувались методи, які використовуються як на емпіричному, так і теоретичному рівнях, а саме: системно-структурний аналіз — для дослідження системи державного управління як цілісності взаємопов'язаних елементів; порівняльний аналіз — для зіставлення зарубіжного досвіду з українською практикою; інституціональний аналіз — для вивчення формальних і неформальних інститутів у сфері безпеки і оборони; нормативно-правовий аналіз — для дослідження чинного законодавства у сфері національної безпеки; кореляційний аналіз — для виявлення статистичних зв'язків між індикаторами національної безпеки; метод головних компонент — для агрегування множини показників в інтегральні індекси оцінки ризиків; експертне оцінювання — для отримання якісних оцінок від фахівців-практиків; моделювання — для створення концептуальних моделей удосконалення механізмів управління; SWOT-аналіз — для оцінки сильних і слабких сторін, можливостей і загроз системи управління; контент-аналіз — для аналізу документів і матеріалів щодо реформування сектору безпеки і оборони; абстрактно-логічний метод — для узагальнення теоретичних положень, встановлення причинно-наслідкових зв'язків і формування висновків та пропозицій [136].

Інформаційними джерелами дослідження стали закони України, укази Президента України, постанови Кабінету Міністрів України, стратегічні документи у сфері національної безпеки і оборони, звіти органів сектору

безпеки і оборони, аналітичні матеріали міжнародних організацій (НАТО, ЄС, ОБСЄ), офіційні матеріали Державної служби статистики України, монографії та статті вітчизняних і зарубіжних науковців, результати експертного опитування [41; 10; 15; 18; 20–22; 27; 37–40; 45; 48–49; 55; 63–64; 71; 76; 79; 90; 98; 102; 134; 137–138; 147; 165; 171–173].

Наукова новизна одержаних результатів дослідження полягає в науково-практичному обґрунтуванні теоретичних положень та напрямів удосконалення механізмів державного управління реформуванням сектору безпеки і оборони України в умовах збройної агресії.

Наукова новизна результатів дослідження конкретизується в таких положеннях:

вперше:

розроблено концептуальну модель оптимізації системи управління сектором безпеки і оборони, яка ґрунтується на принципах цілісності, адаптивності, демократичного цивільного контролю, міжвідомчої координації та прозорості й включає функціональні модулі ідентифікації загроз, оцінки ризиків, планування реагування, реалізації контрзаходів та відновлення;

обґрунтовано необхідність та визначено організаційно-функціональну структуру Національного координаційного центру безпеки як ключового елемента нової архітектури управління сектором безпеки і оборони України.

удосконалено:

теоретико-методологічні засади механізмів державного управління сектором безпеки і оборони шляхом інтеграції принципів системного, адаптивного та упереджувального управління, що дозволяє гнучко реагувати на динамічні зміни безпекового середовища;

систему критеріїв оцінки ефективності чинної нормативно-правової бази та інституційної структури управління сектором безпеки і оборони з урахуванням євроатлантичних стандартів, що дало змогу виявити системні недоліки та об'єктивізувати підстави для подальшого реформування.

набули подальшого розвитку:

науково-методичний інструментарій деліберaційного методу ранжування ризиків, адаптованого до оцінки загроз національній безпеці України з урахуванням специфіки гібридної війни, та концепція упереджувального державного управління шляхом формування системи індикаторів і порогових значень рівня загроз з використанням методу головних компонент для агрегування показників в інтегральні індекси;

типологія моделей координації сектору безпеки і оборони провідних країн НАТО та ЄС за критерієм придатності до адаптації в умовах збройної агресії та обмеженості ресурсів воєнного часу.

Результати дослідження можуть бути безпосередньо використані органами державної влади, зокрема: Радою національної безпеки і оборони України – для вдосконалення координаційних механізмів; Міністерством оборони України – для оптимізації системи управління реформами; Службою безпеки України – для підвищення ефективності аналітичної роботи; Верховною Радою України – для вдосконалення законодавчого забезпечення реформування сектору. Результати дослідження впроваджено у діяльність: Головного управління національної поліції в Черкаській області № 12/23-137.11 від 11.12.2025); Черкаської районної ради (довідка № 20/01-22 від 14.03.2026); Національного університету цивільного захисту України (акт про впровадження від 12.02.2026). Матеріали дисертації можуть також використовуватися в освітньому процесі при підготовці магістрів публічного управління та адміністрування.

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею, в якій викладено авторський підхід до вдосконалення механізмів державного управління реформуванням сектору безпеки і оборони України. Наукові положення, висновки і рекомендації, що виносяться на захист, одержані автором особисто. У працях, опублікованих у співавторстві, здобувачеві належать: обґрунтування методичних засад діагностики ефективності державного управління сектором безпеки і

оборони в умовах російської агресії; аналіз адаптаційних механізмів міжвідомчого комплектування керівного складу закладів вищої освіти зі специфічними умовами навчання; узагальнення зарубіжного досвіду трансформації механізмів державного управління сектором безпеки і оборони в умовах гібридних загроз [95].

Апробація результатів дисертації. Основні положення й результати дисертації доповідались і обговорювались на науково-практичній конференції (м. Київ, 2025 р.) та І Міжнародній науково-практичній конференції «Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення» (м. Івано-Франківськ, 27 листопада 2025 р.) [78].

Публікації. Основні положення дисертаційної роботи опубліковано в наукових працях, у тому числі — у наукових фахових виданнях та тезах доповідей на конференціях.

Структура та обсяг дисертації. Робота складається з анотацій державною та англійською мовами, вступу, трьох розділів, висновків, списку використаних джерел (209 найменувань) та додатків. Загальний обсяг роботи становить 192 сторінки, з яких основний текст — 161 сторінка.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ СЕКТОРОМ БЕЗПЕКИ І ОБОРОНИ

1.1. Сутність та зміст механізмів державного управління в сфері національної безпеки та оборони

Дослідження механізмів державного управління сектором безпеки і оборони потребує чіткого визначення концептуальних засад, що становлять теоретичну основу для розуміння природи та специфіки управлінських процесів у цій критично важливій сфері державної діяльності. Особливо актуальним це питання є для України в умовах тривалої російської агресії та необхідності кардинального реформування системи національної безпеки і оборони відповідно до стандартів НАТО та Європейського Союзу. Системне дослідження зазначених механізмів дозволяє не лише осмислити теоретичні засади їх функціонування, але й розробити практичні рекомендації щодо підвищення ефективності державного управління у досліджуваній сфері [100].

Сучасний стан міжнародної безпеки характеризується кардинальними змінами у структурі загроз, що потребує переосмислення традиційних підходів до організації та функціонування систем національної безпеки. Україна, перебуваючи в епіцентрі геополітичного протистояння, стала полігоном для апробації новітніх форм і методів ведення війни, що поєднують традиційні військові дії з широким спектром невійськових засобів впливу. Це зумовлює необхідність формування адекватної системи державного управління, здатної ефективно протидіяти сучасним викликам і загрозам. Особливого значення набуває розробка теоретичного підґрунтя для розуміння механізмів, що забезпечують координацію між різними складовими сектору безпеки і оборони в умовах гібридної війни та постійної

трансформації характеру загроз [29].

Гібридна війна як новий феномен міжнародних відносин вимагає кардинального перегляду традиційних підходів до організації національної безпеки. Вона характеризується поєднанням військових, політичних, економічних, інформаційних, кіберінструментів впливу, що застосовуються одночасно та скоординовано для досягнення стратегічних цілей агресора. Така багатовимірність сучасних загроз потребує відповідної трансформації механізмів державного управління, їх адаптації до умов невизначеності та швидкозмінного безпекового середовища [151].

Теоретично-методологічною основою дослідження механізмів державного управління у сфері національної безпеки і оборони є синтез фундаментальних положень теорії державного управління, теорії національної безпеки, інституціональної теорії та теорії систем. Кожна з цих теоретичних парадигм привносить специфічні методологічні підходи до розуміння природи та закономірностей функціонування досліджуваної сфери. Теорія державного управління розглядає механізми управління як сукупність принципів, методів, форм і засобів цілеспрямованого впливу держави на суспільні процеси з метою досягнення поставлених цілей. У контексті сфери безпеки і оборони ця теорія акцентує увагу на специфіці об'єкта управління, який характеризується високим ступенем складності, динамічності та невизначеності [100].

Теорія національної безпеки привносить розуміння специфіки безпекової сфери як особливої галузі державної діяльності, що має власні закономірності, принципи та методи функціонування. Ця теорія розглядає національну безпеку як системне явище, що включає різні рівні (індивідуальний, суспільний, державний, міжнародний) та виміри (військовий, політичний, економічний, соціальний, інформаційний, екологічний тощо). Комплексність національної безпеки вимагає застосування інтегрованого підходу до управління, що враховує взаємозв'язки між різними видами безпеки та необхідність їх збалансованого

забезпечення [8].

Систему механізмів державного управління сектором безпеки і оборони України наведено на рис. 1.1.

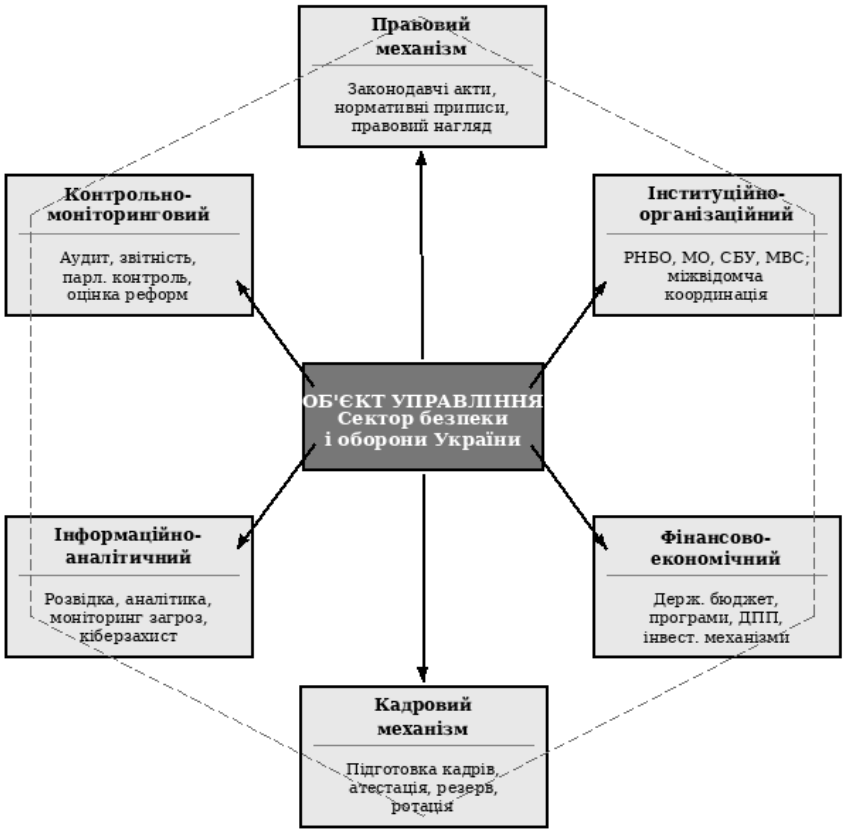

Рис. 1.1. Система механізмів державного управління сектором безпеки і оборони України

Джерело: розроблено автором

Особливістю державного управління у сфері національної безпеки є його багатовимірний характер, що охоплює як внутрішні, так і зовнішні аспекти забезпечення безпеки держави. Внутрішні аспекти включають організацію та координацію діяльності різних відомств і структур, які входять до сектору безпеки і оборони, забезпечення їх ефективної взаємодії та оптимального використання наявних ресурсів. Зовнішні аспекти стосуються взаємодії з міжнародними партнерами, участі у міжнародних організаціях безпеки, адаптації до глобальних тенденцій у сфері безпеки та

оборони. Така багатовимірність вимагає застосування комплексного підходу до аналізу механізмів державного управління, що враховує як національні особливості, так і міжнародний контекст функціонування системи безпеки [100].

Внутрішній вимір державного управління у сфері національної безпеки передбачає створення ефективної системи координації між різними суб'єктами сектору безпеки і оборони. Це включає розподіл функцій та повноважень, створення механізмів міжвідомчої взаємодії, забезпечення інформаційного обміну, координацію планування та виконання завдань. Особливої уваги потребує вирішення проблеми дублювання функцій та конфлікту повноважень між різними структурами, що знижує ефективність системи в цілому [61].

Зовнішній вимір державного управління у сфері національної безпеки охоплює широкий спектр міжнародної взаємодії, включаючи двосторонні та багатосторонні угоди про співробітництво у сфері безпеки, участь у миротворчих операціях, обмін розвідувальною інформацією, спільні навчання та тренування. Для України особливого значення набуває євроатлантична інтеграція, що передбачає поступову адаптацію національної системи безпеки і оборони до стандартів і принципів НАТО. Це вимагає системної трансформації механізмів управління, їх приведення у відповідність до міжнародних вимог та найкращих практик [14].

Інституціональна теорія привносить розуміння того, що ефективність механізмів державного управління значною мірою залежить від якості інституційного середовища, в якому вони функціонують. Інститути, як формальні правила та неформальні норми, що регулюють поведінку акторів у сфері безпеки і оборони, визначають можливості та обмеження для реалізації управлінських функцій держави. Формальні інститути включають конституційні норми, законодавчі акти, підзаконні нормативно-правові документи, що регламентують організацію та діяльність сектору безпеки і оборони. Неформальні інститути охоплюють традиції, звичаї, корпоративну

культуру, неписані правила взаємодії між різними структурами сектору [50].

Інституціональний аналіз дозволяє виявити причини неефективності окремих механізмів управління та розробити заходи щодо їх удосконалення. Слабкість формальних інститутів часто компенсується розвитком неформальних практик, які можуть як сприяти, так і перешкоджати ефективному управлінню. Наприклад, неформальні мережі взаємодії між керівниками різних відомств можуть забезпечувати оперативну координацію в критичних ситуаціях, але водночас можуть створювати передумови для зловживань та корупції.

Процес інституціоналізації механізмів державного управління у сфері національної безпеки передбачає не лише створення формальних правил та процедур, але й формування відповідної організаційної культури, професійних стандартів, етичних норм. Особливого значення набуває інституціоналізація принципів демократичного цивільного контролю, прозорості, підзвітності, що є основними вимогами сучасних демократичних стандартів управління сектором безпеки і оборони [170].

Якість інституційного середовища прямо впливає на ефективність функціонування механізмів державного управління. Слабкі або суперечливі інститути створюють перешкоди для ефективної координації, знижують прозорість прийняття рішень, сприяють виникненню корупційних схем та зловживань. Натомість, сильні та узгоджені інститути забезпечують чіткий розподіл повноважень, прозорість процедур, ефективну координацію між різними суб'єктами управління. Особливого значення набуває адаптація інституційного середовища до вимог євроатлантичної інтеграції, що передбачає гармонізацію національних інститутів із стандартами та принципами НАТО і ЄС [68].

Інституційні реформи у сфері національної безпеки і оборони вимагають комплексного підходу, що включає зміни у законодавстві, організаційних структурах, процедурах прийняття рішень, системах контролю та звітності. Успішність таких реформ залежить від політичної волі

керівництва держави, підтримки з боку громадянського суспільства, наявності необхідних ресурсів та експертизи. Важливим чинником є також час, необхідний для інституціоналізації нових норм та практик, формування відповідної організаційної культури [31].

Системний підхід дозволяє розглядати сферу національної безпеки і оборони як складну відкриту систему, що складається з множини взаємопов'язаних підсистем та елементів. Такий підхід особливо важливий для розуміння механізмів координації та взаємодії між різними суб'єктами сектору безпеки і оборони, а також їх інтеграції з іншими сферами державної політики. Системність передбачає розгляд сектору безпеки і оборони не як простої сукупності окремих органів та структур, а як цілісної системи, де зміни в одному елементі впливають на функціонування всіх інших елементів [2].

Системний аналіз сектору безпеки і оборони включає дослідження структури системи, функцій окремих елементів, характеру зв'язків між ними, механізмів координації та контролю. Особливої уваги потребує аналіз горизонтальних та вертикальних зв'язків у системі управління, виявлення вузьких місць та дисфункцій, що знижують ефективність системи в цілому. Системний підхід також дозволяє оцінити синергетичний ефект від взаємодії різних елементів системи та визначити напрями оптимізації її структури і функціонування [2].

Системний підхід також акцентує увагу на взаємодії системи з зовнішнім середовищем, що включає як внутрішній політичний, економічний та соціальний контекст, так і міжнародне безпекове середовище. Відкритість системи означає її здатність до адаптації та трансформації у відповідь на зміни у зовнішньому середовищі. Це особливо важливо в умовах динамічних змін характеру загроз та викликів національній безпеці. Ефективна система управління повинна мати механізми раннього виявлення змін у безпековому середовищі та швидкого реагування на нові виклики [16].

Кібернетичний підхід як складова системної теорії розглядає

управління у сфері національної безпеки як процес інформаційної взаємодії між керуючою та керованою підсистемами. Цей підхід акцентує увагу на інформаційних потоках, зворотних зв'язках, механізмах саморегуляції системи. В умовах інформаційного суспільства та розвитку цифрових технологій кібернетичний підхід набуває особливого значення для розуміння механізмів управління сучасними системами безпеки і оборони [29].

Адаптивність системи управління національною безпекою проявляється у здатності змінювати свою структуру і функції у відповідь на нові виклики та загрози. Це включає можливість швидкого перерозподілу ресурсів, зміни пріоритетів, модифікації процедур прийняття рішень, створення нових структурних підрозділів або ліквідації застарілих. Адаптивність особливо важлива в умовах невизначеності та швидких змін безпекового середовища, що характерні для сучасного світу [142].

У сучасному понятійно-категоріальному апараті під безпекою розуміють стан і тенденції розвитку захищеності життєво важливих інтересів соціального організму та його структур від зовнішніх і внутрішніх негативних факторів. Безпека є результатом соціальної діяльності із забезпечення безпечного розвитку особистості, сім'ї, суспільства, держави та цивілізації в цілому. Це динамічна категорія, що має множинну предметність в залежності від конкретного історичного періоду існування об'єкта безпеки. Діяльність із забезпечення безпеки різних рівнів соціуму виникає як соціальний феномен у ході розв'язання протиріч між небезпекою та потребою соціального організму управляти безпекою: передбачати, запобігати, нейтралізувати, локалізувати та усувати шкоду від впливу небезпеки [25].

Еволюція поняття безпеки відображає зміни у розумінні характеру загроз та методів їх подолання. Традиційне розуміння безпеки фокусувалося переважно на військових загрозах та захисті території держави від зовнішнього вторгнення. Сучасна концепція безпеки значно розширилася і включає широкий спектр невійськових загроз: економічних, екологічних, інформаційних, технологічних, соціальних. Така трансформація зумовлена

глобалізаційними процесами, розвитком технологій, зміною характеру міжнародних відносин [16].

Багатовимірність сучасної безпеки проявляється не лише у розширенні спектру загроз, але й у множинності суб'єктів безпеки. Якщо раніше основним суб'єктом безпеки вважалася держава, то сьогодні все більшого значення набувають індивідуальна безпека, безпека груп та спільнот, регіональна та глобальна безпека. Це вимагає розробки багаторівневих систем управління безпекою, що забезпечують координацію зусиль різних суб'єктів [176].

Безпека як динамічна категорія має множинну предметність залежно від конкретного історичного періоду існування об'єкта безпеки. Це означає, що зміст поняття безпеки та пріоритети у забезпеченні безпеки змінюються відповідно до еволюції загроз та викликів. Якщо в індустріальну епоху основний акцент робився на військовій безпеці та захисті території, то в постіндустріальному суспільстві все більшого значення набувають інформаційна, кібер, економічна, екологічна та інші види безпеки. Сучасне розуміння безпеки характеризується комплексністю та багатовимірністю, що вимагає відповідної трансформації механізмів державного управління [29].

Концепція людської безпеки, яка отримала розвиток у 1990-х роках, змістила акцент з безпеки держави на безпеку людини. Згідно з цією концепцією, справжня безпека має ґрунтуватися на захисті людей від критичних і поширених загроз для їхнього життя, засобів до існування та гідності. Це включає безпеку від страху та безпеку від нужди. Така переорієнтація вимагає перегляду традиційних підходів до організації системи національної безпеки та розробки нових механізмів управління, що враховують потреби та інтереси людини [176].

Державне управління у сфері національної безпеки і оборони являє собою особливий вид управлінської діяльності, що характеризується специфічністю об'єкта, предмета, суб'єктів, методів та засобів впливу. Об'єктом такого управління виступає сфера національної безпеки як

сукупність суспільних відносин, пов'язаних із забезпеченням захищеності національних інтересів від внутрішніх і зовнішніх загроз. Ця сфера характеризується високим ступенем складності, оскільки включає різнорідні за природою процеси та явища: від традиційних військових загроз до сучасних кіберзагроз , від економічних ризиків до інформаційних воєн [155].

Специфічність об'єкта управління у сфері національної безпеки проявляється у його багатокомпонентності , динамічності та непередбачуваності. Багатокомпонентність означає, що сфера національної безпеки включає різноманітні елементи: військові формування, правоохоронні органи, спеціальні служби, оборонно-промисловий комплекс, наукові установи, освітні заклади, громадські організації. Динамічність виражається у постійних змінах характеру загроз, появі нових викликів, еволюції форм і методів забезпечення безпеки. Непередбачуваність пов'язана з високим ступенем невизначеності у сфері безпеки, складністю прогнозування розвитку подій, особливо в кризових ситуаціях [142].

Згідно із Законом України "Про національну безпеку України", національна безпека України визначається як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Сектор безпеки і оборони включає Міністерство оборони України, Збройні Сили України, Державну спеціальну службу транспорту, Міністерство внутрішніх справ України, Національну гвардію України, Національну поліцію України, Державну прикордонну службу України, Державну міграційну службу України, Державну службу України з надзвичайних ситуацій, Службу безпеки України, Управління державної охорони України, Державну службу спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику [50; 114; 126].

Така розгалужена структура сектору безпеки і оборони відображає комплексний характер сучасних загроз та необхідність багатопланового реагування на них. Кожна з перелічених структур має специфічні функції, повноваження та можливості, що вимагає ефективної координації їх діяльності для досягнення спільних цілей забезпечення національної безпеки. Особливої уваги потребує уникнення дублювання функцій та забезпечення раціонального розподілу ресурсів між різними структурами [170].

Механізми державного управління у сфері національної безпеки і оборони представляють собою складну систему взаємопов'язаних елементів, що включає правові, організаційні, економічні, інформаційні та інші інструменти цілеспрямованого впливу держави на процеси забезпечення національної безпеки. Правові механізми охоплюють конституційні норми, законодавчі акти, підзаконні нормативно-правові документи, що регламентують організацію та діяльність суб'єктів сектору безпеки і оборони. Організаційні механізми включають структури управління, процедури прийняття рішень, системи координації та контролю. Економічні механізми стосуються фінансування, ресурсного забезпечення, планування та використання оборонного бюджету [50].

Правові механізми утворюють нормативну основу функціонування всієї системи національної безпеки. Вони включають ієрархічну систему нормативно-правових актів: від Конституції України до відомчих інструкцій та наказів. Особливе значення мають базові закони у сфері національної безпеки: "Про національну безпеку України", "Про оборону України", "Про Збройні Сили України", "Про розвідувальні органи України" та інші. Ефективність правових механізмів залежить від якості законодавства, його узгодженості, повноти правового регулювання, своєчасності внесення змін у відповідь на нові виклики [50; 114; 118].

Організаційні механізми включають структури управління на різних рівнях: стратегічному, оперативному та тактичному. Стратегічний рівень представлений Президентом України, Радою національної безпеки і оборони

України, Верховною Радою України, Кабінетом Міністрів України. Оперативний рівень включає міністерства та відомства, що входять до сектору безпеки і оборони. Тактичний рівень представлений безпосередніми виконавцями завдань: військовими частинами, підрозділами, службами. Ефективність організаційних механізмів залежить від чіткості розподілу функцій та повноважень, якості координації між різними рівнями та структурами [124].

Інформаційні механізми охоплюють системи збору, обробки, аналізу та поширення інформації, необхідної для прийняття обґрунтованих управлінських рішень у сфері безпеки і оборони. Особливого значення в умовах інформаційної війни набувають механізми протидії дезінформації, забезпечення інформаційної безпеки, стратегічних комунікацій. Ефективність цих механізмів значною мірою залежить від їх узгодженості, компліментарності та адаптивності до змін у безпековому середовищі [61].

Сучасні інформаційні механізми базуються на широкому використанні цифрових технологій, систем штучного інтелекту, великих даних. Це дозволяє значно підвищити швидкість та якість обробки інформації, покращити прогнозування розвитку ситуації, забезпечити більш ефективне планування та координацію дій. Водночас використання цифрових технологій створює нові ризики, пов'язані з кібербезпекою , захистом інформації, можливістю технологічних збоїв [23].

Складність об'єкта управління зумовлює необхідність застосування спеціальних підходів та методів управління, що враховують специфіку безпекової сфери. Особливості цієї специфіки включають: високу ступінь невизначеності та непередбачуваності загроз; необхідність швидкого реагування на критичні ситуації; потребу у забезпеченні секретності окремих аспектів діяльності; взаємозалежність між різними видами безпеки; необхідність координації з міжнародними партнерами. Ці особливості вимагають розробки адекватних механізмів управління, що забезпечують ефективність, оперативність та гнучкість у прийнятті та реалізації

управлінських рішень [2].

Суб'єктами державного управління у сфері національної безпеки і оборони виступають органи державної влади, які наділені відповідними повноваженнями у цій сфері. Центральне місце серед них займає Президент України як Верховний Головнокомандувач Збройних Сил України та голова Ради національної безпеки і оборони України. Рада національної безпеки і оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України. Верховна Рада України здійснює парламентський контроль у сфері національної безпеки і оборони, затверджує Воєнну доктрину України, приймає рішення про введення воєнного чи надзвичайного стану [124].

Кабінет Міністрів України забезпечує виконання рішень Ради національної безпеки і оборони України, що вводяться в дію указами Президента України, здійснює заходи щодо забезпечення обороноздатності і національної безпеки України. Міністерства та інші центральні органи виконавчої влади, які входять до сектору безпеки і оборони, реалізують державну політику у відповідних сферах національної безпеки. Така розгалужена система суб'єктів управління вимагає ефективних механізмів координації та взаємодії для забезпечення єдності управлінських дій [16].

Систематизація механізмів державного управління у сфері національної безпеки і оборони вимагає розробки їх науково обґрунтованої класифікації, що дозволяє краще зрозуміти природу, функції та особливості застосування різних типів управлінських інструментів. За функціональним призначенням механізми державного управління можна поділити на: механізми стратегічного планування, механізми оперативного управління, механізми контролю та моніторингу, механізми координації та взаємодії, механізми ресурсного забезпечення [101].

Механізми стратегічного планування включають розробку довгострокових концепцій, стратегій, доктрин у сфері національної безпеки і оборони. Вони забезпечують визначення пріоритетів, цілей та завдань

державної політики у цій сфері, формування концептуальних засад розвитку сектору безпеки і оборони. До цієї групи належать механізми розробки Стратегії національної безпеки України, Воєнної доктрини України, стратегій розвитку окремих складових сектору безпеки і оборони [5].

Механізми оперативного управління забезпечують щоденне функціонування сил безпеки і оборони, прийняття поточних управлінських рішень, реагування на загрози та виклики. Вони включають системи командування та управління, процедури прийняття рішень в умовах обмеженого часу, механізми мобілізації ресурсів у кризових ситуаціях. Особливого значення набувають автоматизовані системи управління, що забезпечують швидкість та точність прийняття рішень [7]. Механізми контролю та моніторингу призначені для забезпечення ефективності функціонування сектору безпеки і оборони, виявлення проблем та недоліків, оцінки результативності витрачання ресурсів. Вони включають системи внутрішнього та зовнішнього контролю, аудиту, інспектування, звітності. Особливе місце займають механізми демократичного цивільного контролю, що забезпечують підзвітність сил безпеки і оборони суспільству та його представницьким органам [152].

За характером впливу механізми державного управління поділяються на прямі та непрямі. Прямі механізми передбачають безпосередній владний вплив на об'єкт управління через видання наказів, розпоряджень, директив, застосування заходів примусу. Непрямі механізми базуються на створенні умов та стимулів для бажаної поведінки об'єкта управління без прямого примусу. До них належать економічні стимули, моральні заохочення, створення сприятливого інституційного середовища.

За ступенем формалізації розрізняють формальні та неформальні механізми управління. Формальні механізми закріплені у нормативно-правових актах, мають чітко визначені процедури застосування, підлягають офіційному контролю. Неформальні механізми базуються на традиціях, звичаях, особистих відносинах, неписаних правилах взаємодії. У сфері

національної безпеки переважають формальні механізми, що зумовлено потребою у чіткому регулюванні та контролі діяльності сил безпеки і оборони [157].

За часовими рамками застосування механізми поділяються на постійно діючі та тимчасові. Постійно діючі механізми забезпечують щоденне функціонування системи національної безпеки в нормальних умовах. Тимчасові механізми активізуються у кризових ситуаціях, під час загострення загроз, введення особливих правових режимів. Прикладом тимчасових механізмів є системи управління у воєнний час, під час надзвичайного стану, антитерористичних операцій [157].

За територіальним охопленням механізми управління поділяються на загальнонаціональні, регіональні та місцеві. Загальнонаціональні механізми діють на всій території держави і забезпечують єдність державної політики у сфері національної безпеки. Регіональні механізми враховують специфіку окремих регіонів, особливості загроз та викликів на регіональному рівні. Місцеві механізми адаптують загальнодержавну політику до конкретних умов територіальних громад [59].

Принципи державного управління у сфері національної безпеки і оборони включають законність, ефективність, відкритість та прозорість, підзвітність та підконтрольність суспільству, дотримання прав і свобод людини та громадянина, взаємну відповідальність держави та особи у сфері забезпечення національної безпеки. Реалізація цих принципів у практичній діяльності вимагає створення відповідних інституційних механізмів та процедур, що забезпечують їх дотримання [176]. Особливе місце серед принципів займає принцип демократичного цивільного контролю над сектором безпеки і оборони, що передбачає здійснення контролю з боку цивільних органів влади та громадянського суспільства за діяльністю сил безпеки і оборони. Цей принцип є одним із основних вимог для євроатлантичної інтеграції України та потребує системної імплементації в національне законодавство та практику управління. Демократичний

цивільний контроль включає парламентський контроль, громадський контроль, судовий контроль, контроль з боку засобів масової інформації [60].

1.2. Зарубіжний досвід формування систем управління сектором безпеки і оборони: міжнародні та європейські практики

Аналіз зарубіжного досвіду формування та функціонування систем управління сектором безпеки і оборони є важливою складовою наукового обґрунтування напрямів удосконалення відповідних механізмів в Україні. Особливої актуальності це питання набуває в контексті євроатлантичної інтеграції України та необхідності адаптації національної системи безпеки і оборони до стандартів і принципів НАТО та Європейського Союзу. Вивчення міжнародних практик дозволяє виявити найбільш ефективні моделі організації управління, механізми координації між різними структурами сектору, підходи до забезпечення демократичного цивільного контролю та інші аспекти, що можуть бути адаптовані до українських умов [158].

Сучасна система міжнародної безпеки формувалася протягом десятиліть і відображає еволюцію поглядів на характер загроз, принципи організації колективної безпеки, механізми співробітництва між державами. Після завершення "холодної війни" відбулася кардинальна трансформація архітектури європейської безпеки, що включала розширення НАТО на схід, формування нових інституцій безпеки, розвиток концепції кооперативної безпеки. Ці процеси суттєво вплинули на національні системи управління безпекою і обороною країн Європи, зумовивши необхідність їх адаптації до нових геополітичних реалій [77].

Північноатлантичний альянс як найбільш розвинена система колективної безпеки напрацював унікальний досвід інтеграції національних систем оборони в єдину багатонаціональну структуру. Принципи функціонування НАТО базуються на поєднанні національного суверенітету держав-членів з необхідністю забезпечення колективної безпеки. Це вимагає

високого ступеня координації між національними системами управління обороною, стандартизації процедур планування та командування, інтероперабельності збройних сил. Досвід НАТО демонструє можливості ефективного поєднання національних інтересів з колективними зобов'язаннями у сфері безпеки [61].

Інституційна структура НАТО включає політичний та військовий компоненти, що забезпечують баланс між цивільним контролем та професійним військовим управлінням. Рада Північноатлантичного альянсу є вищим органом прийняття рішень, що складається з представників всіх держав-членів. Військовий комітет забезпечує військове планування та керівництво операціями. Інтегрована командна структура об'єднує національні збройні сили під єдиним командуванням для виконання колективних завдань оборони [159].

Процес прийняття рішень у НАТО базується на принципі консенсусу, що забезпечує врахування інтересів всіх держав-членів, але може ускладнювати швидке реагування на загрози. Для подолання цієї проблеми розроблено механізми гнучкого реагування, що дозволяють окремим групам країн-членів здійснювати спільні дії без участі всього альянсу. Прикладом таких механізмів є багатонаціональні корпуси, спеціалізовані командування, тематичні центри передового досвіду. Досвід планування у НАТО демонструє важливість довгострокового стратегічного планування, що поєднується з гнучкістю оперативного реагування. Процес оборонного планування альянсу включає визначення колективних цілей оборони, розподіл завдань між державами-членами, координацію національних програм розвитку збройних сил. Такий підхід дозволяє оптимізувати використання ресурсів, уникнути дублювання зусиль, забезпечити комплементарність національних оборонних спроможностей [25].

Європейський Союз розвинув власну систему управління безпекою і обороною, що відрізняється від натівської моделі більшим акцентом на цивільних аспектах безпеки та комплексному підході до врегулювання криз.

Спільна політика безпеки та оборони ЄС (CSDP) охоплює широкий спектр інструментів: від дипломатичних та економічних засобів до військових місій та операцій. Така комплексність відображає розуміння сучасних загроз як багатовимірних явищ, що вимагають координованого застосування різних інструментів впливу [14].

Узагальнені результати порівняльного аналізу зарубіжних моделей управління сектором безпеки і оборони наведено в табл. 1.1.

Інституційна архітектура CSDP включає Європейську раду як вищий орган політичного керівництва, Раду ЄС як орган прийняття оперативних рішень, Комітет з питань політики та безпеки як координаційний орган, Військовий комітет та Військовий штаб ЄС як органи військового планування. Європейське оборонне агентство відповідає за розвиток оборонних спроможностей, координацію досліджень та розробок у сфері оборони, сприяння європейській оборонній співпраці. Особливістю європейського підходу є акцент на превентивній дипломації, управлінні кризами, постконфліктному відновленню. ЄС розвинув унікальний досвід цивільних місій, що включають поліцейські місії, місії з реформування сектору безпеки, місії з підтримки верховенства права. Такий підхід відображає розуміння безпеки як багатовимірного феномену, що вимагає не лише військових, але й цивільних засобів забезпечення [5].

Концепція комплексного підходу ЄС до безпеки передбачає координацію всіх доступних інструментів політики: дипломатичних, економічних, розвідувальних, правоохоронних, військових. Цей підхід визнає взаємозв'язок між внутрішньою та зовнішньою безпекою, необхідність одночасного вирішення корінних причин конфліктів та їх симптомів. Практична реалізація комплексного підходу вимагає високого ступеня міжінституційної координації, подолання організаційних бар'єрів між різними напрямами політики ЄС [88].

Таблиця 1.1

Порівняльний аналіз зарубіжних моделей управління сектором безпеки і оборони

Країна	Головний координаційний орган	Модель цивільного контролю	Особливості стратегічного планування	Уроки для України
США	Рада національної безпеки (NSC) при Президентові; Міністерство оборони (DoD)	Президентський контроль; потужний цивільний нагляд через Конгрес; принцип верховенства цивільного керівництва	Чотирирічний огляд оборони (QDR); Стратегія національної безпеки; програмно-бюджетний метод PPBS	Ієрархічна вертикаль управління реформами; парламентський контроль; результатоорієнтоване планування
Велика Британія	Комітет з питань національної безпеки (NSC) при Прем'єр-міністрові	Парламентський контроль; сильна роль Кабінету міністрів; незалежний аудит реформ	Стратегічний огляд оборони і безпеки (SDSR); інтегрований огляд (Integrated Review)	Міжвідомча координація; прозора звітність; інтеграція безпекової та зовнішньої політики
Польща	Бюро національної безпеки (ББН) при Президентові; Рада міністрів	Подвійний цивільний контроль: Президент + Прем'єр; парламентські комітети з питань оборони	Стратегічна концепція безпеки Польщі; чотирирічні плани модернізації ЗС; євроатлантична стандартизація	Двоконтурна система контролю; досвід євроатлантичної адаптації стандартів НАТО
Ізраїль	Кабінет з питань оборони і зовнішніх справ; ЦАХАЛ (ЦГШ)	Цивільне керівництво з потужним впливом воєнного командування; оперативна автономія ЗС в умовах постійної загрози	Щорічне оборонне планування; концепція багатовимірної оборони (MDO); адаптивне управління в умовах активних бойових дій	Управління реформами в умовах збройного конфлікту; інтеграція розвідки в планування; швидке прийняття рішень
Україна	РНБО України; Міністерство оборони; Генеральний штаб ЗСУ	Президентський контроль через РНБО; парламентський нагляд (Комітет ВРУ з питань нацбезпеки); цивільний міністр оборони	Стратегія національної безпеки України (2020, 2023); Стратегічний оборонний бюлетень; адаптація стандартів НАТО	Необхідність посилення міжвідомчої координації; впровадження індикативного моніторингу реформ; створення єдиного координаційного центру

Джерело: складено автором на основі аналізу нормативно-правових актів та наукових джерел

Досвід окремих європейських країн демонструє різноманітність національних моделей організації управління сектором безпеки і оборони, що відображає історичні традиції, геополітичне положення, характер загроз та викликів. Французька модель характеризується сильною президентською владою у сфері оборони та зовнішньої політики, централізованою системою управління, розвиненим оборонно-промисловим комплексом. Президент Республіки є главою збройних сил, головує в Раді оборони, приймає ключові рішення щодо застосування військової сили. Інституційна структура французької системи оборони включає Міністерство збройних сил, яке поєднує функції керівництва всіма видами збройних сил, Генеральний секретаріат національної оборони та безпеки як координаційний орган, Генеральний штаб збройних сил як орган військового планування та управління операціями. Особливістю французької моделі є розвиток автономних оборонних спроможностей, включаючи ядерне стримування, що відображає прагнення до стратегічної незалежності [142].

Німецька модель управління обороною формувалася під впливом історичного досвіду та конституційних обмежень на застосування збройних сил. Основними принципами є парламентський контроль над збройними силами, федеральна структура управління, акцент на багатосторонньому співробітництві в рамках НАТО та ЄС. Федеральний міністр оборони здійснює керівництво та командування збройними силами, Бундестаг приймає рішення про участь у зарубіжних операціях, федеральні землі беруть участь у територіальній обороні. Концепція "громадянина в уніформі" стала основою реформування німецьких збройних сил після Другої світової війни. Вона передбачає поєднання військової дисципліни з демократичними цінностями, забезпечення прав військовослужбовців, їх інтеграцію в громадянське суспільство. Інститут парламентського уповноваженого з питань збройних сил забезпечує захист прав військовослужбовців та здійснення парламентського контролю над армією [50].

Британська модель традиційно характеризується сильною роллю

прем'єр-міністра у питаннях оборони та національної безпеки, гнучкістю інституційних структур, акцентом на експедиційних спроможностях збройних сил. Комітет національної безпеки при уряді є центральним органом координації політики безпеки, що включає представників ключових міністерств та відомств. Рада оборони забезпечує стратегічне керівництво збройними силами під головуванням міністра оборони. Особливістю британського підходу є розвиток концепції фьюжн доктрини, що передбачає інтеграцію дипломатичних, інформаційних, військових та економічних інструментів для досягнення стратегічних цілей. Ця концепція відображає розуміння сучасних конфліктів як гібридних за природою, що вимагає відповідного реагування з боку держави. Практична реалізація фьюжн доктрини потребує тісної координації між різними відомствами та службами [62].

Скандинавські країни розвинули унікальну модель "тотальної оборони", що передбачає залучення всього суспільства до забезпечення національної безпеки. Ця модель включає не лише збройні сили, але й цивільну оборону, психологічну стійкість населення, економічну безпеку, кібербезпеку. Швецька концепція психологічної оборони спрямована на підготовку суспільства до протистояння інформаційним впливам та підтримання національної єдності в умовах кризи [60].

Фінська модель поєднує загальний призов до збройних сил з розвиненою системою резерву, що дозволяє швидко мобілізувати значні людські ресурси для оборони країни. Норвезький досвід демонструє ефективність децентралізованої системи територіальної оборони, що базується на місцевих ресурсах та знанні місцевості. Данська модель акцентує увагу на високотехнологічних спроможностях та участі в міжнародних операціях.

Досвід пострадянських країн, що приєдналися до НАТО, є особливо цінним для України, оскільки вони пройшли схожий шлях трансформації систем безпеки і оборони від радянської моделі до євроатлантичних

стандартів. Польща, Чехія, країни Балтії здійснили комплексні реформи, що включали демократизацію системи управління, професіоналізацію збройних сил, модернізацію озброєння та військової техніки, розвиток нових спроможностей.

Польський досвід демонструє важливість політичного консенсусу щодо євроатлантичної інтеграції, системності реформ, поступовості їх впровадження. Реформування польських збройних сил включало скорочення чисельності з одночасним підвищенням якості підготовки, модернізацію командної структури, розвиток професійного сержантського корпусу, впровадження натівських стандартів планування та управління.

Досвід країн Балтії є особливо показовим з точки зору швидкості та ефективності трансформації систем безпеки і оборони. Литва, Латвія та Естонія за відносно короткий період змогли створити сучасні збройні сили, інтегровані в євроатлантичні структури безпеки. Ключовими факторами успіху стали чітке стратегічне бачення, послідовність у проведенні реформ, активна підтримка з боку західних партнерів, ефективне використання міжнародної допомоги [162].

Естонський досвід цифровізації системи управління обороною є унікальним прикладом використання інформаційних технологій для підвищення ефективності управління. Естонія розвинула комплексну систему електронного урядування, що включає і сферу оборони. Цифрова трансформація дозволила значно скоротити бюрократичні процедури, підвищити швидкість прийняття рішень, забезпечити кращу координацію між різними структурами.

Латвійська модель територіальної оборони демонструє ефективність поєднання регулярних збройних сил з добровольчими формуваннями. Національна гвардія Латвії є резервним компонентом збройних сил, що залучає цивільних осіб на добровільній основі для участі в територіальній обороні. Така модель дозволяє збільшити оборонний потенціал країни при обмежених ресурсах, залучити громадянське суспільство до забезпечення

національної безпеки [68].

Литовський досвід реформування сектору безпеки включав не лише збройні сили, але й поліцію, прикордонні війська, спеціальні служби. Комплексний підхід до реформування дозволив забезпечити узгодженість дій різних структур, уникнути дублювання функцій, оптимізувати використання ресурсів. Особливої уваги заслуговує досвід створення єдиної системи кризового управління, що об'єднує цивільні та військові структури [12].

Американська модель управління національною безпекою характеризується складною інституційною архітектурою, що відображає федеральний устрій держави та розподіл повноважень між різними гілками влади. Рада національної безпеки при Президенті США є центральним органом координації політики безпеки, що забезпечує взаємодію між Білим домом, Пентагоном, Державним департаментом, розвідувальними службами та іншими відомствами [57].

Особливістю американської системи є чіткий розподіл між політичним керівництвом та військовим командуванням. Міністр оборони здійснює цивільний контроль над збройними силами, Об'єднаний комітет начальників штабів забезпечує військове планування та консультування політичного керівництва. Система регіональних та функціональних командувань дозволяє ефективно управляти американськими військовими силами по всьому світу [12].

Канадська модель демонструє ефективність інтегрованого підходу до управління безпекою і обороною в умовах федеральної держави. Департамент національної оборони поєднує функції оборони з функціями громадської безпеки, що дозволяє забезпечити кращу координацію між військовими та цивільними структурами. Канадські збройні сили мають уніфіковану структуру, що об'єднує сухопутні, морські та повітряні сили під єдиним командуванням [159].

Австралійський досвід реформування системи національної безпеки включав створення Департаменту прем'єр-міністра та кабінету як

центрального координаційного органу, розвиток національної розвідувальної спільноти, інтеграцію цивільних та військових спроможностей реагування на кризи. Австралійська модель "цілісного уряду" передбачає тісну координацію між різними відомствами для досягнення спільних цілей національної безпеки [60].

Ізраїльська модель управління обороною формувалася в умовах постійної загрози та обмежених ресурсів, що зумовило розвиток унікальних підходів до організації оборони. Система резерву, заснована на загальному призові та короткотерміновій службі з подальшими регулярними зборами, дозволяє підтримувати високий рівень боєготовності при відносно невеликих регулярних збройних силах. Тісна інтеграція цивільного та військового секторів економіки забезпечує швидку мобілізацію ресурсів у разі потреби [8].

Швейцарська модель нейтралітету поєднується з потужною системою територіальної оборони, що базується на загальному призові, розвиненій мережі укріплень, децентралізованій системі командування. Швейцарський досвід демонструє можливість забезпечення ефективної оборони без участі у військових альянсах, але з підтриманням високих стандартів підготовки збройних сил та готовності населення до оборони.

Аналіз зарубіжного досвіду дозволяє виділити кілька ключових тенденцій у розвитку систем управління безпекою і обороною. По-перше, зростає значення міжвідомчої координації та інтегрованого підходу до забезпечення безпеки. Сучасні загрози мають комплексний характер і вимагають координованого застосування різних інструментів державної політики. По-друге, посилюється роль цивільного контролю над сектором безпеки і оборони, що відображає демократичні принципи організації суспільства. По-третє, зростає значення міжнародного співробітництва у сфері безпеки і оборони. Глобальний характер сучасних загроз вимагає колективних зусиль для їх подолання. Країни активно розвивають багатосторонні механізми співробітництва, обмінюються досвідом,

координують свої дії. По-четверте, посилюється роль технологій у забезпеченні безпеки і оборони. Цифровізація, штучний інтелект, кібертехнології кардинально змінюють характер сучасних конфліктів та методи їх ведення [153].

По-п'яте, зростає значення превентивних заходів та управління кризами. Країни намагаються виявляти загрози на ранніх стадіях та запобігати їх ескалації. Це вимагає розвитку систем раннього попередження, аналітичних спроможностей, гнучких механізмів реагування. По-шосте, посилюється роль громадянського суспільства у забезпеченні національної безпеки. Держави намагаються залучити громадян до участі в забезпеченні безпеки, підвищити їх обізнаність щодо загроз та способів протидії їм [25].

Досвід міжнародних організацій у сфері безпеки і оборони демонструє різноманітність підходів до колективного забезпечення безпеки. Організація з безпеки і співробітництва в Європі (ОБСЄ) розвинула унікальну модель превентивної дипломатії та управління конфліктами, що базується на консенсусі та всеосяжному підході до безпеки. ОБСЄ акцентує увагу на політико-військовому, економіко-екологічному та людському вимірах безпеки, визнаючи їх взаємозв'язок та взаємозалежність. Інструменти ОБСЄ включають довгострокові місії, спостерігачів на виборах, програми з контролю над озброєннями, заходи з підвищення довіри та безпеки. Особливістю діяльності ОБСЄ є акцент на превенції конфліктів та постконфліктному відновленню. Організація розвинула ефективні механізми раннього попередження, що дозволяють виявляти потенційні конфлікти на ранніх стадіях та вживати заходів для їх запобігання [153].

Досвід ОБСЄ в Україні демонструє як можливості, так і обмеження міжнародних організацій у врегулюванні конфліктів. Спеціальна моніторингова місія ОБСЄ в Україні стала найбільшою цивільною місією організації, що здійснює спостереження за дотриманням режиму припинення вогню, моніторинг ситуації з правами людини, сприяння діалогу між сторонами конфлікту. Водночас обмеженість мандату місії та принцип

консенсусу в прийнятті рішень знижують ефективність ОБСЄ у врегулюванні збройного конфлікту. Африканський союз розвинув власну архітектуру миру і безпеки, що включає Раду миру і безпеки, Комісію Африканського союзу, регіональні економічні спільноти як будівельні блоки континентальної системи безпеки. Африканська модель акцентує увагу на принципі "африканські рішення для африканських проблем", що передбачає пріоритет регіональних механізмів у врегулюванні конфліктів [141].

Досвід Африканського союзу демонструє важливість регіонального підходу до забезпечення безпеки. Регіональні організації краще розуміють специфіку місцевих конфліктів, мають більшу легітимність у врегулюванні спорів, можуть швидше реагувати на кризи. Водночас обмежені ресурси та інституційна слабкість регіональних організацій часто перешкоджають ефективному виконанню ними функцій забезпечення безпеки [163].

Азіатсько-Тихоокеанський регіон характеризується відсутністю всеосяжної системи колективної безпеки, що зумовлено різноманітністю політичних систем, економічних моделей, культурних традицій країн регіону. Натомість розвинулася мережа двосторонніх альянсів та багатосторонніх діалогових механізмів. Асоціація держав Південно-Східної Азії (АСЕАН) розвинула унікальну модель співробітництва у сфері безпеки, що базується на принципах невтручання, консенсусу, неформального діалогу [59].

Американські альянси в Азіатсько-Тихоокеанському регіоні (з Японією, Південною Кореєю, Австралією, Філіппінами, Таїландом) утворюють мережу двосторонніх угод про безпеку, що забезпечують американську присутність у регіоні та стримування потенційних агресорів. Ця модель демонструє ефективність гнучких альянсових структур, що адаптуються до специфічних умов регіону.

Інновації у сфері управління безпекою і обороною включають розвиток концепції стійкості як здатності суспільства протистояти шокам та швидко відновлюватися після них. Ця концепція передбачає не лише готовність до

реагування на загрози, але й здатність адаптуватися до змін, навчатися на досвіді, постійно вдосконалювати свої захисні механізми. Стійкість стає ключовою характеристикою сучасних систем безпеки [24].

Розвиток концепції гібридних загроз вимагає нових підходів до організації систем безпеки і оборони. Гібридні загрози поєднують військові та невійськові засоби впливу, державних та недержавних акторів, відкриті та приховані дії. Протидія таким загрозам вимагає цілісного підходу, що інтегрує різні інструменти державної політики та залучає все суспільство до забезпечення безпеки. Кібербезпека стає дедалі важливішим компонентом національної безпеки. Країни розвивають національні стратегії кібербезпеки, створюють спеціалізовані структури для захисту кіберпростору, розвивають міжнародне співробітництво у цій сфері. Особливістю кіберсфери є стирання кордонів між внутрішньою та зовнішньою безпекою, цивільними та військовими структурами, державними та приватними акторами [159].

Штучний інтелект та автономні системи озброєння створюють нові можливості та виклики для систем управління безпекою і обороною. Ці технології можуть значно підвищити ефективність військових операцій, але водночас створюють нові етичні та правові дилеми. Країни активно досліджують можливості застосування штучного інтелекту в оборонних цілях, але також намагаються розробити міжнародні норми регулювання цих технологій [80].

Узагальнення зарубіжного досвіду дозволяє сформулювати кілька ключових висновків для України. По-перше, успішність реформування сектору безпеки і оборони значною мірою залежить від політичної волі керівництва держави та широкої суспільної підтримки реформ. По-друге, важливим є системний підхід до реформування, що охоплює всі компоненти сектору безпеки і оборони та забезпечує їх узгоджену трансформацію. По-третє, ефективність реформ підвищується при активному використанні міжнародної допомоги та експертизи. Співробітництво з міжнародними партнерами дозволяє прискорити процес адаптації до міжнародних

стандартів, уникнути типових помилок, використати накопичений досвід. По-четверте, важливим є поступовий характер реформ з урахуванням національних особливостей та наявних ресурсів. По-п'яте, ключовою є розробка довгострокової стратегії реформування з чіткими цілями, завданнями, індикаторами успіху. Стратегічне планування дозволяє забезпечити послідовність реформ, оптимізувати використання ресурсів, підтримувати мотивацію учасників процесу. По-шосте, важливим є забезпечення прозорості та підзвітності процесу реформування, залучення громадянського суспільства до моніторингу та оцінки результатів [57].

Досвід зарубіжних країн демонструє, що не існує універсальної моделі організації системи управління безпекою і обороною. Кожна країна розвиває власну модель з урахуванням своїх особливостей, але використання найкращих міжнародних практик дозволяє значно підвищити ефективність національних систем безпеки. Для України особливо цінним є досвід країн, що пройшли схожий шлях трансформації та успішно інтегрувалися в євроатлантичні структури безпеки [34].

1.3. Сучасні підходи до оцінки ризиків і загроз у контексті гібридних викликів

Трансформація системи міжнародних відносин на початку XXI століття зумовила кардинальні зміни в характері загроз національній безпеці держав, що потребує переосмислення традиційних підходів до їх оцінки та управління ними. Якщо в умовах біполярної системи міжнародних відносин превалювали загрози, які можна було категоризувати за чітко визначеними критеріями, то сучасні виклики характеризуються комплексністю, взаємопов'язаністю та непередбачуваністю розвитку. Особливо гостро ця проблема постала після терористичних атак 11 вересня 2001 року, які продемонстрували неспроможність традиційних систем оцінки ризиків

адекватно передбачити та попередити асиметричні загрози [136].

Подальший розвиток подій, включаючи фінансову кризу 2008 року, пандемію COVID-19 та розгортання повномасштабної російської агресії проти України у 2022 році, остаточно засвідчив актуальність формування нових підходів до оцінки ризиків, здатних врахувати специфіку гібридних форм ведення війни та міждисциплінарний характер сучасних загроз національній безпеці. Ці події стали каталізатором переосмислення ролі державного управління в забезпеченні національної безпеки та актуалізували необхідність розробки проактивних механізмів виявлення, оцінки та реагування на потенційні ризики [83].

Еволюція теоретичних підходів до оцінки ризиків національної безпеки відображає загальні тенденції трансформації державного управління від реактивних до проактивних моделей. Традиційна постановка питання в науковій літературі про окрему оцінку економічних, політичних , військових та інших ризиків вимагала кардинальних змін під впливом глобальних трансформацій, геополітичної турбулентності та зростання економічних і військових ризики. Неочікуваний характер та інтенсивність поширення COVID-19 у поєднанні з іншими виявленими гібридними ризиками визначили значні недоліки в системі оцінки загроз національній безпеці більшості держав світу. Ключовою проблемою традиційних підходів стала їх фрагментарність та відсутність системного бачення взаємозв'язків між різними сферами національної безпеки. Класичні моделі оцінки ризиків, розроблені в умовах відносно стабільного міжнародного порядку, виявилися неспроможними врахувати динамічний характер сучасних загроз та їх здатність до трансформації та адаптації. Це актуалізувало необхідність розробки нових теоретично-методологічних підходів, здатних забезпечити комплексне розуміння природи ризиків та їх потенційного впливу на різні аспекти функціонування держави [77].

Концептуальною основою сучасних підходів до оцінки ризиків стала теорія " упереджувального державного управління" (Anticipatory

Governance), яка формувалася протягом останніх двадцяти років в академічній літературі Заходу та впроваджується на практиці в розвідувальному співтоваристві США та НАТО. Ця теорія базується на розумінні того, що ефективне управління національною безпекою потребує не тільки реагування на актуальні загрози, але й здатності передбачати та попереджати їх виникнення. Упереджувальне управління розглядається як система інститутів, правил та норм, які дозволяють використовувати передбачення з метою зниження ризиків та підвищення здатності реагувати на події на ранніх, а не більш пізніх стадіях їх розвитку [136].

Методологічною основою упереджувального управління став делиберативний метод ранжування ризиків (Deliberative Method), який передбачає активне залучення експертного співтовариства до процесів оцінки загроз та прийняття управлінських рішень. Цей підхід базується на принципах колективного прийняття рішень, використання множинних джерел інформації та систематичної оцінки альтернативних сценаріїв розвитку подій. Відмінністю делиберативного методу від традиційних експертних підходів є акцент на процедурній справедливості, транспарентності процесу прийняття рішень та врахуванні різних точок зору на природу та характер потенційних ризиків.

Класифікацію гібридних загроз національній безпеці України за вимірами, формами прояву та об’єктами впливу відображено на рис. 1.2.

Делиберативний метод ранжування ризиків, вперше розроблений дослідниками з Університету Карнеги-Меллона в 1980-х роках, спочатку застосовувався для ранжування та оцінки ризиків у природоохоронній діяльності, питаннях здоров'я та безпеки в школах. До 2004-2005 років цей метод був розширений до загальної оцінки екологічних загроз, а згодом адаптований для потреб національної безпеки. Методологія включає п'ять основних етапів, кожен з яких має критичне значення для забезпечення якості та достовірності результатів оцінки [57].

ВИМІР ЗАГРОЗИ	ФОРМИ ПРОЯВУ	ПРИКЛАДИ (з 2014 р.)	ОБ'ЄКТ ВПЛИВУ
Воєнний	Збройна агресія; окупація; гібридні операційні групи	Окупація Криму (2014); Донбас; повномасштабне вторгнення (2022)	Суверенітет; тер. цілісність
Кібернетичний	Атаки на КІ; DDoS; шкідливе ПЗ; кіберрозвідка	NotPetya (2017); атаки на Укренерго; ГРУ-операції	Держоргани; енергосистема; фін. сектор
Інформаційно-психологічний	Дезінформація; пропаганда; маніпулювання	RT/Sputnik; тролінг у соцмережах; наратив 'братніх народів'	Суспільна думка; нац. ідентичність
Економіко-енергетичний	Газові шантажі; санкції; блокади; економічний тиск	Газові кризи 2006, 2009; блокада Азовського моря (2018)	Ек. стабільність; енергетика
Внутрішньо-політичний	Підтримка сепаратизму; дестабілізація	Проросійські партії; провокації у Харкові (2014)	Конституційний лад; суспільна єдність

Рис. 1.2. Класифікація гібридних загроз національній безпеці України

Джерело: складено автором на основі аналізу досвіду протидії збройній агресії РФ з 2014 р.

Перший етап передбачає концептуалізацію ризиків та їх класифікацію, що включає визначення меж дослідження, ідентифікацію ключових стейкхолдерів та формулювання основних питань, на які має дати відповіді аналіз. Другий етап зосереджується на визначенні характеристик ризиків, які слід використовувати для їх опису та порівняння. Третій етап передбачає детальний опис ризиків з точки зору їх характеристик у зведених таблицях ризиків, які відображають найкращі практики передачі інформації про ризики. Четвертий етап включає вибір учасників та проведення оцінки ризиків за допомогою фокусних груп експертів. П'ятий етап передбачає аналіз результатів семінарів та виявлення відповідних проблем з отриманих рейтингів.

Розвиток делиберативної методології знайшов подальше втілення у роботах американської корпорації RAND, які стали основоположними для формування відповідних підходів органами виконавчої влади США та Великої Британії. Методологія RAND передбачає поєднання

делиберативного методу з технологіями Delphi та Stakeholders Engagement, що дозволяє забезпечити більш широке залучення заінтересованих сторін до процесів оцінки ризиків національної безпеки. Важливою особливістю підходу RAND є використання методу PortMan, який виконує оцінки компонентів вартості та ризику для кожного проекту на основі узгодженого набору показників, пов'язаних з функціями або можливостями [62].

Однак застосування делиберативного методу має певні обмеження, які необхідно враховувати при його використанні для оцінки ризиків національної безпеки. По-перше, цей метод значну увагу приділяє класифікації та характеристикам суттєвості ризику, залишаючи сам процес оцінки переважно "консультативним", де провідну роль відіграють експерти та співробітники органів виконавчої влади. По-друге, через нестачу часу для аналізу рішень неможливо застосовувати багатоатрибутні методології, такі як теорія багатоатрибутної корисності або процес аналітичної ієрархії. По-третє, порядкове ранжування не вказує на відносні або абсолютні відмінності в величині ризиків, що ускладнює прийняття рішень про значущість різних загроз.

Особливого значення в контексті сучасних підходів до оцінки ризиків набуває концепція гібридних загроз, які поєднують традиційні та нетрадиційні засоби впливу на національну безпеку держав. Гібридні загрози характеризуються використанням широкого спектру інструментів - від кібератак та інформаційних операцій до економічного тиску, дипломатичного впливу та застосування нерегулярних збройних формувань. Ця багатовимірність робить гібридні загрози складними для виявлення та оцінки засобами традиційних підходів, які зосереджуються на окремих категоріях ризиків [175].

Ключовою характеристикою гібридних загроз є їх здатність до адаптації та трансформації залежно від контексту та реакції об'єкта впливу. На відміну від традиційних загроз, які мають відносно стабільні характеристики, гібридні загрози можуть швидко змінювати свої форми

прояву, використовувати різні комбінації інструментів впливу та адаптуватися до контрзаходів, які вживаються для їх нейтралізації. Це створює особливі виклики для систем раннього попередження та вимагає розробки адаптивних підходів до оцінки та управління ризиками.

Аналіз сучасних конфліктів демонструє, що гібридні загрози мають тенденцію до латентного розвитку в рамках уже існуючих трендів, що значно ускладнює їх своєчасне виявлення традиційними методами розвідки та аналізу. Прикладом такого латентного розвитку може служити поступова ескалація російської агресії проти України, яка розпочалася з економічного та інформаційного тиску, переросла у підтримку сепаратистських рухів, анексію Криму та збройну агресію на Донбасі, і кульмінувала повномасштабним вторгненням у лютому 2022 року.

Це актуалізує необхідність розробки нових методологічних підходів, здатних забезпечити раннє попередження про потенційні ризики та своєчасне реагування на них з боку органів державної влади. Такі підходи повинні поєднувати традиційні методи збору та аналізу інформації з інноваційними технологіями, включаючи аналіз великих даних, машинне навчання та штучний інтелект. Трансформація характеру загроз зумовила еволюцію від систем національної безпеки, орієнтованих переважно на військові аспекти, до більш широких концепцій управління ризиками та загрозами всіх рівнів, що закріпилися в західних суспільствах після закінчення холодної війни. Цей перехід відображає визнання того факту, що все більш складні та транснаціональні ризики, такі як критичні відмови інфраструктури, глобальні пандемії або масштабні терористичні атаки, вимагають нових підходів до оцінки ризиків, які виходять за межі традиційних військово-політичних категорій [8].

Концепція управління безпекою набула відомості як наукова концепція та політична практика, що відображає перехід до більш децентралізованої, неформальної та ієрархічної координації між різними акторами системи національної безпеки. Паралельно з цим, вже з 1980-х років систематичне

управління ризиками зарекомендувало себе як стандарт для сучасних суспільств, які прагнуть передбачити та мінімізувати потенційно руйнівні небезпеки та інциденти. Ідея управління ризиками була також перенесена в сферу безпеки як спосіб подолання невизначеності глобалізаційної обстановки в області безпеки після закінчення холодної війни [34].

Особливо важливою в цьому контексті стала концепція "стійкості" (resilience), яка була додана до картини як нова концепція, що може утвердитися в якості глобального метанаративу в сфері безпеки. Концепція стійкості визнає, що уряди, принаймні в межах розумних витрат, не можуть гарантувати ефективну захист усіх людей і об'єктів від усіх видів непередбачених криз і катастроф і, отже, необхідно дати можливість розширити можливості суспільства та громадян, щоб впоратися з такими подіями. Це вимагає систематичних зусиль з планування та підготовки до фактичної кризи, включаючи інформацію про види сценаріїв та збиток, який слід очікувати [111; 149].

Важливою характеристикою сучасних підходів до оцінки ризиків є їх спрямованість на комплексний аналіз взаємозв'язків між різними сферами національної безпеки. Це знайшло відображення у розробці інтегрованих моделей, які об'єднують множину індикаторів та показників для оцінки ризиків. Такі моделі використовують статистичні методи, множинні регресії та аналіз часових рядів для більш точного прогнозування потенційних загроз. Еволюція індикативної оцінки ризиків умовно може бути поділена на три основних етапи: ранні методи, що використовували прості індикатори; розвиток інтегрованих моделей, які об'єднували множину індикаторів; використання технологій та великих даних з машинним навчанням [69].

Особливе місце в сучасній методології оцінки ризиків займає розвиток інформаційних технологій та доступність великих даних, що дозволяє використовувати машинне навчання та алгоритми глибокого навчання для аналізу великих обсягів інформації та виявлення прихованих патернів і тенденцій. Аналітики можуть тепер використовувати машинне навчання та

алгоритми глибокого навчання для аналізу великих обсягів даних та виявлення прихованих патернів і тенденцій, що кардинально змінює можливості в сфері національної безпеки [66].

Передбачається, що штучний інтелект змінить процес прийняття рішень у сфері оборони та безпеки чотирма основними способами. По-перше, за рахунок можливості "когнітивного маневру" з використанням предиктивної аналітики для більш раннього втручання. По-друге, змушуючи людей виходити "з циклу" для прийняття рішень, випереджаючи їх у все більшому числі областей. По-третє, складаючи поради, які вірні, але важко пояснювані. По-четверте, в короткостроковій перспективі, надаючи безпрецедентну суворість процесам прийняття рішень і змушуючи осіб, що приймають рішення, набагато більш чітко описувати ментальні моделі, на яких вони базують рішення.

Однак впровадження нових технологій у сферу оцінки ризиків національної безпеки також створює нові виклики та обмеження. Зокрема, актуалізується проблема забезпечення балансу між автоматизованою аналітикою та експертною оцінкою, оскільки надмірна залежність від алгоритмів може призвести до втрати контексту та нюансів, важливих для адекватного розуміння характеру загроз. Крім того, використання штучного інтелекту в аналізі ризиків національної безпеки піднімає питання про етику, підзвітність та транспарентність процесів прийняття рішень, особливо коли йдеться про рекомендації, які важко пояснити [97; 144].

Розвиток підходів до оцінки ризиків також тісно пов'язаний з еволюцією концепцій "адаптивного управління" та " упереджувальної демократії". Адаптивне управління визнає, що хоча люди в основному є раціональними соціальними акторами, їх знання недосконалі, нерівномірно розподілені, і вони застосовують різні критерії оцінки до різних інституційних умов залежно від комунікацій або прозорості. Адаптивне управління базується на системному підході, на відміну від "рефлексивних" підходів технологічних переходів та концепції залежності від попереднього

розвитку.

Упереджувальна демократія передбачає більш активну участь у формуванні майбутнього, використовуючи Форсайт та підхід "бажаного майбутнього". Цей підхід спрямований на прогнозування сценаріїв майбутнього та використання їх для поліпшення бачення та створення бажаної реальності, що пов'язує дану групу досліджень з так званими "дослідженнями майбутнього", які досить поширені на Заході.

Порівняльний аналіз міжнародних систем оцінки ризиків національної безпеки демонструє різноманіття підходів та методологій , що відображає специфіку геополітичного позиціонування держав, особливості їх інституційних систем та історичний досвід протистояння різним типам загроз. Після терористичних атак 11 вересня 2001 року витрати уряду США на внутрішню безпеку зросли з 16 мільярдів доларів до майже 70 мільярдів доларів на рік у 2013 році, не кажучи вже про додаткові витрати на зарубіжні військові операції та розвідку. Здійснення такого роду діяльності зі складно прогнозованим результатом є складним завданням і вимагає у своїй основі розуміння ризиків, якими необхідно управляти [12].

Американська модель оцінки ризиків національної безпеки базується на широкій мережі розвідувальних агентств та аналітичних центрів, що працюють у рамках скоординованої системи збору, аналізу та поширення інформації. Ключовими учасниками цього процесу є Національна рада з розвідки, Центральне розвідувальне управління, Федеральне бюро розслідувань, Міністерство внутрішньої безпеки, Міністерство оборони, Державний департамент та Агентство національної безпеки. Кожна з цих організацій має свої специфічні функції та області відповідальності, але всі вони інтегровані в єдину систему національної безпеки [41].

Методологічно американський підхід зосереджується на сценарному аналізі та ризик-орієнтованому підході, що включає ідентифікацію, оцінку та пріоритизацію ризиків на основі їх ймовірності та потенційного впливу. Сценарний аналіз включає розробку гіпотетичних сценаріїв для оцінки

потенційних ризиків та їх можливого впливу на національну безпеку. Різні сценарії, такі як терористичні атаки, кібератаки або геополітичні конфлікти, досліджуються для розуміння їх ймовірності та потенційних наслідків [69].

Однак, як показав комплексний аналіз підходів, оцінка цих ризиків виявилася проблематичною. У 2010 році комітет Національної академії наук США, що розглядав підхід Міністерства внутрішньої безпеки США до аналізу ризиків, рекомендував не використовувати інтегровані кількісні оцінки ризиків у своїх методологічних підходах через неоднорідність ризиків та складність побудови інтегрованої моделі. Зосередження на кількісних показниках оцінки ризику призводить до спрощення або ігнорування багатьох аспектів, включаючи соціальні, психологічні та політичні наслідки потенційних загроз [68].

Європейська модель оцінки ризиків національної безпеки характеризується акцентом на співробітництві між державами-членами ЄС та використанням сценарного аналізу для вивчення потенційних загроз безпеці. Система оцінки ризиків на рівні ЄС не має централізованої організації, аналогічної агентствам США, а базується на координації між різними інститутами ЄС та державами-членами. Оцінка ризиків національної безпеки ЄС базується на двох ключових компонентах - Загальній компоненті, що займається загрозами внутрішньої безпеки, та Стратегічній компоненті, що оцінює зовнішні загрози та виклики [77].

Ключовими інститутами, що виконують функції оцінки ризиків у ЄС, є Європейський центр з контролю за хворобами, Європол, Європейська служба зовнішніх зв'язків, Європейське агентство з безпеки мереж та інформації, та Розвідувальний і ситуаційний центр Європейського союзу. Кожен з цих інститутів спеціалізується на певних аспектах безпеки, але всі вони працюють у рамках загальної стратегії ЄС щодо внутрішньої безпеки [82].

Особливістю європейського підходу є намагання поєднати технократичну легітимацію з демократичним контролем, що відображається в прагненні до більшої прозорості та громадського обговорення процесів

оцінки ризиків. Європейська комісія опублікувала загальні керівні принципи проведення національних оцінок ризиків у сфері управління кризами та стихійними лихами, які передбачають формування національних систем оцінки ризиків, що враховують від 50 до 100 сценаріїв середньо- та довгострокового характеру.

Проте розвиток комплексних оцінок ризиків у Європі піддається критичному аналізу з точки зору їх впливу на процеси європейської інтеграції. Просування стандартизованих або науково-орієнтованих оцінок ризиків може розглядатися як ще один значущий, хоча й прихований, інструмент для просування політики внутрішньої безпеки ЄС на більш широкій основі. Оцінки ризиків є технократичною формою розробки політики безпеки, яка використовує начебто об'єктивні знання для легітимації та раціоналізації спірних рішень та інститутів [163].

Китайський досвід оцінки ризиків національної безпеки нерозривно пов'язаний з оцінками "комплексної потужності" держави, яка розуміється як сукупність економічної, військової та політичної могутності країни в певний період. Ці оцінки здійснюються китайськими вченими з кінця 1980-х років і значною мірою мають у своїй методологічній основі роботи західних політологів. Китайські методики оцінки комплексної потужності інтегрували у свій кількісний апарат не тільки статистичні індикатори та показники, але й достатньо гнучкі експертні оцінки. У перших оцінках комплексної потужності держави враховувалися наступні параметри: технології, трудові ресурси, капітал, інформація, природні ресурси, військова потужність, ВВП, дипломатія та контрольно-регулятивна потужність уряду [31].

Спільною тенденцією розвитку міжнародних систем оцінки ризиків є перехід від вузькоспеціалізованих підходів до комплексних методологій , що враховують взаємозв'язки між різними сферами національної безпеки. Це знаходить відображення у формуванні національних оцінок ризиків, які враховують широкий спектр потенційних загроз, включаючи природні катастрофи, техногенні аварії, кібератаки, терористичні загрози, пандемії та

геополітичні конфлікти [13].

Індикативний підхід до оцінки ризиків національної безпеки являє собою методологію, основану на використанні визначених індикаторів або показників, які можуть вказувати на можливі ризики або потенційні загрози. Цей підхід можна віднести до інструментальних підходів і, говорячи ширше, до інструментальних теорій, предмет яких формується під впливом застосовуваних методів, зокрема методів математичної статистики. Інструментальний характер індикативного підходу характеризує його застосовність переважно не до об'єктів фізичного світу, а до опосередкованих предметів і об'єктів, які є продовженням інтелектуальної діяльності людини [99].

Теоретичною основою індикативного підходу є акторно-мережева теорія, згідно з якою людські суб'єкти не є єдиними суб'єктами, які складають соціальну сферу, оскільки нелюдські суб'єкти також є її частиною. Внесок акторно-мережевої теорії в соціальну теорію полягає у визнанні того, що соціальні суб'єкти та соціальні відносини не існують без нелюдських суб'єктів, і якщо вони будуть вивчені в ізоляції один від одного, можна упустити важливу динаміку. Це особливо актуально в контексті достатньо цікавої концепції військово-технічного детермінізму, згідно з якою сам факт володіння тими чи іншими технологіями військового призначення може здійснювати зворотний вплив на дії держав як акторів міжнародних відносин [70].

Поєднання теорії індикативних оцінок та акторно-мережевої теорії, що задає параметри аналітики, прийнятної для взаємодії акторів, дозволить забезпечити більш ефективну побудову та подальше застосування системи оцінки ризиків національної безпеки. Процес прийняття рішень та управління постійно реалізуються на основі зв'язків між суб'єктами та змістом, з яким вони мають справу. Це створює можливості для поєднання оцінок в рамках методології оцінки ризиків національної безпеки держави [59].

Практичне застосування індикативного підходу передбачає

формування системи індикаторів, що охоплює різні сфери національної безпеки. Мілітарні індикатори включають військовий бюджет, чисельність збройних сил, арсенал ядерної та хімічної зброї, військові операції. Економічні індикатори охоплюють валютний обмін та інфляцію, зовнішньоторговельний баланс, ріст ВВП, зайнятість та безробіття. Соціальні індикатори включають демографічні показники, рівень освіти, рівень бідності та нерівності, охорону здоров'я. Політичні індикатори відображають політичну стабільність, рівень корупції, громадянські права та свободи [175].

Особливого значення в контексті сучасних загроз набувають індикатори кібербезпеки, що відслідковують кібератаки та інциденти, рівень кіберзахисту. Екологічні індикатори включають екологічні катастрофи, забруднення навколишнього середовища, зміну клімату. Кримінальні індикатори охоплюють рівень злочинності, транснаціональну злочинність.

Індикативний підхід до застосування цих індикаторів при аналізі державної національної безпеки полягає в тому, щоб постійно збирати та обробляти масиви державних даних, що відносяться до цих індикаторів; одержувані індекси по кожному з індикаторів ранжувати для кожної з країн, отримуючи рейтинги країн по відповідним індексам; за допомогою кореляційного аналізу ранжувань знаходити дублюючі індекси та усувати дублювання; виявляти тренди переміщення країн в ранжуваннях та встановлювати коридори допустимої державної динаміки; у випадках виходу за межі коридорів фіксувати настання ризиків та загроз національній безпеці [99].

Методологічною особливістю індикативного підходу є застосування методу головних компонент для усунення статистичного дублювання між індикаторами та показниками. Цей метод дозволяє агрегувати ряд змінних у невелику кількість головних компонент, досягаючи таким чином усунення статистичного дублювання при мінімальній втраті корисної інформації. Ефективність цього методу для створення удосконалених композитних індексів, що оцінюють різні латентні ключові соціально-економічні

характеристики і при цьому не дублюють один одного, була обґрунтована на прикладі індексів високотехнологічного розвитку.

Застосування методу головних компонент дозволяє виділити базові індекси, що відображають різні латентні ключові характеристики національної безпеки. Зокрема, аналіз дозволяє виділити такі основні компоненти, як загальний рівень безпеки, що відображає загальний рівень підтримання правопорядку та стабільності; виникнення конфліктів, що відображає реальну частоту більш крупних конфліктів; стійкість уряду, що відображає ступінь статичності уряду ; міжетнічну напруженість, що поєднує стабільність уряду з наявністю міжетнічної напруженості [135].

Індикативна оцінка ризиків розглядається як складова частина "датазалежного" державного управління, яке базується на принципах доказової політики. Доказова політика являє собою підхід до розробки та реалізації державної політики, в якому рішення та заходи приймаються на основі ретельного аналізу наукових досліджень та зібраних даних. Основний принцип доказової політики полягає в тому, що державні дії та програми повинні бути засновані на наукових фактах, емпіричних доказах та кращих практиках [156].

Рух за політику, засновану на фактичних даних, прагнув сприяти ретельному аналізу програм послуг та варіантів політики, тим самим забезпечуючи корисний внесок для політиків у їх постійному розгляді питань розробки політики та поліпшення програм. Однак тепер стало ясно, що перші надії на масштабні та швидкі поліпшення в політиці та програмах в результаті більш тісної інтеграції з ретельними дослідженнями не матеріалізувалися так швидко, як очікувалося.

Специфіка застосування сучасних підходів до оцінки ризиків і загроз у контексті України визначається особливостями геополітичного становища держави, характером загроз, з якими вона стикається, та необхідністю адаптації міжнародних методологій до національних умов. Досвід України демонструє критичну важливість розробки системи раннього попередження

про гібридні загрози, яка б поєднувала традиційні методи розвідки з сучасними технологіями аналізу великих даних.

Формування ефективної національної системи оцінки ризиків потребує врахування декількох ключових чинників. По-перше, це необхідність інтеграції різних відомств та агентств у єдину систему координації, що дозволить забезпечити комплексний підхід до аналізу загроз. По-друге, важливою є розробка національної методології індикативних оцінок, адаптованої до специфіки українських реалій та сумісної з міжнародними стандартами. По-третє, критично важливим є розвиток спроможностей щодо моніторингу та оцінки інформаційних загроз, кібератак та інших форм гібридного впливу [113].

Впровадження індикативного підходу в українських умовах потребує формування національної системи індикаторів та показників, що враховуватиме специфіку викликів, з якими стикається держава. Це включає розробку індикаторів територіальної цілісності, соціальної згуртованості, економічної стійкості та інформаційної безпеки. Особливої уваги потребує створення системи моніторингу регіональних ризиків, враховуючи неоднорідність загроз у різних регіонах країни. Перспективи розвитку національної системи оцінки ризиків пов'язані з інтеграцією до європейських та євроатлантичних систем безпеки, що передбачає гармонізацію методологій та стандартів, розвиток спільних механізмів моніторингу та реагування на загрози. Це створює можливості для використання кращих міжнародних практик та отримання доступу до сучасних технологій аналізу ризиків [141].

Таким чином, сучасні підходи до оцінки ризиків і загроз у контексті гібридних викликів характеризуються переходом від традиційних реактивних моделей до проактивних систем упереджувального управління, що базуються на принципах індикативного аналізу та використанні сучасних технологій обробки великих даних.

Висновки до розділу 1

У першому розділі дисертаційного дослідження здійснено комплексний аналіз теоретичних засад механізмів державного управління сектором безпеки і оборони, що дозволяє сформулювати наступні основні висновки:

Дослідження показало, що сучасна теорія державного управління у сфері національної безпеки базується на інтеграції кількох теоретично-методологічних підходів: теорії державного управління, теорії національної безпеки, інституціональної теорії та системного підходу. Ключовою особливістю механізмів державного управління сектором безпеки і оборони є їх комплексний характер, що передбачає поєднання різних інструментів впливу - нормативно-правових, організаційних, економічних, інформаційних та технологічних [13].

Встановлено, що національна безпека як об'єкт державного управління має динамічний характер і потребує постійної адаптації управлінських механізмів до змінюваних внутрішніх та зовнішніх умов. Специфіка державного управління у сфері безпеки і оборони полягає у необхідності забезпечення балансу між ефективністю та демократичною підзвітністю, централізацією та децентралізацією, секретністю та транспарентністю [157].

Типологія механізмів державного управління сектором безпеки і оборони включає інституційні механізми (створення та функціонування спеціалізованих органів), процедурні механізми (стратегічне планування, координація, контроль), ресурсні механізми (бюджетне фінансування, матеріально-технічне забезпечення) та інформаційні механізми (розвідка, аналітика, комунікації) [101].

Компаративний аналіз міжнародних практик дозволив виявити основні моделі організації систем управління сектором безпеки і оборони. Модель НАТО характеризується принципом колективної безпеки, стандартизацією процедур оборонного планування та інтеграцією національних систем управління. Ключовими елементами є цикл оборонного планування, система командування та управління, механізми міжвідомчої координації [156].

Модель ЄС базується на концепції комплексного підходу до безпеки (comprehensive approach), що передбачає інтеграцію цивільних та військових інструментів, превентивну дипломатію та пост-конфліктне відновлення. Особливістю європейського підходу є акцент на цивільному управлінні сектором безпеки і оборони та демократичному контролі [112].

Національні моделі провідних країн світу демонструють різноманітність підходів: французька модель президентського управління, німецька модель парламентського контролю, британська модель кабінетної системи, американська модель розподілу повноважень між виконавчою та законодавчою владою. Досвід пострадянських країн показує важливість поетапних реформ та адаптації західних стандартів до національних особливостей.

Для України особливу цінність має досвід країн, що здійснили успішний транзит від авторитарних до демократичних систем управління сектором безпеки і оборони, зокрема Польщі, країн Балтії, які поєднали реформування систем управління з євроатлантичною інтеграцією.

Аналіз еволюції підходів до оцінки ризиків національної безпеки показав перехід від традиційних реактивних моделей до проактивних систем упереджувального управління (Anticipatory Governance). Ключовою особливістю сучасних підходів є здатність до раннього виявлення та попередження загроз на основі систематичного аналізу індикаторів та трендів.

Делиберативний метод ранжування ризиків, розроблений в Університеті Карнегі -Меллона та удосконалений корпорацією RAND, став методологічною основою для формування систем оцінки ризиків у провідних країнах світу. Цей підхід забезпечує поєднання експертного аналізу з кількісними методами оцінки та враховує множинні фактори ризику. Особливе значення набуває концепція гібридних загроз, які поєднують традиційні та нетрадиційні засоби впливу і характеризуються латентним розвитком, адаптивністю та міждисциплінарним характером. Оцінка таких

загроз потребує нових методологічних підходів, що інтегрують різні джерела інформації та використовують сучасні технології аналізу даних.

Індикативний підхід до оцінки ризиків базується на акторно-мережевій теорії та передбачає систематичний моніторинг широкого спектру індикаторів національної безпеки з використанням методу головних компонент для усунення статистичного дублювання. Цей підхід є складовою частиною "датазалежного" державного управління та доказової політики [67].

На основі проведеного аналізу встановлено, що ефективні механізми державного управління реформуванням сектору безпеки і оборони повинні базуватися на наступних принципах: системності та комплексності; адаптивності та гнучкості; демократичного цивільного контролю; транспарентності та підзвітності; професіоналізації та деполітизації; міжвідомчої координації та інтеграції.

Теоретичною основою для розробки механізмів державного управління реформуванням має стати синтез неоінституціональної теорії, теорії стратегічного управління та концепції упереджувального управління. Це дозволить забезпечити поєднання довгострокового стратегічного планування з оперативним реагуванням на зміни у безпековому середовищі [101].

Специфіка українського контексту вимагає врахування факторів гібридної війни, необхідності одночасного проведення реформ та забезпечення оборони, інтеграції до євроатлантичних структур безпеки. Це актуалізує потребу у розробці адаптивних механізмів управління, здатних функціонувати в умовах невизначеності та високого рівня ризиків [44; 53].

Проведений теоретичний аналіз створює підґрунтя для емпіричного дослідження сучасного стану державного управління сектором безпеки і оборони України, виявлення основних проблем та розробки практичних рекомендацій щодо удосконалення механізмів управління реформами. Особливої уваги потребують питання формування системи індикаторів ефективності реформ, механізмів координації між різними органами влади та

інститутами громадянського суспільства, а також адаптації міжнародних стандартів до українських реалій [164].

Таким чином, теоретичні засади механізмів державного управління сектором безпеки і оборони, розглянуті в першому розділі, створюють концептуальну базу для подальшого аналізу практичних аспектів реформування та розробки рекомендацій щодо удосконалення системи управління в цій критично важливій сфері державної політики [32].

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ДЕРЖАВНОГО УПРАВЛІННЯ СЕКТОРОМ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

2.1. Оцінка ефективності існуючих механізмів державного управління сектором безпеки і оборони

Ефективність механізмів державного управління сектором безпеки і оборони України є критично важливою для забезпечення національної безпеки держави, особливо в умовах триваючої російської агресії та гібридних викликів сучасності. Оцінка цієї ефективності потребує комплексного підходу, що враховує як інституційні, так і функціональні аспекти діяльності органів державної влади у сфері безпеки і оборони [170].

Методологічною основою оцінки ефективності механізмів державного управління сектором безпеки і оборони має стати системний підхід, що дозволяє розглядати цей сектор як складну багаторівневу систему взаємопов'язаних елементів. Особливість державного управління у сфері безпеки і оборони полягає у необхідності забезпечення максимального рівня захищеності національних інтересів при оптимальному використанні обмежених ресурсів держави [155].

Концептуальні засади оцінки ефективності базуються на розумінні того, що сектор безпеки і оборони являє собою сукупність органів державної влади, збройних сил, правоохоронних органів, розвідувальних служб та інших інститутів, діяльність яких спрямована на захист національних інтересів України. Ефективність управління цим сектором визначається здатністю забезпечити адекватну відповідь на існуючі та потенційні загрози при мінімальних витратах ресурсів та максимальному дотриманні принципів демократичного врядування. Теоретичну основу оцінки ефективності

складають принципи нового державного менеджменту, що передбачають орієнтацію на результат, підзвітність, прозорість та ефективне використання ресурсів. У контексті сектору безпеки і оборони ці принципи мають бути адаптовані з урахуванням специфіки діяльності силових відомств та необхідності дотримання режиму секретності у відповідних сферах [179].

Системний аналіз ефективності механізмів державного управління сектором безпеки і оборони України дозволяє виділити кілька ключових рівнів оцінки. Перший рівень - стратегічний, що включає оцінку відповідності цілей та завдань сектору національним інтересам та стратегічним пріоритетам держави. Другий рівень - тактичний, що передбачає аналіз ефективності конкретних механізмів координації, планування та контролю. Третій рівень - оперативний, що зосереджується на оцінці результативності виконання конкретних функцій та завдань [5].

Особливе значення для оцінки ефективності має аналіз інституційної структури сектору безпеки і оборони України. Центральне місце в цій структурі займає Рада національної безпеки і оборони України як координаційний орган при Президентові України. РНБО здійснює координацію та контроль діяльності органів виконавчої влади у сфері національної безпеки і оборони, що робить її ключовим елементом системи управління сектором [123].

Динаміку оборонних видатків України у 2014–2024 роках наведено на рис. 2.1.

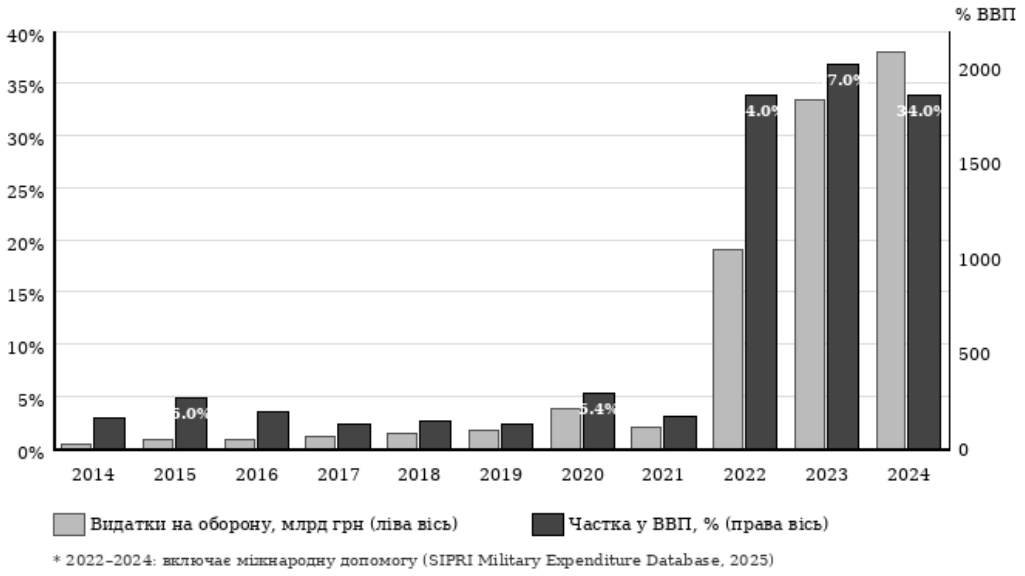

Рис. 2.1. Динаміка оборонних видатків України, 2014–2024 роки

Джерело: складено автором за даними SIPRI Military Expenditure Database (2025) та Міністерства фінансів України

Аналіз функціонування РНБО як координаційного механізму показує як позитивні, так і проблемні аспекти. До позитивних аспектів можна віднести централізацію стратегічного планування у сфері національної безпеки, забезпечення міжвідомчої координації при прийнятті ключових рішень, оперативність реагування на загрози в умовах кризових ситуацій. Водночас існують проблеми, пов'язані з дублюванням функцій між РНБО та профільними міністерствами, недостатньою прозорістю процесів прийняття рішень, обмеженими можливостями парламентського контролю за діяльністю у сфері національної безпеки [7].

Методологічний підхід до оцінки ефективності механізмів державного управління сектором безпеки і оборони має базуватися на системі критеріїв та показників, що дозволяють здійснити комплексний аналіз функціонування всіх елементів системи. Виходячи з специфіки сфери національної безпеки, така система критеріїв має включати як кількісні, так і якісні показники ефективності. Першочерговим критерієм ефективності є здатність системи державного управління забезпечити територіальну цілісність та суверенітет України. Цей критерій відображає фундаментальне призначення сектору

безпеки і оборони та може бути оцінений через аналіз результативності протидії зовнішнім загрозам, ефективності оборонних операцій, рівня контролю над державною територією. В умовах триваючої російської агресії цей критерій набуває особливої актуальності та вимагає постійного моніторингу [81].

Другим важливим критерієм є забезпечення внутрішньої безпеки держави, що включає протидію тероризму, організованій злочинності, корупції у сфері національної безпеки. Ефективність за цим критерієм може бути оцінена через статистичні показники злочинності, рівень розкриття злочинів проти національної безпеки, результативність антитерористичних операцій, ступінь протидії гібридним загрозам [99].

Третім критерієм є ефективність використання бюджетних ресурсів, виділених на потреби національної безпеки і оборони. Цей критерій відображає економічну складову ефективності державного управління та включає аналіз співвідношення витрат та результатів, оптимальності розподілу ресурсів між різними напрямами діяльності, прозорості бюджетного процесу у сфері безпеки і оборони [174].

Четвертим критерієм є дотримання принципів демократичного цивільного контролю над сектором безпеки і оборони. Ефективність за цим критерієм оцінюється через рівень парламентського нагляду, прозорість діяльності силових відомств, дотримання прав людини у процесі забезпечення національної безпеки, розвиток громадянського суспільства у сфері безпекової політики [179].

П'ятим критерієм є адаптивність системи управління до змінюваних умов безпекового середовища. Цей критерій особливо важливий в умовах гібридних загроз та швидко змінюваного характеру викликів національній безпеці. Ефективність оцінюється через швидкість реагування на нові загрози, здатність до інституційних змін, гнучкість у перерозподілі ресурсів [78].

На основі зазначених критеріїв можна сформувати систему показників для оцінки ефективності механізмів державного управління сектором безпеки і оборони України. Ці показники мають бути згруповані за відповідними напрямами оцінки та включати як абсолютні, так і відносні величини. Група показників інституційної ефективності включає показники, що характеризують якість інституційної архітектури сектору безпеки і оборони. До них належать: рівень координації між різними відомствами сектору, швидкість прийняття управлінських рішень, ступінь дублювання функцій між органами управління, якість стратегічного планування, ефективність системи підзвітності та контролю.

Оцінка рівня координації між різними відомствами сектору може здійснюватися через аналіз кількості міжвідомчих робочих груп та комісій, частоти проведення координаційних нарад, рівня узгодженості планових документів різних відомств. Важливим показником є також кількість випадків неузгодженості позицій різних органів сектору з ключових питань національної безпеки. Швидкість прийняття управлінських рішень може оцінюватися через середній час, що витрачається на підготовку та прийняття рішень різних рівнів складності, кількість рівнів погодження управлінських рішень, частоту випадків прострочення термінів прийняття важливих рішень. Особливе значення має аналіз швидкості реагування на кризові ситуації та надзвичайні події [7].

Ступінь дублювання функцій між органами управління може бути оцінений через аналіз розподілу повноважень між різними відомствами, кількість випадків перетину компетенцій, ефективність розмежування відповідальності. Цей показник особливо важливий для оптимізації структури управління та підвищення загальної ефективності системи.

Якість стратегічного планування оцінюється через аналіз повноти та своєчасності розробки стратегічних документів, ступінь їх взаємоузгодженості, рівень деталізації планів та програм, якість системи

моніторингу виконання стратегічних документів. Важливим є також аналіз зв'язку між стратегічним плануванням та бюджетним процесом.

Група показників функціональної ефективності характеризує результативність виконання основних функцій сектору безпеки і оборони. До цієї групи належать показники оборонної спроможності, ефективності протидії загрозам національній безпеці, якості кризового управління, результативності міжнародного співробітництва у сфері безпеки.

Оцінка оборонної спроможності як ключового показника функціональної ефективності включає аналіз готовності Збройних Сил України до виконання завдань за призначенням, рівня технічного оснащення військ, ефективності системи військової освіти та підготовки кадрів. Важливими індикаторами є співвідношення чисельності особового складу до встановлених потреб, рівень укомплектованості підрозділів сучасними зразками озброєння та військової техніки, показники бойової готовності військових частин. В умовах російської агресії особливого значення набувають показники ефективності протидії гібридним загрозам. Ці показники включають результативність інформаційно-психологічних операцій, ефективність протидії кібератакам, якість роботи з виявлення та нейтралізації диверсійно-розвідувальних груп, рівень координації між різними органами у протидії гібридним загрозам. Оцінка цих показників ускладнюються специфічним характером гібридних загроз та необхідністю використання закритої інформації [1].

Якість кризового управління оцінюється через швидкість та адекватність реагування на кризові ситуації, ефективність систем раннього попередження, здатність до мобілізації ресурсів у критичних ситуаціях. Важливими показниками є середній час реагування на надзвичайні ситуації, рівень координації між різними службами під час кризи, ефективність системи інформування населення про загрози та необхідні заходи.

Результативність міжнародного співробітництва у сфері безпеки може бути оцінена через кількість та якість міжнародних угод у сфері безпеки і

оборони, рівень інтеграції з євроатлантичними структурами безпеки, ефективність участі у міжнародних миротворчих операціях, обсяг отриманої міжнародної військово-технічної допомоги. Група показників ресурсної ефективності характеризує оптимальність використання людських, фінансових та матеріальних ресурсів сектору безпеки і оборони. Ці показники включають аналіз структури видатків на національну безпеку і оборону, ефективність системи державного оборонного замовлення, рівень корупційних ризиків у сфері закупівель для потреб безпеки і оборони.

Аналіз структури видатків на національну безпеку і оборону передбачає оцінку співвідношення витрат на утримання особового складу, закупівлю озброєння та військової техніки, будівництво військової інфраструктури, проведення науково-дослідних робіт. Оптимальна структура видатків має забезпечувати баланс між поточними потребами та перспективним розвитком оборонних спроможностей [96].

Ефективність системи державного оборонного замовлення оцінюється через своєчасність виконання контрактів, якість отриманої продукції, рівень цін порівняно з ринковими, ступінь розвитку вітчизняного оборонно-промислового комплексу. Важливими показниками є частка вітчизняної продукції у структурі державного оборонного замовлення, рівень інноваційності закуповуваної продукції, ефективність трансферу технологій. Рівень корупційних ризиків у сфері закупівель для потреб безпеки і оборони може бути оцінений через аналіз прозорості процедур закупівель, кількість порушень законодавства про публічні закупівлі, ефективність системи внутрішнього аудиту та фінансового контролю. Зниження корупційних ризиків є критично важливим для забезпечення ефективного використання бюджетних коштів [164].

Особливого значення у контексті оцінки ефективності механізмів державного управління сектором безпеки і оборони набуває аналіз кадрової політики. Ефективність кадрової політики може бути оцінена через показники плинності кадрів у керівних посадах, рівень професійної

підготовки управлінських кадрів, ефективність системи підвищення кваліфікації, якість кадрового планування та прогнозування потреб у персоналі [32].

Плинність кадрів у керівних посадах характеризує стабільність системи управління та її здатність забезпечити наступність у реалізації довгострокових стратегій. Високий рівень плинності може свідчити про проблеми в системі мотивації, невідповідність посадових окладів ринковим, політизацію кадрових рішень. Водночас надмірна стабільність може призводити до консервації неефективних підходів та зниження інноваційного потенціалу системи. Рівень професійної підготовки управлінських кадрів оцінюється через аналіз освітнього рівня керівників, наявність спеціалізованої підготовки у сфері національної безпеки, досвід роботи на різних посадах системи управління. Важливим показником є також участь керівників у програмах міжнародного обміну досвідом та навчання у провідних закордонних навчальних закладах [1].

Ефективність системи підвищення кваліфікації характеризується регулярністю проведення навчальних заходів, їх відповідністю актуальним потребам системи управління, якістю навчальних програм, рівнем застосування отриманих знань у практичній діяльності. Система підвищення кваліфікації має забезпечувати постійне оновлення знань та навичок управлінського персоналу відповідно до змінюваних викликів у сфері національної безпеки [65].

Якість кадрового планування та прогнозування потреб у персоналі оцінюється через наявність довгострокових кадрових стратегій, точність прогнозування потреб у кадрах різних категорій, ефективність системи добору та відбору кандидатів на керівні посади. Важливим є також аналіз системи оцінки результатів діяльності управлінського персоналу та зв'язку результатів оцінки з кар'єрним просуванням.

Критично важливим аспектом оцінки ефективності механізмів державного управління сектором безпеки і оборони є аналіз системи

стратегічного планування та прогнозування. Ефективна система стратегічного планування має забезпечувати узгодженість між довгостроковими цілями національної безпеки, середньостроковими планами розвитку оборонних спроможностей та короткостроковими оперативними завданнями. Якість стратегічного планування у сфері національної безпеки може бути оцінена через аналіз повноти та обґрунтованості стратегічних документів, їх відповідності міжнародним стандартам та кращим практикам, рівня деталізації цілей та завдань. Важливим показником є також ступінь участі відповідних зацікавлених сторін у процесі розробки стратегічних документів, включаючи представників наукового співтовариства, громадянського суспільства та міжнародних партнерів [83].

Ефективність системи прогнозування загроз національній безпеці характеризується точністю прогнозів, своєчасністю виявлення нових викликів та загроз, якістю аналітичного забезпечення процесів прийняття рішень. Особливого значення набуває здатність системи до прогнозування гібридних загроз, які за своєю природою важко піддаються традиційним методам аналізу та прогнозування [78].

Аналіз функціонування інформаційно-аналітичних систем сектору безпеки і оборони показує як досягнення, так і проблемні аспекти. До досягнень можна віднести створення єдиних інформаційних баз даних, розвиток систем автоматизованого збору та обробки інформації, підвищення рівня координації між різними аналітичними підрозділами. Водночас існують проблеми технічної сумісності різних інформаційних систем, недостатнього рівня захисту інформації, обмеженого використання сучасних методів аналізу великих даних. Особливе місце в оцінці ефективності механізмів державного управління займає аналіз системи цивільного контролю над сектором безпеки і оборони. Ефективність цивільного контролю може бути оцінена через рівень парламентського нагляду за діяльністю силових відомств, якість громадського контролю, прозорість процедур прийняття рішень у сфері національної безпеки [11].

Рівень парламентського нагляду характеризується регулярністю розгляду питань національної безпеки у профільних комітетах Верховної Ради України, якістю парламентських слухань з питань оборони та безпеки, ефективністю контролю за використанням бюджетних коштів на потреби національної безпеки. Важливим показником є також рівень експертизи депутатського корпусу з питань національної безпеки та оборони.

Якість громадського контролю оцінюється через активність громадських організацій у сфері безпекової політики, рівень їх професійної компетентності, ступінь впливу на процеси прийняття рішень. Розвиток громадянського суспільства у сфері безпекової політики є важливим індикатором демократизації сектору безпеки і оборони та підвищення рівня довіри суспільства до силових відомств. Прозорість процедур прийняття рішень у сфері національної безпеки має балансувати між необхідністю забезпечення секретності критично важливої інформації та потребою суспільства в інформованості про основні напрями безпекової політики держави. Ефективна система має забезпечувати максимальну можливу прозорість при збереженні необхідного рівня секретності [41].

Методологічно важливим аспектом оцінки ефективності є використання порівняльного аналізу з міжнародними стандартами та кращими практиками. Такий аналіз дозволяє виявити сильні та слабкі сторони вітчизняної системи управління, визначити пріоритетні напрями реформування, скористатися досвідом інших країн у вирішенні аналогічних проблем. Порівняльний аналіз має враховувати специфічні умови функціонування України, включаючи географічне положення, історичний досвід, рівень економічного розвитку, особливості політичної системи. Механічне копіювання досвіду інших країн без урахування національної специфіки може призвести до зниження ефективності системи управління [11].

Важливим елементом порівняльного аналізу є оцінка відповідності вітчизняної системи управління сектором безпеки і оборони стандартам

НАТО та ЄС. Така оцінка особливо актуальна в контексті євроатлантичних прагнень України та процесу інтеграції до західних структур безпеки. Основними критеріями відповідності є демократичний цивільний контроль, прозорість та підзвітність, професіоналізм, дотримання прав людини. Комплексна оцінка ефективності механізмів державного управління сектором безпеки і оборони має базуватися на інтегральній системі показників, що дозволяють отримати об'єктивну картину стану системи управління. Така система має включати як кількісні показники, що піддаються точному вимірюванню, так і якісні показники, оцінка яких здійснюється експертними методами.

Для забезпечення об'єктивності оцінки доцільно використовувати метод експертних оцінок з залученням широкого кола фахівців у сфері національної безпеки, державного управління, військової справи. Експертна група має включати як представників органів державної влади, так і незалежних експертів з наукових установ, аналітичних центрів, громадських організацій. Методологічною основою інтегральної оцінки може стати метод модифікованої ранжированої бальної оцінки, який дозволяє поєднати різнорідні показники в єдину систему оцінки. При цьому кожен показник отримує певну вагу залежно від його важливості для загальної ефективності системи управління [87].

Процедура інтегральної оцінки ефективності передбачає розрахунок бальних оцінок для кожного показника з подальшим їх агрегуванням у комплексний індекс ефективності. При цьому на першому етапі здійснюється ранжування за кожним показником з присвоєнням відповідних балів. На другому етапі виробляється зважування показників відповідно до їх значущості. На третьому етапі розраховується інтегральна оцінка як середньозважена сума балів за всіма показниками.

Результати комплексної оцінки дозволяють класифікувати рівень ефективності механізмів державного управління сектором безпеки і оборони за наступною шкалою: високий рівень ефективності (більше 80 балів), рівень

вище середнього (60-80 балів), середній рівень (40-60 балів), рівень нижче середнього (20-40 балів), низький рівень (менше 20 балів). Аналіз поточного стану ефективності механізмів державного управління сектором безпеки і оборони України, проведений на основі запропонованої методології, свідчить про наявність як позитивних тенденцій, так і серйозних проблем, що потребують невідкладного вирішення. До позитивних тенденцій слід віднести підвищення рівня координації між різними відомствами сектору в умовах протидії російській агресії, зміцнення системи цивільного контролю, розвиток міжнародного співробітництва у сфері безпеки і оборони [43].

Водночас залишаються актуальними проблеми дублювання функцій між окремими органами управління, недосконалості системи стратегічного планування, обмеженості ресурсного забезпечення, недостатньої прозорості окремих процедур прийняття рішень. Особливо гостро стоїть питання оптимізації структури управління сектором з метою усунення зайвих ланок та підвищення оперативності прийняття рішень.

Критичним аспектом є ефективність використання бюджетних ресурсів, виділених на потреби національної безпеки і оборони. Аналіз показує, що, незважаючи на зростання обсягів фінансування, існують резерви підвищення ефективності витрачання коштів через оптимізацію структури видатків, впровадження сучасних технологій закупівель, посилення контролю за цільовим використанням коштів. Особливої уваги потребує розвиток системи моніторингу та оцінки ефективності діяльності сектору безпеки і оборони. Ефективна система моніторингу має забезпечувати постійне відстеження ключових показників ефективності, своєчасне виявлення негативних тенденцій, формування рекомендацій щодо корегування управлінських рішень. Важливим елементом такої системи є регулярне проведення аудиту ефективності з залученням незалежних експертів [158].

Перспективні напрями підвищення ефективності механізмів державного управління сектором безпеки і оборони включають цифровізацію

процесів управління, розвиток аналітичних спроможностей, впровадження міжнародних стандартів якості управління, посилення інституційної спроможності органів сектору. Цифровізація має забезпечити автоматизацію рутинних процесів, підвищення швидкості обробки інформації, покращення координації між різними рівнями управління. Розвиток аналітичних спроможностей передбачає створення потужних аналітичних центрів, підготовку висококваліфікованих аналітиків, впровадження сучасних методів аналізу даних, включаючи технології штучного інтелекту та машинного навчання. Це дозволить підвищити якість прогнозування загроз, покращити обґрунтованість управлінських рішень, забезпечити більш ефективне використання наявної інформації [6].

Впровадження міжнародних стандартів якості управління, зокрема стандартів НАТО та ЄС, сприятиме підвищенню професійного рівня управлінських кадрів, покращенню процедур прийняття рішень, посиленню системи контролю якості. Важливим аспектом є адаптація цих стандартів до специфічних умов України з урахуванням національних особливостей та пріоритетів. Посилення інституційної спроможності органів сектору передбачає розвиток людських ресурсів, модернізацію матеріально-технічної бази, вдосконалення організаційних структур, створення ефективних систем мотивації персоналу. Особлива увага має приділятися підготовці управлінських кадрів вищої ланки, здатних ефективно керувати в умовах сучасних викликів національній безпеці [1].

Таким чином, комплексна оцінка ефективності існуючих механізмів державного управління сектором безпеки і оборони України засвідчує наявність значного потенціалу для підвищення якості управління при одночасному існуванні серйозних викликів, що потребують системного підходу до їх вирішення. Подальший розвиток системи управління має базуватися на науково обґрунтованих підходах, урахуванні кращого міжнародного досвіду та специфіки національних умов функціонування сектору безпеки і оборони України [13].

2.2. Аналіз інституційних та нормативно-правових засад реформування сектору безпеки і оборони

Формування сучасної інституційної архітектури сектору безпеки і оборони України відбувалось у контексті складних трансформаційних процесів, зумовлених здобуттям незалежності, змінами геополітичної ситуації та необхідністю адаптації до сучасних викликів і загроз. Аналіз європейського досвіду, зокрема еволюції правових основ Спільної політики безпеки та оборони Європейського Союзу, дозволяє виявити закономірності інституційного розвитку та визначити перспективи вдосконалення українських механізмів державного управління [160].

Початковий етап формування інституційної структури сектору безпеки і оборони України характеризувався адаптацією радянських управлінських моделей до нових політико-правових реалій. Конституція України 1996 року заклала фундаментальні засади розподілу повноважень у сфері національної безпеки, визначивши Президента України як гаранта державної незалежності, територіальної цілісності і національної безпеки. Водночас була створена система органів, покликаних забезпечувати координацію діяльності у сфері національної безпеки, ключовим елементом якої стала Рада національної безпеки і оборони України [179].

Інституційна еволюція сектору безпеки і оборони України демонструє певні паралелі з розвитком європейських інтеграційних механізмів у сфері безпеки. Як і у випадку Європейського Союзу, де формування Спільної зовнішньої політики та політики безпеки відбувалось поетапно, починаючи з Маастрихтського договору 1992 року, українська система також пройшла кілька ключових етапів реформування. Особливо значущими стали зміни після 2014 року, коли російська агресія актуалізувала питання ефективності управлінських механізмів та їх адаптації до гібридних загроз [24].

Аналіз європейського досвіду показує, що ефективність інституційних механізмів у сфері безпеки та оборони значною мірою залежить від чіткого

розподілу повноважень та налагодженої координації між різними органами влади. У Європейському Союзі цей процес супроводжувався створенням спеціалізованих структур, таких як Комітет з питань політики та безпеки, Військовий комітет та Військовий штаб ЄС. В Україні подібну роль покликані відігравати Рада національної безпеки і оборони, Генеральний штаб Збройних Сил України та інші профільні структури [34].

Структуру суб'єктів сектору безпеки і оборони України відповідно до Закону України «Про національну безпеку України» показано на рис. 2.2.

Рис. 2.2. Суб'єкти сектору безпеки і оборони України

Джерело: складено відповідно до Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII

Трансформація інституційної архітектури сектору безпеки і оборони України після 2014 року відображає прагнення до наближення до євроатлантичних стандартів управління. Реформування Міністерства оборони України, створення нових структур у складі Збройних Сил, модернізація Служби безпеки України та інших силових відомств спрямовувались на підвищення ефективності управління та забезпечення демократичного цивільного контролю над сектором безпеки і оборони. Водночас досвід Європейського Союзу демонструє важливість поступового розвитку інституційних механізмів, враховуючи національні особливості та геополітичний контекст [158].

Особливістю української моделі управління сектором безпеки і оборони є центральна роль Президента України у формуванні та реалізації політики національної безпеки. Ця специфіка відрізняє українську систему від європейських моделей, де процеси прийняття рішень характеризуються більш колегіальним характером. Водночас поконституційні зміни 2019 року, що закріпили стратегічний курс України на набуття повноправного членства у Європейському Союзі та Північноатлантичному альянсі, створили правові передумови для поглиблення інституційних реформ у напрямі євроатлантичної інтеграції [75].

Формування ефективної нормативно-правової бази управління сектором безпеки і оборони є критично важливим завданням для забезпечення національної безпеки держави. Аналіз європейського досвіду правового регулювання, зокрема еволюції правових основ Спільної політики безпеки та оборони ЄС від Маастрихтського договору до Лісабонського договору, дозволяє виявити ключові принципи побудови комплексної системи правового регулювання сектору безпеки і оборони [156].

Конституційні засади управління сектором безпеки і оборони України закладені у статтях 17, 18, 85, 102, 106, 107 Основного Закону, які визначають основні принципи забезпечення національної безпеки, суверенітету і територіальної цілісності держави. Особливе значення має стаття 85 Конституції, яка визначає повноваження Верховної Ради України у сфері національної безпеки, зокрема щодо визначення засад внутрішньої і зовнішньої політики, затвердження Державного бюджету України та контролю за його виконанням. Водночас стаття 106 встановлює повноваження Президента України як гаранта державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина [33].

Розвиток українського законодавства у сфері національної безпеки демонструє поступове наближення до європейських стандартів правового регулювання. Прийняття Закону України "Про національну безпеку України"

(2018 рік) стало важливим кроком у систематизації правових норм та визначенні сучасної архітектури сектору безпеки і оборони. Цей законодавчий акт встановив правові та організаційні засади, основні напрями і порядок забезпечення національної безпеки України, повноваження державних органів, підприємств, установ, організацій, права та обов'язки громадян у цій сфері. Аналіз європейського досвіду показує важливість чіткого розмежування компетенції різних органів влади у сфері безпеки та оборони. У Європейському Союзі цей принцип реалізується через систему "опор", де питання Спільної зовнішньої політики та політики безпеки регулюються окремими правовими механізмами, що відрізняються від наднаціональних методів регулювання економічної інтеграції. В Україні подібне розмежування здійснюється через систему спеціальних законів у сфері національної безпеки, оборони, діяльності розвідувальних органів та правоохоронних структур [114].

Законодавче забезпечення демократичного цивільного контролю над сектором безпеки і оборони є одним з ключових елементів євроатлантичної системи управління. В Україні цей принцип закріплений у Законі України "Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави" та конкретизується у профільних законах про Збройні Сили України, Службу безпеки України, Національну гвардію України та інші структури сектору безпеки і оборони. Водночас практична реалізація цих механізмів потребує постійного вдосконалення з урахуванням викликів гібридної війни та необхідності забезпечення ефективності управління в умовах збройної агресії [126].

Особливою характеристикою української нормативно-правової бази є її адаптація до умов гібридних загроз та російської агресії. Прийняття законів про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях, про правовий режим воєнного стану, про особливий порядок місцевого самоврядування в окремих районах Донецької та Луганської областей відображає специфіку правового

регулювання у кризових умовах. Ці законодавчі ініціативи не мають аналогів у європейському досвіді, оскільки ЄС не стикався з подібними викликами територіальної цілісності [121].

Процес адаптації українського законодавства до європейських стандартів у сфері безпеки та оборони відбувається з урахуванням складного еволюційного шляху формування правових основ Спільної політики безпеки та оборони Європейського Союзу. Досвід ЄС демонструє важливість поступового розвитку правових механізмів, що враховують специфіку міждержавного співробітництва у чутливій сфері національної безпеки та суверенітету держав-членів [31].

Аналіз Лісабонського договору 2007 року, який суттєво реформував правове регулювання Спільної політики безпеки та оборони ЄС, розкриває принципові підходи до інституційного будівництва у сфері безпеки. Введення посади Високого представника Союзу з питань зовнішньої політики та політики безпеки, який одночасно є віце-президентом Європейської комісії, демонструє тенденцію до консолідації управління зовнішньополітичною діяльністю. Для України цей досвід актуальний в контексті необхідності посилення координації між різними органами сектору безпеки і оборони та подолання міжвідомчих протиріч. Принцип "конструктивного утримання", закріплений у правовому регулюванні СПБО ЄС, який дозволяє державам-членам не брати участь у конкретних операціях, не блокуючи при цьому рішень решти учасників, може бути адаптований до українських реалій у контексті розробки гнучких механізмів залучення різних структур сектору безпеки до реалізації конкретних завдань. Особливо це актуально для операцій, що потребують міжвідомчої координації, коли не всі структури мають необхідні ресурси або повноваження для повноцінної участі [75].

Європейська модель цивільного управління кризами, що включає поліцейські місії, місії з питань правосуддя та цивільної адміністрації, місії з цивільного захисту та спостережні місії, надає важливі орієнтири для

розвитку української системи реагування на кризові ситуації. Створення в Україні Державної служби України з надзвичайних ситуацій, реформування системи цивільного захисту та розвиток спроможностей у сфері кібербезпеки відображають імплементацію європейських підходів з урахуванням специфіки гібридних загроз.

Механізми фінансування операцій у сфері безпеки та оборони, зокрема досвід функціонування механізму "Athena" в Європейському Союзі, демонструють важливість створення прозорих та ефективних систем управління ресурсами. В Україні подібні принципи знайшли відображення у реформуванні системи оборонного планування, запровадженні програмно-цільового методу у сфері національної безпеки та створенні Фонду національної безпеки та оборони як спеціального механізму фінансування пріоритетних проектів [141].

Правове регулювання участі третіх країн в операціях ЄС, зокрема укладання рамкових угод про участь з Норвегією, Ісландією, Канадою, Україною та іншими країнами, ілюструє важливість формування правових основ міжнародного співробітництва у сфері безпеки. Для України, яка активно розвиває партнерські відносини з країнами НАТО та ЄС, цей досвід є особливо цінним у контексті розробки правових механізмів участі в міжнародних місіях та операціях з підтримання миру. Інституціоналізація стратегічного планування у сфері безпеки, що відображена в Європейській стратегії безпеки та подальших концептуальних документах ЄС, підкреслює необхідність системного підходу до формування політики безпеки. В Україні це знайшло втілення у розробці Стратегії національної безпеки, Стратегії кібербезпеки, Воєнної доктрини та інших стратегічних документів, які формують комплексну систему планування у сфері національної безпеки [24].

Трансформація інституційних механізмів управління сектором безпеки і оборони України після 2014 року відбувалася під впливом двох ключових факторів: необхідності ефективного протистояння російській агресії та

прагнення до євроатлантичної інтеграції. Аналіз цих процесів у порівнянні з еволюцією інституційної архітектури Європейського Союзу у сфері безпеки дозволяє виявити як спільні закономірності, так і унікальні особливості української моделі реформування [112].

Реформування Міністерства оборони України, яке включало відокремлення політико-стратегічного та військово-оперативного рівнів управління, запровадження сучасних методів стратегічного планування та створення ефективної системи логістичного забезпечення, демонструє адаптацію кращих практик країн НАТО до українських реалій. Подібно до того, як у Європейському Союзі формувалися спеціалізовані структури для координації військової політики, в Україні було створено Головне управління оборонного планування та політики безпеки, яке відповідає за стратегічне планування у сфері оборони [164].

Особливого значення набула реформа системи військового управління, що передбачала створення об'єднаних сил та запровадження принципів об'єднаного планування і управління операціями. Ця трансформація відображає імплементацію досвіду НАТО щодо інтегрованого підходу до управління силами, водночас враховуючи специфіку гібридної війни та необхідності забезпечення ефективної взаємодії між різними видами та родами військ в умовах асиметричних загроз. Модернізація Служби безпеки України, що включала демілітаризацію, деполітизацію та звуження функцій до питань контррозвідки, боротьби з тероризмом та захисту державної таємниці, демонструє адаптацію європейських стандартів функціонування спецслужб до українського контексту. Створення Державного бюро розслідувань як незалежного правоохоронного органу відображає європейський підхід до спеціалізації правоохоронних структур та забезпечення їх професійності і незалежності [83].

Інституціоналізація кібербезпеки через створення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України та Державної служби спеціального зв'язку та захисту

інформації демонструє розуміння важливості комплексного підходу до протидії кіберзагрозам. Цей досвід корелює з європейськими ініціативами у сфері кібербезпеки, зокрема створенням Європейського агентства з кібербезпеки та розробкою стратегії кібербезпеки ЄС [62].

Розвиток системи стратегічних комунікацій, що включає створення відповідних підрозділів у структурі органів сектору безпеки і оборони, відображає адаптацію досвіду протидії інформаційним загрозам. Європейський Союз розробив подібні механізми для протидії дезінформації та зовнішньому інформаційному втручанню, що знайшло відображення у створенні групи стратегічних комунікацій East StratCom Task Force [139].

Реформування системи цивільного контролю включало посилення ролі парламентського нагляду, створення інституту цивільних керівників у військових відомствах та запровадження механізмів громадського контролю. Ці зміни відповідають європейським принципам демократичного управління сектором безпеки, водночас враховуючи необхідність збереження ефективності управління в умовах активних бойових дій.

Трансформація системи військової освіти та професійної підготовки кадрів, що включала створення Національного університету оборони України, запровадження євроатлантичних стандартів військової освіти та розвиток партнерських відносин з провідними військовими навчальними закладами країн НАТО, демонструє системний підхід до модернізації кадрового потенціалу сектору безпеки і оборони [32].

Координація діяльності органів сектору безпеки і оборони залишається одним з найбільш складних завдань державного управління, що потребує збалансування принципів ефективності, законності та демократичного контролю. Досвід Європейського Союзу у формуванні координаційних механізмів демонструє важливість створення чітких процедур взаємодії між різними інституціями при збереженні їх функціональної автономії. Водночас українська практика виявляє специфічні проблеми координації, зумовлені особливостями правової системи та викликами гібридної війни [75].

Ключовою проблемою координації в Україні є недостатня чіткість розподілу повноважень між органами сектору безпеки і оборони у питаннях протидії гібридним загрозам. На відміну від традиційних військових загроз, гібридні загрози часто виходять за межі компетенції будь-якого окремого органу, потребуючи координованої відповіді різних структур. Європейський досвід показує важливість створення спеціалізованих координаційних механізмів, подібних до Комітету з питань політики та безпеки ЄС, який забезпечує координацію на політичному рівні [160].

Проблема дублювання функцій між різними органами сектору безпеки і оборони потребує системного вирішення через чітке законодавче розмежування компетенції. Аналіз європейського досвіду показує, що ефективність координації залежить не стільки від кількості координаційних структур, скільки від якості правового регулювання їх взаємодії. Рада національної безпеки і оборони України як координаційний орган потребує посилення інструментальних можливостей для забезпечення виконання своїх рішень усіма органами сектору. Інформаційне забезпечення координації залишається слабким місцем української системи управління сектором безпеки і оборони. Відсутність єдиної інформаційно-аналітичної системи, яка б забезпечувала обмін інформацією між різними органами в режимі реального часу, знижує ефективність реагування на загрози. Європейський досвід створення Центру оцінки ситуацій ЄС (EU Situation Centre) демонструє важливість централізованої аналітичної підтримки прийняття рішень у сфері безпеки [148].

Перспективи розвитку інституційної архітектури сектору безпеки і оборони України визначаються декількома ключовими тенденціями. По-перше, необхідність адаптації до викликів четвертої промислової революції, включаючи кіберзагрози , використання штучного інтелекту та інших новітніх технологій у сфері безпеки. По-друге, поглиблення євроатлантичної інтеграції потребує подальшого наближення українських інституцій до стандартів НАТО та ЄС. По-третє, досвід гібридної війни актуалізує

необхідність розвитку міжсекторального підходу до забезпечення національної безпеки [58].

Розвиток публічно-приватного партнерства у сфері безпеки та оборони відкриває нові можливості для підвищення ефективності управління при збереженні державного контролю над критично важливими функціями. Європейський досвід створення Європейського оборонного агентства та розвитку спільних програм у сфері оборонних технологій може бути адаптований до українських умов через створення відповідних інституційних механізмів підтримки інновацій у сфері безпеки. Перспективним напрямом інституційного розвитку є створення регіональних координаційних центрів, які б забезпечували ефективну взаємодію центральних органів влади з місцевими структурами в питаннях забезпечення безпеки. Досвід ЄС у розвитку регіональних механізмів співробітництва у сфері безпеки може надати корисні орієнтири для формування таких структур в Україні [163].

Стратегічною перспективою є формування інтегрованої системи управління національною безпекою, яка б поєднувала традиційні механізми державного управління з інноваційними підходами, включаючи використання великих даних, штучного інтелекту та інших технологій для підтримки прийняття рішень. Реалізація цієї перспективи потребує не лише технологічної модернізації, але й глибокого реформування правових та інституційних основ управління сектором безпеки і оборони з урахуванням кращих європейських практик та специфіки українського контексту [145].

2.3. Індикативний підхід до оцінки ризиків національній безпеці України: методичні аспекти

Розвиток сучасних підходів до оцінки ризиків національної безпеки в умовах зростання глобальної турбулентності та появи нових типів загроз актуалізує необхідність переходу від традиційних експертно-аналітичних

методів до більш формалізованих і точних інструментів прогнозування. Пандемія COVID-19, гібридні конфлікти, кіберзагрози та інші виклики XXI століття продемонстрували обмеженість класичних підходів до аналізу безпекових ризиків, заснованих переважно на якісних оцінках та експертних судженнях. У цьому контексті індикативний підхід до оцінки ризиків національної безпеки набуває особливого значення як методологічна основа для формування системи "упереджаючого державного управління" [151].

Концептуальним підґрунтям індикативного підходу є теорія "упереджаючого державного управління", що формувалася протягом останніх двох десятиліть в академічній літературі та впроваджувалася на практиці розвідувальним співтовариством США та НАТО. Ця теорія базується на деліберaційному методі ранжування ризиків, коли ступінь ризику визначає орієнтири стратегічного планування. Водночас недостатньо комплексного узагальнення наукової літератури з цього питання, що могло б бути доповнено окремими українськими розробками індикативних інструментів оцінки якості державного управління.

Методологічною основою індикативного підходу є інструментальна парадигма державного управління, в якій процес прийняття рішень базується на отриманні даних, їх статистичній обробці та аналізі результатів обробки. Дана методологія може бути використана стосовно сфери національної безпеки держави з урахуванням можливості виникнення непередбачених ризиків і загроз, які можуть латентно розвиватися в рамках уже існуючих трендів. Розвиток індикативних оцінок дозволяє вибудувати систему " упереджаючого управління" як сукупність оцінок, що в практичному плані допоможе поліпшити взаємодію між верхніми і нижніми рівнями індикаторів та показників [167].

Теоретичні підходи до оцінки ризиків у контексті національної безпеки можна умовно розділити на чотири основні напрями. Перший складають роботи, які в рамках системно-логічного аналізу сформувалися під впливом публікацій дослідників з Університету Карнегі-Меллон, що використовують деліберaційний метод ранжування ризиків. Другим етапом еволюції цього

методу стали розробки американської корпорації RAND та створені під її впливом підходи до оцінки , які багато в чому стали основоположними для вибудовування відповідних методологій органами виконавчої влади США та Великобританії [69].

Третю частину підходів з проблем оцінки ризиків складають окремі розрізнені роботи на основі верифікаційного методу дослідження, які застосовують переважно кількісні методи до оцінки складових частин національної безпеки держави. Четверта група досліджень стосується використання "упереджаючих" механізмів у прогнозуванні ризиків наукових розробок та нових інноваційних технологій, включаючи концепції "адаптивного" управління та "упереджаючої" демократії [47].

Індикативний підхід до державного управління визначається як вивчення функціонування систем державного управління за допомогою об'єктивних даних, розподілених за індикаторами і агрегованих у показниках та індексах. Індикативна оцінка ризиків національної безпеки є однією зі сфер застосування даного підходу і полягає в комплексній оцінці стану захищеності держави за сукупністю груп індикаторів і показників. Цей підхід еволюціонував з часом, враховуючи потреби і можливості в області управління ризиками та прогнозування, пройшовши шлях від простих індикаторів до інтегрованих моделей та використання технологій великих даних [174].

Аналіз світового досвіду застосування індикативних підходів до оцінки ризиків національної безпеки демонструє різноманітність методологічних підходів та інституційних рішень, які відображають специфіку геополітичного становища, рівня розвитку аналітичних спроможностей та характеру загроз, з якими стикаються різні держави [51].

Досвід Сполучених Штатів Америки в галузі оцінки ризиків національної безпеки характеризується найбільш розвиненою системою інституційного забезпечення та методологічного супроводу. Розвідувальне співтовариство США відіграє вирішальну роль в оцінці ризиків національної безпеки, збираючи, аналізуючи і синтезуючи розвідувальні дані з різних

джерел для забезпечення всебічної оцінки загроз і ризиків. Ключовими методами оцінки є сценарний аналіз, що включає розробку гіпотетичних сценаріїв для оцінки потенційних ризиків та їх можливого впливу на національну безпеку, і ризик-орієнтований підхід, який передбачає ідентифікацію, оцінку та пріоритизацію ризиків на основі їх імовірності та потенційного впливу [73].

Міністерство внутрішньої безпеки США як основний розробник методологічних підходів до оцінки ризики зазвичай розглядає наслідки з точки зору втрачених життів або економічного збитку, рідко враховуючи ширший спектр факторів. Комітет Національної академії наук США в 2010 році рекомендував не використовувати інтегровані кількісні оцінки ризиків через неоднорідність ризиків та складність побудови інтегрованої моделі. Водночас американська система передбачає постійний моніторинг і оцінку ризиків національної безпеки для відповідної адаптації стратегій і політики, включаючи регулярне оновлення і перегляд оцінок ризиків на основі нових загроз, технологічних досягнень і геополітичних подій [74].

Європейський Союз працює на основі спільного підходу до оцінки ризиків національної безпеки, що включає різні методології, структури та пріоритети. Оцінка ризиків в ЄС передбачає співробітництво між державами-членами, установами та агентствами, включаючи обмін інформацією, спільний аналіз і об'єднання досвіду для оцінки спільних проблем безпеки . Система оцінки ризиків на рівні ЄС використовує сценарний аналіз для вивчення потенційних загроз безпеки і вразливостей, розробляючи сценарії для оцінки впливу різних подій на ЄС та його держави-члени [4].

Європейський Союз підтримав ідею проведення комплексних національних оцінок ризиків в рамках своєї діяльності в області внутрішньої безпеки. У 2010 році Європейська комісія опублікувала загальні керівні принципи проведення національних оцінок ризиків у сфері управління кризами та стихійними лихами. До 2014 року Комісія представила перший огляд природних і антропогенних ризиків, що був заснований на відповідних національних внесках. Національна оцінка ризиків в ЄС на сьогоднішній

момент враховує від 50 до 100 сценаріїв середньо- та довгострокового характеру.

Особливий інтерес представляє китайський досвід оцінки ризиків національної безпеки, який нерозривно пов'язаний з оцінками "комплексної потужності" держави. Ці оцінки здійснюються китайськими вченими з кінця 1980-х років і багато в чому мають у своїй методологічній основі роботи західних політологів. Китайські методики оцінки комплексної потужності інтегрували у свій кількісний апарат у якості зважених показників не тільки статистичні індикатори і показники, але й досить гнучкі експертні оцінки. У перших оцінках комплексної потужності держави враховувались наступні параметри: технології, трудові ресурси, капітал, інформація, природні ресурси, військова потужність, ВВП, дипломатія та контрольно-регулятивна потужність уряду [42].

Загальною тенденцією міжнародного досвіду є перехід від систем національної безпеки, орієнтованих на військові аспекти, до більш широких концепцій управління ризиками і загрозами всіх рівнів. Систематичне управління ризиками зарекомендувало себе як стандарт для сучасних суспільств, які прагнуть передбачити і мінімізувати потенційно руйнівні небезпеки та інциденти. Концепція "стійкості" була додана як нова концепція, яка може стати глобальним метанаративом управління безпекою [51].

Формування ефективної системи індикаторів для оцінки ризиків національної безпеки України вимагає врахування як універсальних підходів до класифікації загроз, так і специфічних викликів, з якими стикається українська держава в умовах гібридної війни та прагнення до євроатлантичної інтеграції. Індикативний підхід до оцінки ризиків національної безпеки передбачає використання визначених індикаторів або показників, які можуть вказувати на можливі ризики або потенційні загрози [33].

Систему індикаторів оцінки ризиків і загроз національній безпеці України наведено в табл. 2.1.

Таблиця 2.1

Система індикаторів оцінки ризиків і загроз національній безпеці України

Сфера безпеки	Ключові індикатори	Порогові значення (рівні загрози)	Джерела даних
Воєнна	Інтенсивність бойових дій; втрати особового складу та техніки; просування лінії фронту	Низький — локальні сутички; Середній — активізація по всьому периметру; Високий — прорив оборони; Критичний — загроза великих населених пунктів	Генштаб ЗСУ; МО України; РНБО
Кібернетична	Кількість кібератак на держоргани та КІ; рівень захищеності державних мереж; час відновлення після інцидентів	Низький — поодинокі атаки; Середній — серійні атаки на держоргани; Високий — порушення роботи КІ; Критичний — масштабні збої державних систем	ДССЗЗІ; CERT-UA; СБУ
Інформаційна	Охоплення деструктивного контенту; рівень довіри до держінститутів; індекс інформаційної стійкості суспільства	Низький — локальні дезінформаційні кампанії; Середній — цільові кампанії впливу; Високий — підрив суспільної довіри; Критичний — дестабілізація громадської думки	МІП; СБУ; незалежні медіамонітори
Економічна	Падіння ВВП; рівень інфляції; стан золотовалютних резервів	Низький — зниження ВВП до 5%; Середній — 5–15%; Високий — 15–30%; Критичний — понад 30% або дефолт	НБУ; Мінфін; Держстат
Енергетична	Ступінь пошкодження енергоінфраструктури; рівень генерації електроенергії; запаси палива	Низький — поодинокі пошкодження, компенсація мережею; Середній — часткові відключення; Високий — системні перебої; Критичний — масштабний блекаут	Укренерго; Міненерго; НКРЕКП
Внутрішньо-політична	Рівень соціальної напруженості; показники довіри до влади; індекс політичної стабільності	Низький — поодинокі протести; Середній — зростання незадоволення; Високий — масові заворушення; Критичний — загроза конституційному ладу	КМІС; Центр Разумкова; РНБО

Джерело: розроблено автором

Базову систему індикаторів для оцінки ризиків національної безпеки доцільно структурувати за основними категоріями загроз. Мілітарні індикатори включають військовий бюджет як обсяг фінансування збройних сил, чисельність збройних сил та кількість активних військовослужбовців і військової техніки, арсенал спеціальних видів озброєння, військові операції і активність збройних сил у конфліктах. Економічні індикатори охоплюють валютний обмін та інфляцію як стабільність фінансової системи, зовнішньоторговельний баланс і стан торговельних відносин з іншими країнами, зростання ВВП, рівень зайнятості та безробіття.

Соціальні індикатори включають демографічні показники, рівень освіти та доступ до освіти, рівень бідності і нерівності, стан охорони здоров'я і доступ до медичних послуг. Політичні індикатори характеризують політичну стабільність, рівень корупції в уряді та суспільстві, стан громадянських прав і свобод. Особливе значення в сучасних умовах мають індикатори кібербезпеки, що включають кількість та характер кібератак і інцидентів, рівень кіберзахисту та ефективність заходів із захисту інформаційних систем. Екологічні індикатори відображають екологічні катастрофи, рівень забруднення навколишнього середовища, вплив зміни клімату на безпеку. Кримінальні індикатори характеризують рівень злочинності в країні та діяльність організованих злочинних угруповань. Для України особливого значення набувають індикатори, пов'язані з гібридними загрозами, включаючи інформаційні операції, втручання у внутрішні справи, підривну діяльність та спроби дестабілізації суспільно- політичної ситуації [89].

Індикативний підхід до застосування цих індикаторів при аналізі національної безпеки України передбачає постійний збір і обробку масивів даних, що відносяться до цих індикаторів, ранжування отримуваних індексів за кожним з індикаторів, усунення дублювання за допомогою кореляційного аналізу ранжувань , виявлення трендів і встановлення коридорів допустимої

динаміки, фіксування настання ризиків і загроз національній безпеці у випадках виходу за межі коридорів.

Система індикаторів національної безпеки України повинна враховувати специфічні виклики, пов'язані з російською агресією та анексією частини території. Це вимагає розробки спеціальних індикаторів для оцінки стану тимчасово окупованих територій, ефективності політики реінтеграції, впливу вимушеного переміщення населення на соціально-економічний розвиток регіонів. Важливими є індикатори, що характеризують прогрес у сфері європейської та євроатлантичної інтеграції, включаючи виконання критеріїв членства в НАТО та ЄС. Індикатори мають бути конкретними, вимірюваними, досяжними, релевантними і пов'язаними з часовими рамками відповідно до критеріїв SMART. Для кожного обраного індикатора фіксуються початкові базові значення, що дозволяє мати точку відліку для вимірювання прогресу, визначаються цільові значення, пов'язані з кінцевими результатами, здійснюється регулярний моніторинг і вимірювання з аналізом та інтерпретацією отриманих даних. У разі невідповідності очікуваним результатам стратегія може бути скоригована, включаючи перегляд цілей, тактики, ресурсів або термінів [19].

Особливістю системи індикаторів для оцінки національної безпеки України є необхідність врахування фактору часу та динаміки загроз. Гібридний характер сучасних викликів вимагає розробки індикаторів раннього попередження, здатних виявляти латентні загрози на ранніх стадіях їх розвитку. Система повинна бути гнучкою і адаптивною, здатною швидко реагувати на появу нових типів загроз та змінювати пріоритети відповідно до еволюції безпекового середовища.

Ефективна система оцінки ризиків національної безпеки вимагає комплексного підходу, що поєднує кількісні та якісні методи аналізу. Методологічна база такої системи повинна забезпечувати можливість

оперативного реагування на зміни в безпековому середовищі та надавати достовірну інформацію для прийняття обґрунтованих управлінських рішень.

Кількісні методи оцінки ризиків національної безпеки базуються на статистичному аналізі великих масивів даних та математичному моделюванні. Основою цього підходу є створення системи показників, що дозволяють вимірювати та порівнювати рівні ризиків у динаміці. Методологія передбачає розробку інтегральних індексів безпеки, що агрегують інформацію з різних сфер та дозволяють отримати узагальнену оцінку стану національної безпеки. При цьому використовуються методи кореляційно-регресійного аналізу для виявлення взаємозв'язків між різними факторами ризику та їх впливу на загальний рівень безпеки держави.

Особливу увагу у кількісному аналізі приділяється аналізу часових рядів для виявлення трендів та циклічних коливань у динаміці показників безпеки. Використання методів прогнозування дозволяє екстраполювати виявлені тенденції на майбутнє та розробляти сценарії можливого розвитку ситуації. Статистичні методи класифікації та кластерного аналізу сприяють групуванню ризиків за ступенем їх важливості та можливими наслідками. Якісні методи оцінки ризиків включають експертний аналіз, сценарне планування та деліберaційні процедури. Експертна оцінка передбачає залучення фахівців різних галузей для аналізу складних та багатофакторних ризиків, які важко піддаються формалізації. Метод Дельфі дозволяє досягти консенсусу серед експертів щодо найбільш імовірних сценаріїв розвитку подій та їх можливих наслідків. Сценарний аналіз передбачає розробку альтернативних варіантів розвитку ситуації з урахуванням різних комбінацій факторів ризику.

Інтеграція кількісних та якісних підходів здійснюється через створення комплексних моделей оцінки ризиків, що враховують як статистичні дані, так і експертні судження. Методологія передбачає використання багатокритеріального аналізу для ранжування ризиків за ступенем їх

пріоритетності. При цьому застосовуються методи нечіткої логіки для роботи з неповною або неточною інформацією.

Особливістю методології оцінки ризиків національної безпеки України є необхідність врахування специфіки гібридних загроз. Гібридні ризики характеризуються міждисциплінарним характером, високою динамікою змін та складністю прогнозування їх розвитку. Це вимагає розробки спеціальних індикаторів раннього попередження, здатних виявляти латентні загрози на ранніх стадіях їх формування. Методологія оцінки регіональних аспектів національної безпеки повинна враховувати нерівномірність розподілу ризиків по території держави та різну ступінь вразливості окремих регіонів. Оцінка впливу військової організації держави на соціально-економічний розвиток регіонів здійснюється за напрямами: зміна обсягу податкових надходжень до консолідованого бюджету регіону, зміна обсягу надходжень до територіальних відділень позабюджетних фондів, зміна розміру споживацького попиту в регіоні, зміна рівня зайнятості населення регіону, зміна наукового потенціалу регіону [42].

Система індикативної оцінки повинна забезпечувати можливість швидкого реагування на зміни в безпековому середовищі. Це досягається через створення системи моніторингу в режимі реального часу, що дозволяє відстежувати критичні показники та своєчасно сигналізувати про наближення небезпечних порогових значень. Методологія передбачає розробку алгоритмів автоматичного аналізу вхідної інформації та формування попереджень про потенційні загрози.

Валідація методології здійснюється через зіставлення результатів прогнозування з фактичним розвитком подій, що дозволяє коригувати параметри моделей та підвищувати точність оцінок. Система повинна бути адаптивною та здатною навчатися на основі накопиченого досвіду, постійно удосконалюючи алгоритми аналізу та прогнозування.

Базовий набір стандартних процедур індикативного забезпечення національної безпеки України має реалізовуватися профільними центрами та органами, що відповідають за безпеку. Цей набір складається з аналітичної, проектної та виконавської частин. Аналітична частина передбачає аналіз трендів за кожним з базових індексів за останній трирічний період, виділення негативних трендів для подальшого аналізу та розробки проектів на основі аналітики. Особливу увагу приділяється ситуаціям, коли негативні тренди властиві предметним або цільовим кластерам в цілому, оскільки в таких випадках небезпека особливо висока і потребує розробки комплексних проектів дій.

Проектна частина включає складання та реалізацію планів дій в рамках розроблених проектів. Дії оцінюються з точки зору їх внеску в поліпшення показників тих базових індексів, по яких має місце негативний тренд. Комплексні проекти та плани у випадку негативного тренду за кластером вимагають взаємодії кількох агентств, що зумовлює необхідність створення міжвідомчих систем реалізації таких проектів. Виконавська частина передбачає проведення коригуючих дій за результатами оцінки реалізації планів: уточнення проектів, удосконалення планів, зміна неефективних заходів, впровадження відомчої та персональної відповідальності за недосягнення результатів.

Практична реалізація індикативного підходу в Україні стикається з низкою викликів та обмежень. Основною проблемою є недостатність розвитку інформаційно-аналітичної інфраструктури, що ускладнює збір, обробку та аналіз великих масивів даних. Фрагментарність інформаційних систем різних відомств створює перешкоди для формування єдиної картини стану національної безпеки. Брак стандартизованих процедур збору та обробки інформації знижує якість та порівнянність даних [74].

Адаптація міжнародного досвіду до українських умов вимагає врахування специфіки правової системи та інституційної архітектури сектору

безпеки і оборони. На відміну від країн з розвиненою системою аналітичних центрів, Україна потребує створення відповідної інфраструктури думок-танків та дослідницьких інститутів, здатних забезпечити якісне експертне супроводження індикативних оцінок. Важливим є питання підготовки кваліфікованих кадрів, здатних працювати з сучасними методами аналізу даних та моделювання ризиків [148].

Особливості застосування індикативного підходу в умовах російської агресії пов'язані з необхідністю оперативного реагування на швидко мінливу ситуацію та високим рівнем невизначеності. Гібридний характер загроз вимагає розробки спеціальних індикаторів для оцінки інформаційних, кіберзагроз та інших нетрадиційних форм впливу. Система повинна бути здатною виявляти ознаки підготовки до ескалації конфлікту та надавати раннє попередження про можливі зміни в характері загроз [175].

Регіональний вимір індикативної оцінки національної безпеки набуває особливого значення з огляду на різну ступінь впливу конфлікту на окремі регіони України. Необхідним є врахування специфіки прикордонних областей, регіонів з високою концентрацією критично важливої інфраструктури, територій з компактним проживанням національних меншин. Система індикаторів має забезпечувати можливість оцінки стану тимчасово окупованих територій на основі доступної інформації та дистанційних методів моніторингу [23].

Інтеграція індикативного підходу з існуючою системою стратегічного планування в сфері національної безпеки передбачає узгодження з процесами розробки та реалізації Стратегії національної безпеки, стратегій у сферах оборони, кібербезпеки, боротьби з тероризмом. Індикативні оцінки мають стати основою для коригування стратегічних документів та оперативного планування діяльності органів сектору безпеки і оборони [139].

Перспективи розвитку індикативного підходу в Україні пов'язані з впровадженням сучасних інформаційних технологій, включаючи штучний

інтелект, машинне навчання та технології великих даних. Створення національної системи моніторингу загроз національній безпеці на основі індикативних методів може стати важливим елементом цифрової трансформації сектору безпеки і оборони. Розвиток міжнародного співробітництва у сфері обміну інформацією та координації оцінок загроз сприятиме підвищенню ефективності національної системи індикативного моніторингу та її інтеграції з європейськими та євроатлантичними механізмами забезпечення безпеки [145].

Висновки до розділу 2

У другому розділі здійснено комплексний аналіз сучасного стану державного управління сектором безпеки і оборони України, що дає підстави для таких висновків.

Оцінка ефективності існуючих механізмів державного управління сектором безпеки і оборони засвідчила, що, попри суттєвий прогрес у реформуванні сектору після 2014 року та в умовах повномасштабної збройної агресії, система управління зберігає ознаки фрагментарності: розподіл повноважень між суб’єктами сектору залишається недостатньо чітким, а координаційні механізми не забезпечують належної узгодженості дій у режимі реального часу.

Аналіз інституційних та нормативно-правових засад реформування показав, що сформована законодавча база загалом відповідає євроатлантичним підходам, однак її практична імплементація стримується інерційністю інституційної структури, дублюванням функцій органів управління та недостатньою спроможністю механізмів демократичного цивільного контролю. Імплементація європейських практик правового регулювання потребує подальшої гармонізації національного законодавства зі стандартами НАТО та ЄС [105].

Обґрунтовано методичні засади застосування індикативного підходу до оцінки ризиків національній безпеці України: визначено систему індикаторів та показників оцінки загроз, методологію кількісного та якісного оцінювання ризиків, а також практичні аспекти імплементації індикативного підходу в українських умовах. Доведено, що індикативний підхід створює об’єктивне інформаційно-аналітичне підґрунтя для прийняття управлінських рішень щодо реформування сектору безпеки і оборони [148].

Отримані результати аналізу є емпіричною основою для розроблення концептуальної моделі та практичних рекомендацій щодо удосконалення механізмів державного управління реформуванням сектору безпеки і оборони, поданих у третьому розділі.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ РЕФОРМУВАННЯМ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

3.1. Концептуальні засади оптимізації системи управління сектором безпеки і оборони

Система управління сектором безпеки і оборони України переживає процес кардинальних змін, зумовлених необхідністю адекватної відповіді на сучасні безпекові виклики та досягнення стандартів євро-атлантичної інтеграції. Формування концептуальних засад оптимізації цієї системи потребує комплексного аналізу принципів демократичного управління, міжнародного досвіду та специфічних умов, в яких функціонує український сектор безпеки і оборони. Актуальність такої оптимізації підтверджується як воєнним досвідом України у протистоянні російській агресії, так і необхідністю приведення національних механізмів управління у відповідність до стандартів НАТО та Європейського Союзу [51].

Концептуальна основа оптимізації системи управління сектором безпеки і оборони України ґрунтується на принципах, що відповідають сучасним викликам національної безпеки та вимогам демократичного врядування. Визначення цих принципів потребує врахування як теоретичних напрацювань у сфері безпекових студій, так і практичного досвіду провідних демократичних держав світу [155].

Принцип єдиного стратегічного керівництва передбачає формування централізованої системи прийняття рішень на найвищому рівні державного управління з одночасним забезпеченням ефективної координації між усіма складовими сектору безпеки і оборони. Цей принцип відповідає сучасним вимогам інтегрованого підходу до національної безпеки, коли загрози мають комплексний характер і потребують скоординованої відповіді різних

відомств. Реалізація даного принципу передбачає створення дієвого механізму стратегічного планування, що об'єднує оборонне, політичне, економічне та інформаційне планування в єдину систему. Особливого значення набуває формування інституційної спроможності для прийняття швидких рішень в умовах невизначеності, що є критично важливим в умовах гібридних загроз [166].

Принцип демократичного цивільного контролю становить основу легітимності функціонування сектору безпеки і оборони в демократичній державі. Цей принцип передбачає підпорядкування військових та силових структур цивільній владі, забезпечення парламентського нагляду за їх діяльністю та прозорості у витрачанні бюджетних коштів. Європейський досвід демонструє, що ефективний цивільний контроль не означає мікроуправління військовими операціями, а полягає у визначенні стратегічних цілей, забезпеченні ресурсами та здійсненні нагляду за дотриманням законності. Особливого значення набуває розвиток інституційної спроможності цивільних керівників у сфері безпеки та оборони, формування відповідної експертизи та аналітичних можливостей [11].

Принцип адаптивності системи управління відображає необхідність швидкого реагування на зміни безпекового середовища та появу нових загроз. Сучасні виклики характеризуються динамічністю та непередбачуваністю, що вимагає від системи управління здатності до швидкої трансформації структур, процедур та підходів. Реалізація цього принципу передбачає створення гнучких організаційних структур, розвиток культури інновацій та постійного навчання, а також формування механізмів швидкого залучення додаткових ресурсів. Критично важливою є здатність системи до самоаналізу та корекції власного функціонування на основі отриманого досвіду та зміни зовнішніх умов.

Принцип міжвідомчої координації та інтеграції спрямований на подолання традиційної фрагментації у функціонуванні різних складових сектору безпеки і оборони. Сучасні загрози часто мають міжсекторальний

характер і не можуть бути ефективно подолані зусиллями окремих відомств. Це вимагає створення дієвих механізмів координації, обміну інформацією та спільного планування. Реалізація даного принципу передбачає формування єдиної інформаційно-аналітичної системи, стандартизацію процедур взаємодії та створення спільних структур для вирішення комплексних завдань. Особлива увага приділяється подоланню міжвідомчих бар'єрів та формуванню культури співпраці [65].

Загальну архітектуру запропонованої концептуальної моделі інтегрованого управління реформуванням сектору безпеки і оборони відображено на рис. 3.1.

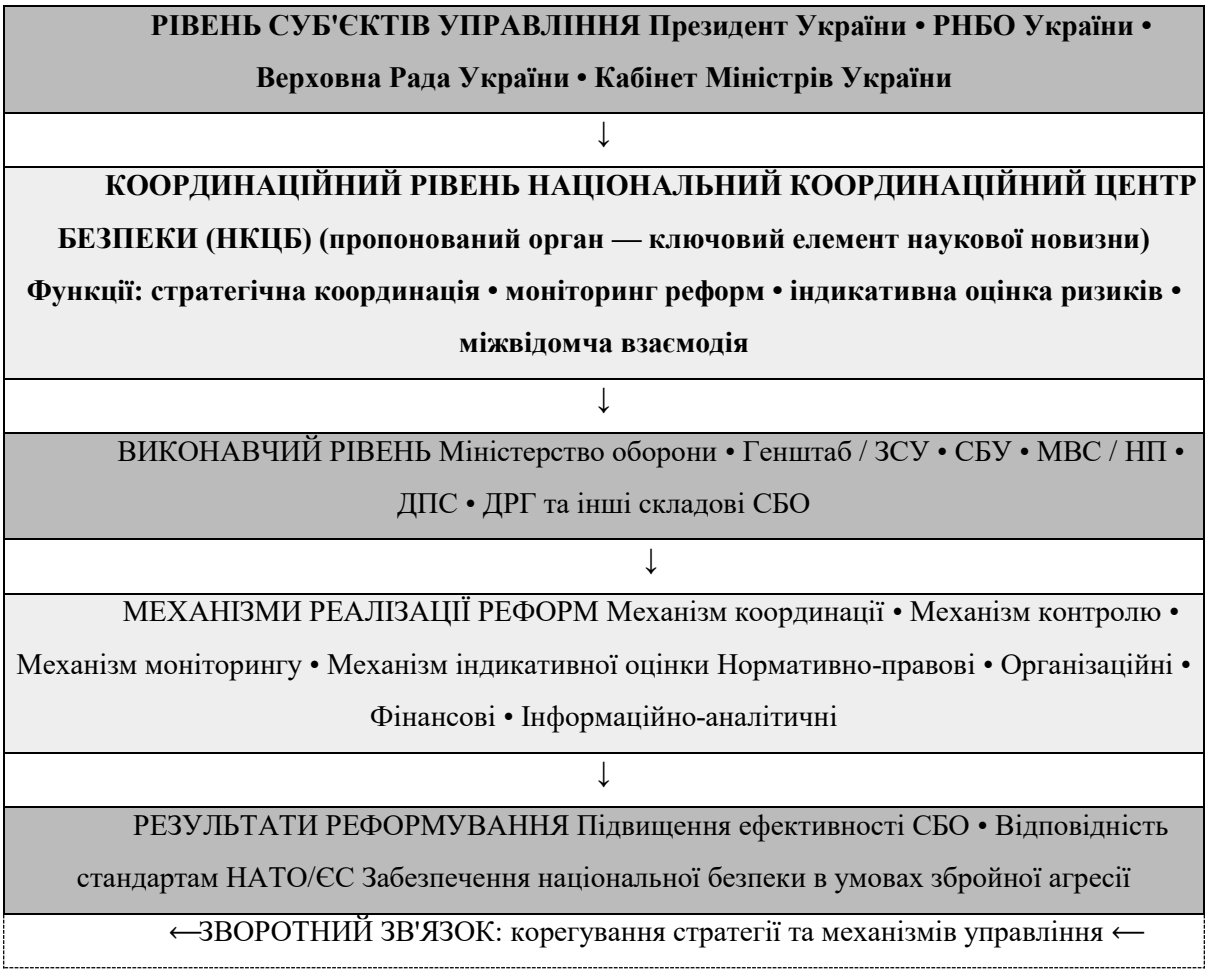

Рис. 3.1. Концептуальна модель інтегрованого управління реформуванням сектору безпеки і оборони України

Джерело: розроблено автором

Принцип прозорості та підзвітності забезпечує легітимність функціонування сектору безпеки і оборони та довіру з боку суспільства. Цей принцип передбачає максимально можливе оприлюднення інформації про діяльність силових структур з урахуванням вимог національної безпеки, регулярне звітування перед парламентом та громадськістю, а також створення ефективних механізмів розслідування порушень. Реалізація принципу прозорості сприяє підвищенню професійності персоналу, зменшенню корупційних ризиків та зміцненню довіри громадян до державних інституцій безпеки [30].

Принцип професіоналізації кадрового складу спрямований на формування високопрофесійного персоналу, здатного ефективно виконувати завдання в умовах сучасних загроз. Це передбачає створення дієвих систем відбору, підготовки, атестації та мотивації кадрів, розвиток професійних компетентностей та лідерських якостей. Особлива увага приділяється формуванню аналітичних спроможностей, здатності до стратегічного мислення та роботи в умовах невизначеності. Професіоналізація також включає розвиток культури безперервного навчання та адаптації до нових викликів. Аналіз функціонування існуючої системи управління сектором безпеки і оборони України виявляє низку структурних недоліків та системних проблем, що знижують її ефективність та перешкоджають адекватному реагуванню на сучасні загрози. Ці проблеми накопичувались протягом тривалого часу і стали особливо очевидними в умовах російської агресії, коли система опинилась під критичним навантаженням.

Фрагментація управлінських повноважень становить одну з найсерйозніших проблем існуючої системи. Розподіл відповідальності між різними органами влади часто є нечітким, що призводить до дублювання функцій, неефективного використання ресурсів та зниження оперативності прийняття рішень. Зокрема, координація між Радою національної безпеки і оборони України, профільними міністерствами та силовими відомствами

потребує істотного вдосконалення. Відсутність чітких механізмів розмежування повноважень між стратегічним, оперативним та тактичним рівнями управління створює додаткові ускладнення у функціонуванні системи [124].

Недостатність аналітичних спроможностей обмежує здатність системи до прогнозування загроз, оцінки ризиків та розробки адекватних стратегій реагування. Існуючі аналітичні структури часто працюють ізольовано, що перешкоджає формуванню комплексного розуміння безпекового середовища. Відсутність єдиної методології аналізу загроз та ризиків призводить до неузгодженості оцінок різних відомств та ускладнює процес прийняття обґрунтованих рішень. Особливої уваги потребує розвиток спроможностей для аналізу гібридних загроз, які поєднують військові та невійськові компоненти.

Слабкість інформаційно-комунікаційних систем перешкоджає ефективному обміну інформацією між різними складовими сектору безпеки і оборони. Технологічна застарілість, несумісність систем різних відомств та недостатній рівень кібербезпеки знижують оперативність та надійність управлінських процесів. Це особливо критично в умовах ведення бойових дій, коли швидкість та точність передачі інформації можуть мати вирішальне значення для успіху операцій. Кадрові проблеми включають недостатність фахівців з необхідними компетентностями, особливо у сферах стратегічного планування, аналітики та управління ризиками. Система підготовки та перепідготовки кадрів не завжди відповідає сучасним вимогам і потребує модернізації. Відсутність чітких критеріїв професійного росту та недостатня мотивація призводять до втрати кваліфікованих спеціалістів. Особливої уваги потребує формування нового покоління керівників, здатних працювати в умовах демократичного цивільного контролю та європейських стандартів управління [166].

Недосконалість правового регулювання створює прогалини та суперечності у функціонуванні системи управління. Застарілість багатьох нормативно-правових актів, їх неузгодженість між собою та з міжнародними стандартами перешкоджають ефективному функціонуванню системи. Особливо проблемним є регулювання міжвідомчої взаємодії, розподілу повноважень та відповідальності у кризових ситуаціях. Аналіз цих недоліків дозволяє визначити пріоритетні напрями оптимізації системи управління сектором безпеки і оборони. Першочерговими завданнями є усунення дублювання функцій через чітке розмежування повноважень, створення ефективних механізмів координації та інтеграції, розвиток аналітичних спроможностей та модернізація інформаційно-комунікаційних систем. Не менш важливими є питання кадрового забезпечення та правового регулювання, які становлять основу для всіх інших реформ [65].

Європейський досвід управління сектором безпеки і оборони надає цінні уроки для формування оптимальної моделі української системи. Аналіз практик провідних європейських країн дозволяє виявити найкращі підходи та механізми, які можуть бути адаптовані до українських умов з урахуванням національної специфіки та поточних викликів [160].

Досвід Великої Британії демонструє ефективність інтегрованого підходу до національної безпеки через створення Ради національної безпеки під головуванням прем'єр-міністра. Ця модель забезпечує координацію між усіма відомствами, залученими до питань безпеки, та дозволяє приймати швидкі рішення на найвищому політичному рівні. Британська система характеризується чітким розподілом стратегічного та оперативного рівнів управління, розвиненими аналітичними спроможностями та ефективним парламентським наглядом. Особливо цінним є досвід створення об'єднаних аналітичних структур, які забезпечують комплексну оцінку загроз та розробку інтегрованих стратегій реагування [87].

Французька модель управління сектором безпеки відзначається високим рівнем централізації та координації через офіс президента і Генеральний секретаріат з питань національної оборони та безпеки. Ця система забезпечує єдність стратегічного керівництва та оперативність прийняття рішень у кризових ситуаціях. Французький досвід демонструє важливість розвитку власних аналітичних спроможностей та створення ефективних механізмів стратегічного планування. Особливо корисним є підхід до інтеграції цивільних та військових експертів у процесі розробки політики безпеки. Німецька система управління безпекою характеризується розвиненим федеральним підходом та ефективною координацією між федеральним і земельним рівнями. Німецький досвід демонструє важливість парламентського контролю за сектором безпеки через спеціалізовані комітети та уповноваженого з оборонних питань. Система забезпечує високий рівень прозорості та підзвітності при збереженні оперативності управління. Особливо цінним є німецький підхід до цивільного контролю за збройними силами та розвиток професійної цивільної експертизи у сфері безпеки [168].

Скандинавські країни демонструють ефективні моделі інтегрованого управління національною безпекою з акцентом на цивільну готовність та стійкість суспільства. Їх досвід особливо актуальний для України в контексті протидії гібридним загрозам та забезпечення всеохопної оборони. Скандинавські системи характеризуються високим рівнем довіри між державою та суспільством, ефективною координацією між різними секторами та розвиненими механізмами кризового управління [168].

Досвід країн Центральної та Східної Європи, які пройшли шлях від посттоталітарної трансформації до членства в НАТО та ЄС, є особливо релевантним для України. Польський досвід демонструє важливість поступових, але послідовних реформ, спрямованих на приведення системи управління безпекою у відповідність до демократичних стандартів. Чеський

та угорський досвід показує значення розвитку цивільної експертизи та створення ефективних механізмів парламентського нагляду.

Загальноєвропейські стандарти, викладені у документах Європейської комісії та Ради Європи, підкреслюють важливість демократичного управління сектором безпеки, прозорості, підзвітності та дотримання прав людини. Ці стандарти передбачають ефективний демократичний контроль та нагляд за діяльністю силових структур, їх функціонування в межах чіткої правової бази, затвердженої національним законодавцем, включаючи ефективний цивільний контроль. Європейський підхід підкреслює необхідність залучення громадянського суспільства до розробки та моніторингу політики безпеки, що сприяє підвищенню легітимності та ефективності системи [33].

Адаптація європейського досвіду до українських умов потребує врахування специфічних факторів, зокрема тривалої військової агресії, необхідності швидкого реформування та обмежених ресурсів. Ключовими елементами, які можуть бути успішно імплементовані, є створення інтегрованих координаційних механізмів, розвиток аналітичних спроможностей, вдосконалення системи цивільного контролю та підвищення прозорості функціонування системи. Важливо також запозичити європейські підходи до стратегічного планування, кризового управління та міжнародної співпраці у сфері безпеки [17].

Організаційно-правові механізми оптимізації системи управління сектором безпеки і оборони України мають забезпечити структурну перебудову існуючої системи відповідно до сучасних вимог та європейських стандартів. Ці механізми включають як інституційні зміни, так і вдосконалення нормативно-правової бази, що регулює функціонування сектору безпеки [80].

Інституційна реформа має передбачати створення єдиного органу стратегічного планування та координації, який би забезпечував інтегрований

підхід до національної безпеки. Пропонується трансформація Ради національної безпеки і оборони України у повноцінний координаційний центр з відповідними аналітичними спроможностями та виконавчими повноваженнями. Цей орган має стати ключовою ланкою у процесі розробки стратегії національної безпеки, координації діяльності різних відомств та забезпечення єдності підходів до вирішення безпекових завдань [6].

Створення Національного центру ситуаційного аналізу та стратегічного планування при РНБО України дозволить консолідувати аналітичні спроможності різних відомств та забезпечити комплексну оцінку загроз. Цей центр має включати експертів з різних сфер – від військової справи до економіки та кібербезпеки – та забезпечувати безперервний моніторинг безпекового середовища. Важливою функцією центру має стати розробка сценаріїв розвитку подій та підготовка рекомендацій для прийняття політичних рішень [82].

Вдосконалення системи координації передбачає створення міжвідомчих робочих груп з ключових напрямів національної безпеки. Ці групи мають забезпечити постійну взаємодію між профільними міністерствами, силовими відомствами та іншими державними органами. Особлива увага приділяється створенню механізмів швидкого реагування на кризові ситуації, включаючи чіткі процедури ескалації рішень та мобілізації ресурсів [168].

Реформа системи стратегічного планування має забезпечити узгодженість довгострокових та середньострокових планів розвитку різних складових сектору безпеки. Пропонується запровадження єдиного циклу планування, який би синхронізував бюджетне планування з розробкою стратегічних документів. Це дозволить оптимізувати використання ресурсів та забезпечити послідовність у реалізації реформ.

Правове забезпечення оптимізації потребує комплексного перегляду та оновлення законодавчої бази. Першочерговим завданням є прийняття нового

Закону України "Про національну безпеку", який би чітко визначив повноваження та відповідальність різних органів влади, механізми координації та процедури прийняття рішень у сфері національної безпеки. Цей закон має стати правовою основою для всієї системи управління безпекою. Необхідно також оновити законодавство про оборону, внутрішні справи, службу безпеки та інші силові структури з метою усунення суперечностей та прогалин у регулюванні їх діяльності. Особливої уваги потребує законодавче забезпечення цивільного контролю за силовими структурами, включаючи розширення повноважень парламентських комітетів та створення незалежних органів нагляду [114; 118; 126].

Правове регулювання інформаційного обміну між відомствами має забезпечити баланс між потребою у координації та вимогами інформаційної безпеки. Пропонується розробка спеціального закону про інформаційну взаємодію у сфері національної безпеки, який би визначив принципи, процедури та технічні стандарти обміну інформацією [103; 140].

Створення правових механізмів участі громадянського суспільства у процесах формування політики безпеки сприятиме підвищенню прозорості та підзвітності системи. Це включає законодавче забезпечення доступу до інформації, процедур громадського обговорення стратегічних документів та механізмів громадського контролю за діяльністю силових структур. Інституційне забезпечення має також передбачати створення спеціалізованих органів для вирішення специфічних завдань. Зокрема, доцільним є створення Агентства з кібербезпеки, яке би координувало зусилля різних відомств у протидії кіберзагрозам. Аналогічно, створення Агентства з протидії гібридним загрозам дозволило б консолідувати зусилля у цій критично важливій сфері [89].

Технологічні рішення та цифровізація управлінських процесів становлять важливий напрям оптимізації системи управління сектором безпеки і оборони. Сучасні інформаційно-комунікаційні технології надають

унікальні можливості для підвищення ефективності, прозорості та оперативності управлінських рішень, що є критично важливим в умовах динамічного безпекового середовища.

Створення єдиної інформаційно-аналітичної системи сектору безпеки і оборони має стати основою технологічної модернізації управлінських процесів. Ця система має забезпечити інтеграцію інформаційних ресурсів різних відомств, стандартизацію форматів даних та створення єдиного інформаційного простору для прийняття рішень. Система має включати модулі для збору, обробки, аналізу та візуалізації інформації, а також засоби для моделювання сценаріїв та підтримки прийняття рішень. Впровадження технологій штучного інтелекту та машинного навчання може значно підвищити якість аналітичної роботи. Ці технології дозволяють обробляти великі обсяги неструктурованої інформації, виявляти приховані закономірності та тренди, автоматизувати рутинні аналітичні процеси. Особливо перспективним є використання ШІ для аналізу відкритих джерел інформації, моніторингу соціальних мереж та виявлення дезінформаційних кампаній [6].

Розвиток систем ситуаційного центру нового покоління забезпечить можливість безперервного моніторингу безпекової ситуації та швидкого реагування на виникаючі загрози. Сучасні ситуаційні центри мають бути обладнані засобами відеоконференцзв'язку, системами візуалізації даних, засобами моделювання та прогнозування. Важливо забезпечити можливість роботи в режимі реального часу з представниками різних відомств та рівнів управління.

Цифровізація документообігу та адміністративних процесів дозволить підвищити швидкість та прозорість прийняття управлінських рішень. Електронний документообіг має забезпечити можливість відстеження статусу рішень, контролю термінів виконання та аналізу ефективності управлінських процесів. Важливо також запровадити електронні системи

планування та звітності, які дозволять автоматизувати рутинні процеси та звільнити час для стратегічної діяльності.

Кібербезпека інформаційних систем управління має бути пріоритетним напрямом технологічної модернізації. Сучасні кіберзагрози вимагають створення національної системи кібербезпеки на основі стримування, кіберстійкості та взаємодії. Система захисту має включати засоби виявлення та попередження кіберінцидентів , механізми швидкого відновлення після атак та процедури забезпечення безперервності роботи критично важливих систем. Розвиток мобільних технологій та засобів зв'язку забезпечить можливість управління в умовах високої мобільності та децентралізації. Сучасні мобільні пристрої та засоби захищеного зв'язку дозволяють керівникам залишатися в курсі ситуації та приймати рішення незалежно від місця перебування. Це особливо важливо в умовах ведення бойових дій або інших кризових ситуацій [23].

Впровадження технологій блокчейн може підвищити прозорість та захищеність управлінських процесів, особливо у сферах закупівель, кадрових рішень та фінансового управління. Блокчейн технології забезпечують незмінність записів та можливість аудиту всіх операцій, що сприяє боротьбі з корупцією та підвищенню довіри до системи управління.

Створення цифрових платформ для взаємодії з громадянським суспільством дозволить підвищити участь громадян у процесах формування політики безпеки. Ці платформи мають забезпечити можливість отримання зворотного зв'язку від громадськості, проведення онлайн-консультацій та збору пропозицій щодо вдосконалення системи безпеки [54; 154].

Технологічна модернізація має супроводжуватися відповідною підготовкою персоналу та зміною організаційної культури. Впровадження нових технологій потребує інвестицій у навчання співробітників, створення служб технічної підтримки та розвиток культури цифрової грамотності у сфері управління.

Кадрове забезпечення та професіоналізація системи управління становить фундаментальну основу успішної оптимізації сектору безпеки і оборони. Без професійного, мотивованого та компетентного персоналу неможливо забезпечити ефективне функціонування навіть найдосконаліших організаційних структур та технологічних систем.

Стратегія кадрового забезпечення має ґрунтуватися на принципах меритократії, коли призначення на посади та кар'єрне зростання відбуваються виключно на основі професійних якостей та досягнень. Це передбачає створення прозорих та об'єктивних систем відбору, атестації та просування по службі. Важливо запровадити єдині стандарти професійної компетентності для різних категорій посад та регулярно їх оновлювати відповідно до змін у безпековому середовищі.

Розвиток системи професійної освіти та підготовки кадрів для сектору безпеки і оборони потребує кардинального оновлення. Навчальні заклади мають модернізувати свої програми відповідно до сучасних викликів та міжнародних стандартів. Особливої уваги потребує підготовка фахівців з стратегічного планування, аналізу ризиків, кризового управління та міжнародної співпраці. Доцільно створити спеціалізовані програми для підготовки цивільних керівників у сфері безпеки, які поєднували б теоретичну підготовку з практичним досвідом.

Система безперервної професійної освіти має забезпечити постійне оновлення знань та навичок персоналу відповідно до динаміки безпекового середовища. Це включає регулярні курси підвищення кваліфікації, участь у міжнародних програмах обміну досвідом, стажування у провідних інституціях партнерських країн. Важливо також розвивати внутрішньовідомчі програми навчання та обміну досвідом між різними підрозділами. Формування аналітичної культури в системі управління безпекою передбачає підготовку фахівців, здатних працювати з великими обсягами інформації, проводити комплексний аналіз загроз та розробляти

обґрунтовані рекомендації. Аналітики мають володіти не лише предметними знаннями у своїй сфері, але й навичками критичного мислення, системного аналізу та прогнозування. Доцільно створити спеціалізовану аналітичну службу з єдиними стандартами підготовки та методологією роботи [153].

Розвиток лідерських якостей керівного складу є критично важливим для успішного проведення реформ. Сучасні керівники у сфері безпеки мають поєднувати професійну експертизу з навичками стратегічного мислення, управління змінами та роботи в команді. Важливо розвивати програми підготовки резерву керівних кадрів, які включали б як теоретичну підготовку, так і практичні завдання з управління складними проектами.

Мотиваційні механізми мають забезпечити залучення та утримання кращих фахівців у системі управління безпекою. Це включає конкурентну оплату праці, можливості кар'єрного зростання, соціальні гарантії та визнання професійних досягнень. Важливо також створити систему нематеріальної мотивації, яка підкреслювала б важливість та престижність роботи у сфері національної безпеки.

Гендерний баланс та різноманітність кадрового складу сприяють підвищенню ефективності управлінських рішень. Державам-членам слід забезпечити розумну кількість жінок у різних секторах безпеки на всіх рівнях, включаючи міністерства оборони та національні делегації в міжнародних органах безпеки. Залучення жінок та представників різних соціальних груп збагачує процес прийняття рішень різними перспективами та підходами. Міжнародна співпраця у сфері кадрового забезпечення дозволяє скористатися досвідом партнерських країн та міжнародних організацій. Україна активно співпрацює з НАТО у сферах розбудови спроможностей, включаючи навчання та освіту, а також надання обладнання. Участь українських фахівців у міжнародних навчальних програмах, стажування у структурах НАТО та ЄС, спільні навчання та семінари сприяють підвищенню професійного рівня та засвоєнню кращих практик [9].

Цивільна експертиза у сфері безпеки потребує особливої уваги та розвитку. Демократичний цивільний контроль неможливий без професійної цивільної експертизи, здатної на рівних конкурувати з військовою у питаннях стратегії, планування та аналізу. Доцільно створити програми підготовки цивільних експертів з безпеки, які включали б як академічну підготовку, так і практичний досвід роботи у відповідних структурах.

Етичні стандарти та професійна культура мають стати невід'ємною частиною кадрової політики. Це включає дотримання принципів доброчесності, прозорості, відповідальності та служіння суспільним інтересам. Важливо розвивати кодекси професійної етики, системи внутрішнього контролю та механізми запобігання корупції [152].

Таким чином, концептуальні засади оптимізації системи управління сектором безпеки і оборони України базуються на принципах демократичного врядування, ефективної координації та професійного управління. Успішна реалізація цих засад потребує комплексного підходу, який поєднує інституційні реформи, технологічну модернізацію, правове забезпечення та розвиток людського капіталу. Врахування європейського досвіду та міжнародних стандартів, адаптованих до українських умов, дозволить створити сучасну, ефективну та демократично підзвітну систему управління національною безпекою, здатну адекватно відповідати на виклики XXI століття [166].

3.2. Модель інтегрованого управління ризиками національної безпеки в умовах гібридних загроз

Сучасне безпекове середовище характеризується появою принципово нових типів загроз, які поєднують військові та невійськові засоби впливу, відкриті та приховані методи дії, а також розмивають межі між війною та

миром. Гібридні загрози стали однією з найбільш серйозних викликів для національної безпеки демократичних держав, що потребує розробки адекватних механізмів протидії та принципово нових підходів до управління ризиками. Альянс НАТО визначає гібридні методи ведення війни як комбінацію військових та невійськових засобів, включаючи дезінформацію, кібератаки, економічний тиск, розгортання нерегулярних збройних груп та використання регулярних сил. Що є новим у атаках, які спостерігались в останні роки, так це їх швидкість, масштаб та інтенсивність, що стало можливим завдяки швидким технологічним змінам та глобальній взаємопов'язаності [174].

Українська модель протидії гібридним загрозам, що формується в умовах тривалої російської агресії, може стати важливим внеском у розвиток теорії та практики забезпечення національної безпеки. Досвід України демонструє, що традиційні підходи до управління безпекою, засновані на чіткому розмежуванні між військовими та цивільними загрозами, внутрішньою та зовнішньою безпекою, виявляються недостатніми для протидії гібридним викликам. Російські гібридні загрози включають саботаж критичної інфраструктури, вандалізм, мілітаризацію міграції та військове залякування, які особливо загострюються навколо важливих міжнародних подій та мають на меті підрив єдності західних союзників [161].

Концептуальна основа інтегрованого управління ризиками національної безпеки ґрунтується на розумінні того, що гібридні загрози вимагають комплексної відповіді, яка поєднує традиційні військові засоби із невійськовими інструментами протидії. Інтегрований підхід передбачає координацію зусиль усіх складових національної безпеки, включаючи державні органи, приватний сектор та громадянське суспільство, а також створення нових механізмів міжвідомчої взаємодії та координації.

Теоретичні засади інтегрованого управління ризиками базуються на системному підході до національної безпеки, який розглядає її як складну

адаптивну систему, здатну до самоорганізації та еволюції у відповідь на зміни зовнішнього середовища. Система національної безпеки в умовах гібридних загроз має характеризуватися нелінійністю, складністю взаємозв'язків між елементами, емерджентністю властивостей, що виникають на рівні системи в цілому, та здатністю до адаптації та навчання на основі отриманого досвіду [3].

Природа гібридних загроз полягає у їх багатомірності, адаптивності до конкретних умов цільової держави та здатності впливати одночасно на декілька сфер національної безпеки. Гібридні загрози характеризуються використанням різноманітних інструментів впливу - від традиційних військових засобів до інформаційно-психологічних операцій, економічного тиску, кіберзброї та дипломатичних маніпуляцій. Особливістю гібридних загроз є їх спрямованість не лише на військове поразку противника, але й на підрив його політичної стабільності, економічного потенціалу, соціальної згуртованості та міжнародного авторитету [151].

Інформаційна складова гібридних загроз набуває особливого значення в сучасних умовах, коли інформаційні технології стали невід'ємною частиною життя суспільства. Інформаційні маніпуляції та партнерства з місцевими медіа стають все більш помітними в гібридних кампаніях, спрямованих на підрив довіри до ЄС та НАТО в регіоні. Деякі ключові антизахідні наративи (проросійські) продовжують відігравати деструктивну роль у публічних сферах Західних Балкан як частина зусиль Росії підірвати довіру до ЄС та НАТО в регіоні. Боротьба з дезінформацією та іноземним втручанням в інформаційний простір вимагає координованих зусиль органів влади, підвищення медіа-грамотності населення та розвитку технічних засобів виявлення та нейтралізації інформаційних загроз.

Економічна складова гібридних загроз включає використання економічних важелів для досягнення політичних цілей, включаючи торговельні війни, енергетичний шантаж, фінансові маніпуляції та підрив

економічної стабільності цільової держави. Ці заходи можуть мати довготривалий характер та спрямовуватися на створення економічної залежності або підрив конкурентоспроможності національної економіки. Протидія економічним аспектам гібридних загроз потребує тісної координації між органами економічної політики, фінансового регулювання та національної безпеки [36].

Кібернетичний вимір гібридних загроз стає все більш критичним у міру зростання цифровізації суспільства та економіки. Кіберзагрози стали значною, тривалою загрозою для націй, при цьому цілеспрямовані кібератаки порушують критичні служби, спричиняючи серйозні ускладнення на багатьох рівнях. Кібератаки можуть бути спрямовані на критичну інфраструктуру, державні інформаційні системи, приватний сектор або громадян, створюючи каскадні ефекти по всій системі національної безпеки. Інтеграція кіберрозвідки загроз у процеси управління ризиками дозволяє оптимізувати результати оцінки ризиків та покращити захист критичної інфраструктури [35].

Соціально-психологічний аспект гібридних загроз спрямований на підрив соціальної згуртованості, посилення внутрішніх суперечностей та конфліктів, зниження довіри до державних інституцій та демократичних процесів. Ці заходи можуть включати підтримку радикальних рухів, розпалювання міжетнічних або міжконфесійних конфліктів, маніпулювання громадською думкою через соціальні мережі та інші канали впливу. Правовий виклик гібридних загроз полягає в тому, що багато з них здійснюються в "сірій зоні" між війною та миром, що ускладнює їх правову кваліфікацію та вибір адекватних заходів протидії. Традиційне міжнародне право та національне законодавство часто не передбачають ефективних механізмів протидії таким загрозам, що потребує розвитку нових правових інструментів та процедур.

Методологічні засади управління ризиками в умовах гібридних загроз

мають враховувати специфіку цих загроз, їх динамічний характер, багатосекторальний вплив та складність взаємозв'язків між різними типами ризиків. Інтегроване управління ризиками являє собою загальноорганізаційну дисципліну, що характеризується певними атрибутами, включаючи стратегію, оцінку, реагування, комунікацію та звітність, моніторинг та технології. Воно підкріплюється каркасом практик, процесів та сприяючих технологій, що підтримують культуру обізнаності про ризики, покращене прийняття рішень та продуктивність.

Системний підхід до управління ризиками гібридних загроз передбачає розуміння їх як складної адаптивної системи, де зміни в одному елементі можуть мати непередбачувані наслідки для інших компонентів системи безпеки. Це вимагає розробки динамічних моделей оцінки ризиків, здатних до постійного оновлення та адаптації до нових умов. Системний підхід також передбачає врахування синергетичних ефектів від взаємодії різних типів загроз та можливості каскадних збоїв у критично важливих системах.

Ризик-орієнтований підхід до управління гібридними загрозами базується на принципі пропорційності заходів протидії рівню та характеру загроз. Цей підхід передбачає постійну оцінку та переоцінку ризиків, пріоритизацію заходів протидії відповідно до їх критичності та ефективності, а також оптимізацію використання ресурсів. Ризик-орієнтований підхід також включає розробку сценаріїв розвитку подій та планів реагування на різні типи інцидентів. Адаптивне управління є ключовою методологічною особливістю управління ризиками гібридних загроз, оскільки ці загрози характеризуються високою динамікою та непередбачуваністю. Адаптивне управління передбачає здатність системи швидко реагувати на зміни в характері загроз, корегувати стратегії та тактики протидії, навчатися на власному досвіді та досвіді партнерів. Це вимагає створення гнучких організаційних структур, розвитку культури інновацій та експериментування.

Превентивний підхід спрямований на запобігання реалізації гібридних

загроз через створення стримуючих факторів, підвищення стійкості критично важливих систем та зменшення уразливості до потенційних атак. Превентивні заходи включають розвиток оборонних спроможностей, підвищення обізнаності населення про гібридні загрози, зміцнення кіберзахисту, диверсифікацію енергетичних джерел та ланцюгів постачання.

Проактивний підхід передбачає активні дії з виявлення та нейтралізації гібридних загроз на ранніх стадіях їх розвитку, до того як вони зможуть завдати значної шкоди. Це включає розвиток розвідувальних спроможностей, системи раннього попередження, механізмів швидкого реагування та контрзаходів. Проактивний підхід також може включати превентивні дипломатичні, економічні або інформаційні заходи для стримування потенційних агресорів.

Реактивний підхід фокусується на швидкому та ефективному реагуванні на гібридні інциденти після їх виникнення з метою мінімізації шкоди та швидкого відновлення нормального функціонування. Реактивні заходи включають кризове управління, координацію діяльності служб швидкого реагування, комунікацію з громадськістю та міжнародними партнерами, а також заходи з відновлення пошкоджених систем та структур.

Структурна модель інтегрованого управління ризиками національної безпеки в умовах гібридних загроз має забезпечити ефективну координацію між різними рівнями управління та секторами безпеки, оптимальний розподіл повноважень та відповідальності, а також гнучкість та адаптивність до змінних умов безпекового середовища. Ця модель повинна поєднувати централізоване стратегічне керівництво з децентралізованою оперативною діяльністю, забезпечуючи баланс між єдністю командування та швидкістю реагування на локальні загрози.

Стратегічний рівень управління ризиками включає формування загальнодержавної політики та стратегії протидії гібридним загрозам, визначення національних пріоритетів безпеки, розподіл ресурсів між різними

напрямами протидії та координацію з міжнародними партнерами. На стратегічному рівні здійснюється довгострокове планування розвитку спроможностей протидії гібридним загрозам, формування нормативно-правової бази, розробка доктринальних документів та стратегічних планів. Ключовою структурою стратегічного рівня має стати Національний центр координації протидії гібридним загрозам при Раді національної безпеки і оборони України, який би забезпечував загальне керівництво, координацію діяльності всіх відомств та інтеграцію зусиль у єдину систему протидії [80].

Стратегічний рівень також відповідає за формування політики міжнародної співпраці у сфері протидії гібридним загрозам, укладання відповідних угод та меморандумів, участь у міжнародних ініціативах та програмах. На цьому рівні здійснюється аналіз глобальних трендів у розвитку гібридних загроз, оцінка їх впливу на національну безпеку України та розробка довгострокових стратегій адаптації. Функції стратегічного рівня включають також координацію з законодавчою та судовою владою для забезпечення правового супроводу протидії гібридним загрозам, розробку відповідного законодавства та забезпечення його ефективної імплементації. Важливим аспектом є координація з громадянським суспільством та приватним сектором для забезпечення широкої підтримки заходів протидії гібридним загрозам та мобілізації всіх ресурсів суспільства [43].

Оперативний рівень управління ризиками відповідає за практичну реалізацію стратегічних рішень через конкретні програми, проекти та заходи протидії гібридним загрозам. На цьому рівні функціонують спеціалізовані структури різних відомств, які здійснюють постійний моніторинг загроз, аналіз ризиків, розробку тактичних планів та координацію операційної діяльності. Оперативний рівень забезпечує трансформацію стратегічних цілей у конкретні завдання для виконавчих структур та контролює їх виконання [132].

На оперативному рівні функціонують міжвідомчі координаційні

центри, що забезпечують взаємодію між різними відомствами та структурами у процесі протидії гібридним загрозам. Ці центри відповідають за планування комплексних операцій, розподіл завдань між виконавцями, координацію їх дій у часі та просторі, а також моніторинг результатів виконання.

Оперативний рівень також включає спеціалізовані аналітичні структури, що здійснюють глибокий аналіз конкретних типів гібридних загроз, розробляють методики їх виявлення та протидії, готують рекомендації для прийняття тактичних рішень. Ці структури забезпечують науково-методичну підтримку практичної діяльності з протидії гібридним загрозам та розробляють нові підходи та технології. Важливою складовою оперативного рівня є системи навчання та підготовки кадрів для роботи в умовах гібридних загроз. Ці системи забезпечують підготовку фахівців з різних аспектів протидії гібридним загрозам, проведення регулярних навчань та тренувань, обмін досвідом з міжнародними партнерами [52].

Тактичний рівень включає безпосереднє виконання конкретних заходів протидії гібридним загрозам силами та засобами оперативних підрозділів різних відомств та структур. На цьому рівні здійснюється практична реалізація планів реагування, проводяться контрзаходи, забезпечується захист критично важливих об'єктів, здійснюється розслідування інцидентів та відновлення після атак. Тактичний рівень характеризується високою динамічністю та потребує швидкого прийняття рішень в умовах обмеженої інформації та часового тиску.

Структури тактичного рівня включають оперативні підрозділи силових відомств, служб надзвичайних ситуацій, кіберзахисту, інформаційної безпеки та інші спеціалізовані формування. Ці підрозділи мають бути готові до швидкого розгортання та дії в різних умовах, включаючи міські та сільські райони, критично важливі об'єкти, кіберпростір та інформаційне середовище.

Критично важливою є здатність тактичного рівня до швидкого масштабування відповіді відповідно до характеру та інтенсивності загрози.

Це вимагає створення резервних спроможностей, можливостей швидкого посилення угруповань сил та засобів, а також гнучких процедур мобілізації додаткових ресурсів. Координаційні механізми між різними рівнями управління мають забезпечити ефективну вертикальну інтеграцію системи управління ризиками гібридних загроз. Ці механізми включають регулярні наради та конференц-зв'язки між керівниками різних рівнів, систему звітності про стан справ та результати діяльності, процедури ескалації складних питань на вищий рівень управління.

Горизонтальна інтеграція в моделі управління ризиками забезпечується через створення міжсекторальних платформ співпраці та обміну інформацією між різними відомствами, приватним сектором та громадянським суспільством. ЄС створив основи для практичного створення гібридних груп швидкого реагування як один з інструментів у гібридному інструментарії ЄС для підтримки держав-членів ЄС, партнерських країн та місій і операцій CSDP під час протидії гібридним загрозам. Ці платформи мають включати представників усіх зацікавлених сторін та забезпечувати регулярний обмін інформацією, координацію планів та спільну розробку заходів протидії.

Міжсекторальна співпраця особливо важлива у сфері захисту критичної інфраструктури, оскільки більшість об'єктів критичної інфраструктури належить приватному сектору. Це вимагає створення ефективних механізмів державно-приватного партнерства, включаючи обмін інформацією про загрози, координацію заходів захисту, спільне планування заходів реагування на інциденти [35].

Важливою складовою горизонтальної інтеграції є залучення академічних інституцій, аналітичних центрів та експертного співтовариства до процесів аналізу гібридних загроз та розробки заходів протидії. Це забезпечує доступ до найновіших наукових досліджень, незалежної експертизи та інноваційних підходів до вирішення складних проблем безпеки. Регіональна інтеграція передбачає координацію зусиль з протидії

гібридним загрозам з сусідніми країнами та регіональними партнерами, які стикаються з аналогічними викликами. Це включає обмін інформацією про загрози, координацію заходів реагування на транскордонні інциденти, спільні навчання та тренування, розробку регіональних стандартів та процедур [96].

Функціональні компоненти моделі включають систему раннього попередження, механізми оцінки та аналізу загроз, засоби протидії та нейтралізації, системи відновлення після інцидентів, а також механізми навчання та адаптації. Кожен компонент має свої специфічні завдання, функції та інструменти, але всі вони функціонують як єдина інтегрована система, забезпечуючи синергетичний ефект від їх скоординованої взаємодії.

Система раннього попередження про гібридні загрози має забезпечити своєчасне виявлення ознак підготовки та початку гібридних операцій противника через інтеграцію різноманітних джерел інформації та аналітичних засобів. Ця система повинна поєднувати технічні засоби моніторингу інформаційного простору, кіберсередовища та фізичного простору з аналітичними спроможностями для інтерпретації отриманих даних та виявлення прихованих закономірностей. Важливим елементом є створення індикаторів та критеріїв для оцінки рівня гібридних загроз, що дозволить своєчасно активувати відповідні механізми реагування та мобілізувати необхідні ресурси.

Система раннього попередження має включати автоматизовані засоби моніторингу соціальних мереж, новинних ресурсів, форумів та інших платформ для виявлення координованих інформаційних кампаній, дезінформації та пропаганди. Технології штучного інтелекту та машинного навчання дозволяють обробляти великі обсяги текстової, аудіо та відео інформації для виявлення аномальних патернів та підозрілої активності. Кібермоніторинг як складова системи раннього попередження включає постійне спостереження за мережевою активністю, виявлення аномалій у трафіку, ідентифікацію нових типів шкідливого програмного забезпечення та

відслідковування кіберзлочинних угруповань. Інтеграція різних джерел кіберрозвідки дозволяє створити комплексну картину кіберзагроз та передбачити можливі напрями атак.

Фізичний моніторинг включає спостереження за критично важливими об'єктами інфраструктури, транспортними вузлами, кордонами та іншими стратегічно важливими територіями для виявлення підозрілої активності, можливих актів саботажу або підготовки до них. Використання супутникових знімків, безпілотних літальних апаратів та інших засобів дистанційного зондування дозволяє розширити можливості фізичного моніторингу. Функціональна архітектура системи управління ризиками гібридних загроз базується на принципах модульності, масштабованості, взаємозамінності компонентів та відмовостійкості. Модульний підхід дозволяє системі адаптуватися до різних типів загроз через активацію відповідних модулів, швидко переконфігоровуватися відповідно до зміни обстановки та ефективно використовувати доступні ресурси. Принцип масштабованості забезпечує можливість нарощування потужності системи відповідно до інтенсивності загроз, а взаємозамінність компонентів гарантує стійкість системи до відмов окремих елементів.

Модуль ідентифікації та класифікації загроз відповідає за виявлення потенційних гібридних загроз, їх первинну обробку та категоризацію відповідно до типу, рівня небезпеки, географічного охоплення та потенційного впливу. Цей модуль використовує широкий спектр джерел інформації, включаючи відкриті джерела, розвідувальні дані, технічні засоби спостереження, повідомлення від громадян та партнерських організацій. Модуль включає засоби автоматичного збору та первинної обробки інформації, алгоритми машинного навчання для виявлення аномалій та підозрілих патернів , а також експертні системи для класифікації виявлених загроз.

Функціонал модуля включає моніторинг інформаційного простору для

виявлення дезінформаційних кампаній, пропаганди та маніпулятивного контенту. Аналіз соціальних мереж дозволяє виявляти координовані інформаційні операції, штучне нагнітання соціальної напруженості, поширення екстремістських ідей. Кібермоніторинг спрямований на виявлення кіберзагроз, включаючи підготовку до кібератак, розповсюдження шкідливого програмного забезпечення, компрометацію критично важливих систем.

Модуль також здійснює моніторинг економічного середовища для виявлення ознак економічних атак, включаючи маніпуляції на фінансових ринках, торговельні війни, енергетичний шантаж, атаки на критично важливі ланцюги постачання. Фізичний моніторинг включає спостереження за критичною інфраструктурою, транспортними системами, енергетичними об'єктами для виявлення ознак підготовки до саботажу або диверсій.

Модуль оцінки ризиків здійснює комплексний аналіз потенційного впливу ідентифікованих загроз на різні сфери національної безпеки, оцінює ймовірність їх реалізації та можливі наслідки. Встановлена система внутрішнього контролю та управління ризиками надає можливість запобігати та своєчасно реагувати на загрози, що виникають у ході будь-якого виду діяльності, при цьому успіх виконання запланованих завдань та досягнення поставлених цілей залежать від цього процесу. Цей модуль використовує кількісні та якісні методи оцінки, включаючи статистичний аналіз, експертні оцінки, моделювання сценаріїв розвитку подій та аналіз каскадних ефектів від реалізації загроз [93].

Методологічною основою модуля є ризик-орієнтований підхід, який передбачає систематичну оцінку всіх аспектів виявлених загроз, включаючи їх джерела, механізми дії, потенційні цілі, можливі наслідки та ймовірність реалізації. Модуль використовує матриці ризиків для візуалізації та пріоритизації загроз, дерева подій для аналізу причинно-наслідкових зв'язків, моделі Монте-Карло для імітаційного моделювання складних сценаріїв.

Особливою функцією модуля є оцінка каскадних та системних ризиків, коли реалізація однієї загрози може спричинити ланцюгову реакцію в інших сферах або системах. Це особливо важливо для гібридних загроз, які характеризуються комплексним впливом на різні сфери національної безпеки одночасно [56].

Модуль планування та координації реагування розробляє стратегії, тактики та конкретні плани протидії виявленим гібридним загрозам, забезпечує координацію дій різних відомств та структур, оптимально розподіляє завдання та ресурси, а також здійснює постійний моніторинг виконання розроблених планів. Цей модуль є ключовою ланкою між аналітичною та виконавчою складовими системи управління ризиками, забезпечуючи трансформацію результатів аналізу у конкретні дії з протидії загрозам.

Функціонал модуля включає розробку сценарних планів для різних типів гібридних інцидентів, що дозволяє швидко активувати відповідні заходи протидії без необхідності розробки нових планів у кризовій ситуації. Планування здійснюється на основі результатів оцінки ризиків з урахуванням доступних ресурсів, правових обмежень, політичних факторів та міжнародних зобов'язань.

Координаційна функція модуля забезпечує синхронізацію дій різних відомств та структур, уникнення дублювання зусиль, оптимізацію використання ресурсів та максимізацію синергетичного ефекту від скоординованих дій. Модуль підтримує постійний зв'язок з усіма учасниками процесу протидії, координує їх планування, забезпечує обмін інформацією та взаємну підтримку.

Модуль виконання контрзаходів включає практичну реалізацію розроблених планів протидії гібридним загрозам силами та засобами відповідних органів та структур, координацію їх оперативної діяльності та забезпечення ефективного використання всіх доступних інструментів

протидії. Цей модуль є виконавчою ланкою системи управління ризиками та відповідає за безпосередню реалізацію контрзаходів у реальному часі. Функціональні можливості модуля включають координацію діяльності військових, правоохоронних, розвідувальних, кіберзахисних та інших спеціалізованих структур, забезпечення синхронізації їх дій у часі та просторі, оптимізацію використання наявних сил та засобів. Модуль забезпечує правове супроводження всіх контрзаходів, дотримання принципів демократичного врядування та міжнародного права навіть в умовах кризових ситуацій [146].

Особливою функцією модуля є забезпечення адаптивності контрзаходів до динамічних змін у характері загроз. Гібридні загрози часто змінюють свою тактику у відповідь на контрзаходи, що вимагає постійної корекції планів та методів протидії. Модуль забезпечує швидку переорієнтацію зусиль, зміну пріоритетів, перерозподіл ресурсів відповідно до еволюції загроз.

Модуль відновлення та адаптації здійснює комплексний аналіз наслідків гібридних інцидентів, організовує швидке та ефективне відновлення пошкоджених систем і структур, а також розробляє науково обґрунтовані рекомендації щодо вдосконалення всієї системи протидії на основі детального аналізу отриманого досвіду та виявлених недоліків. Цей модуль забезпечує зворотний зв'язок та постійне вдосконалення системи управління ризиками, що є критично важливим для ефективної протидії гібридним загрозам, які постійно еволюціонують.

Відновлювальна функція модуля включає координацію робіт з ліквідації наслідків гібридних атак, відновлення функціонування критично важливих систем, надання допомоги постраждалим, мінімізацію економічних збитків. Особливої уваги потребує психологічна реабілітація суспільства після інформаційно-психологічних атак, відновлення довіри до державних інституцій, подолання соціального розколу. Аналітична функція модуля

спрямована на глибокий аналіз механізмів реалізації гібридних загроз, ефективності застосованих контрзаходів, виявлення слабких місць у системі протидії, ідентифікацію нових типів загроз та методів їх реалізації. Результати аналізу використовуються для вдосконалення всіх компонентів системи управління ризиками [46].

Технологічне забезпечення інтегрованого управління ризиками гібридних загроз становить критично важливий фундамент ефективного функціонування всієї системи та визначає її спроможність адекватно реагувати на швидко змінні та складні виклики сучасного безпекового середовища. Сучасні інформаційні та комунікаційні технології не лише надають унікальні можливості для збору, обробки та аналізу великих обсягів різноманітної інформації, але й дозволяють автоматизувати багато процесів, підвищити швидкість реагування та забезпечити високу точність аналітичних висновків.

Архітектура технологічної платформи базується на принципах відкритості, масштабованості, інтероперабельності та безпеки. Відкрита архітектура дозволяє інтегрувати різноманітні технологічні рішення та системи, забезпечуючи гнучкість та можливість поступової модернізації. Масштабованість забезпечує можливість нарощування обчислювальних потужностей та функціональних можливостей відповідно до зростання обсягів даних та складності завдань. Інтероперабельність гарантує ефективну взаємодію між різними системами та компонентами, а безпека захищає критично важливу інформацію та процеси від несанкціонованого доступу та впливу.

Система збору та інтеграції інформації являє собою розподілену мережу засобів збору даних з різноманітних джерел, включаючи відкриті джерела інформації в мережі Інтернет, соціальні мережі та медіаплатформи, технічні засоби спостереження та моніторингу, сенсорні мережі на критично важливих об'єктах, розвідувальні дані від партнерських служб, повідомлення

та сигнали від громадян через спеціалізовані додатки та телефонні лінії. Система забезпечує автоматичний збір інформації у режимі реального часу, її первинну обробку, нормалізацію форматів, усунення дублювання та стандартизацію для подальшого аналізу.

Важливим компонентом системи є засоби семантичної обробки неструктурованої інформації, включаючи текстові документи, аудіо та відеоматеріали, зображення. Технології обробки природної мови дозволяють автоматично аналізувати великі обсяги текстової інформації, виявляти ключові теми, настрої, емоційне забарвлення, виявляти пропаганду та дезінформацію. Системи розпізнавання образів та відео аналітика дозволяють обробляти візуальну інформацію для виявлення підозрілих об'єктів, осіб, активностей.

Створення єдиної онтології гібридних загроз є критично важливим елементом системи збору інформації, оскільки дозволяє стандартизувати термінологію, класифікацію загроз, методи їх опису та аналізу. Це забезпечує кращу взаємодію між різними відомствами та системами, підвищує якість аналітичної роботи та полегшує обмін інформацією з міжнародними партнерами.

Аналітичні системи штучного інтелекту представляють собою комплекс взаємопов'язаних технологій машинного навчання, глибокого навчання, експертних систем та когнітивних обчислень, спрямованих на автоматичний аналіз великих масивів різнорідної інформації для виявлення прихованих закономірностей, аномалій та індикаторів гібридних загроз. Ці системи здатні обробляти структуровані та неструктуровані дані, виявляти складні кореляції між різними типами інформації, прогнозувати розвиток ситуацій та генерувати рекомендації для прийняття рішень.

Технології машинного навчання використовуються для автоматичної класифікації загроз, кластеризації подій, виявлення аномалій у поведінці різних систем та суб'єктів. Алгоритми навчання без учителя дозволяють

виявляти раніше невідомі типи загроз та патерни поведінки, що особливо важливо в умовах постійної еволюції гібридних загроз. Навчання з підкріпленням може використовуватися для оптимізації стратегій протидії та адаптації до змін у тактиці противника.

Глибоке навчання та нейронні мережі застосовуються для аналізу складних багатовимірних даних, розпізнавання образів у великих масивах інформації, обробки природної мови для виявлення дезінформації та маніпулятивного контенту. Рекурентні нейронні мережі та трансформери особливо ефективні для аналізу темпоральних даних та виявлення динамічних патернів у розвитку загроз.

Системи природного мовного процесингу (NLP) дозволяють автоматично аналізувати текстові повідомлення у соціальних мережах, новинні матеріали, документи для виявлення координованих інформаційних кампаній, дезінформації, пропаганди, екстремістського контенту. Сентимент-аналіз допомагає оцінювати емоційне забарвлення контенту та його вплив на громадську думку.

Експертні системи інтегрують знання експертів з різних галузей безпеки у формалізовану базу знань, що дозволяє автоматизувати процеси прийняття рішень, забезпечити консистентність аналітичних висновків, зберігати та передавати експертний досвід. Системи підтримки прийняття рішень комбінують результати автоматичного аналізу з експертними знаннями для генерування рекомендацій щодо оптимальних стратегій реагування.

Платформи візуалізації та підтримки прийняття рішень забезпечують ефективне представлення результатів аналізу у зручному для сприйняття та інтерпретації форматі, що є критично важливим для швидкого розуміння складної інформації та прийняття обґрунтованих рішень в умовах обмеженого часу. Ці платформи включають інтерактивні дашборди з можливістю налаштування відображення інформації відповідно до потреб

конкретних користувачів, геоінформаційні системи для просторового аналізу загроз та візуалізації їх географічного розподілу, засоби тривимірного моделювання та віртуальної реальності для імерсивної візуалізації складних сценаріїв.

Інтерактивні дашборди забезпечують режим реального часу відображення ключових індикаторів стану безпеки, автоматичні сповіщення про критичні події, можливість деталізації інформації на різних рівнях абстракції. Користувачі можуть налаштовувати персоналізовані робочі простори, створювати власні аналітичні представлення, експортувати дані для подальшого аналізу.

Геоінформаційні системи дозволяють візуалізувати географічне розподілення загроз, аналізувати просторові кореляції між різними типами інцидентів, моделювати поширення загроз по території, оптимізувати розміщення сил та засобів протидії. Інтеграція з супутниковими даними та аерофотозйомкою забезпечує актуальну інформацію про стан території та об'єктів.

Засоби моделювання сценаріїв дозволяють конструювати різні варіанти розвитку подій, оцінювати їх ймовірність та можливі наслідки, порівнювати ефективність різних стратегій реагування. Імітаційне моделювання дозволяє тестувати нові підходи та стратегії без ризику для реальних систем. Інструменти колективної роботи забезпечують можливість спільного аналізу інформації групами експертів, обмін думками та гіпотезами, колективне прийняття рішень. Системи відеоконференцій, спільного редагування документів, колективних аналітичних сесій підвищують ефективність командної роботи.

Системи автоматизованого реагування представляють собою комплекс технологій, що дозволяють швидко активувати певні контрзаходи у відповідь на виявлені загрози без необхідності прямого втручання оператора, що є особливо важливим для протидії швидкоплинним загрозам, таким як

кібератаки, дезінформаційні кампанії або фізичні атаки на критичну інфраструктуру. Ці системи базуються на заздалегідь визначених правилах та алгоритмах реагування, машинному навчанні для адаптації до нових типів загроз, інтеграції з системами управління безпекою для координованої відповіді.

Автоматичне реагування на кіберзагрози включає ізоляцію підозрілих мережевих сегментів, блокування шкідливого трафіку, оновлення правил фаєрволів, активацію резервних систем. Системи можуть автоматично аналізувати шкідливе програмне забезпечення, генерувати сигнатури для антивірусних систем, розповсюджувати оновлення захисту по всій мережі.

Протидія дезінформації може включати автоматичне виявлення та позначення підозрілого контенту, зниження його рейтингу у пошукових системах та соціальних мережах, генерацію контрнаративів , активацію каналів офіційної комунікації для поширення достовірної інформації.

Фізичний захист критичної інфраструктури може включати автоматичну активацію систем безпеки, перенаправлення транспортних потоків, ізоляцію критично важливих об'єктів, мобілізацію сил швидкого реагування. Однак усі автоматизовані системи повинні працювати під контролем людини-оператора для забезпечення адекватності та пропорційності реагування, особливо в складних або неоднозначних ситуаціях.

Технології блокчейн та розподілених реєстрів можуть використовуватися для забезпечення цілісності та автентичності критично важливої інформації, особливо в умовах активних інформаційних атак та спроб фальсифікації даних. Блокчейн технології забезпечують створення незмінних записів про ключові рішення, події, транзакції, що важливо для подальшого аудиту, розслідування інцидентів та встановлення відповідальності.

Застосування блокчейн для захисту цілісності даних включає створення

розподілених реєстрів для зберігання критично важливих документів, забезпечення незмінності журналів подій у системах безпеки, захист від підміни офіційної інформації органів влади. Смарт-контракти можуть автоматизувати виконання певних процедур реагування на загрози за умови виконання заздалегідь визначених умов.

Децентралізована ідентифікація та автентифікація на основі блокчейн може підвищити безпеку доступу до критично важливих систем, захистити від атак на системи управління ідентифікацією, забезпечити незалежну верифікацію особистості користувачів. Квантові технології, хоча поки що знаходяться на стадії активного розвитку, мають потенціал кардинально змінити ландшафт інформаційної безпеки та створити нові можливості як для захисту, так і для атак. Квантова криптографія може забезпечити принципово новий рівень захисту комунікацій, оскільки базується на фундаментальних законах квантової фізики, що робить перехоплення інформації технічно наявним та запобігає несанкціонованому доступу [17].

Квантові обчислення можуть значно підвищити аналітичні спроможності для обробки надвеликих масивів даних, розв'язання складних оптимізаційних задач, моделювання складних систем. Водночас квантові комп'ютери можуть створити загрозу для існуючих систем шифрування, що вимагає розробки квантово-стійких алгоритмів криптографії.

Квантові сенсори можуть забезпечити надвисоку чутливість для виявлення фізичних загроз, включаючи несанкціоноване проникнення, вибухові речовини, радіоактивні матеріали. Квантові мережі можуть створити абсолютно захищені канали комунікації між критично важливими об'єктами. Кіберфізичні системи безпеки інтегрують цифрові та фізичні компоненти для забезпечення комплексного багаторівневого захисту критичної інфраструктури від різноманітних типів гібридних загроз. Ці системи поєднують сенсорні мережі для моніторингу фізичного стану об'єктів, системи управління технологічними процесами, засоби

кіберзахисту, системи штучного інтелекту для аналізу загроз та автоматичного реагування.

Інтеграція фізичного та кіберзахисту дозволяє виявляти комбіновані атаки, коли кіберзасоби використовуються для здійснення фізичного впливу на об'єкти, або фізичні методи застосовуються для компрометації кіберсистем. Системи можуть автоматично адаптувати рівень захисту відповідно до поточного рівня загроз, перерозподіляти ресурси між різними напрямами захисту.

Прогностичне обслуговування на основі аналізу даних сенсорів дозволяє запобігати відмовам критично важливого обладнання, що може бути використане противником для дестабілізації роботи об'єктів. Системи можуть моделювати каскадні ефекти від пошкодження окремих компонентів та автоматично активувати резервні системи.

Міжнародна співпраця в рамках управління ризиками гібридних загроз є абсолютно необхідною складовою ефективної системи національної безпеки в умовах глобалізованого та взаємопов'язаного світу, оскільки гібридні загрози за своєю природою часто мають транснаціональний характер, використовують глобальні інформаційні мережі, міжнародні фінансові системи, транскордонні ланцюги постачання та не можуть бути ефективно подолані зусиллями лише окремої держави без координації з міжнародними партнерами та союзниками. Стратегічне партнерство з НАТО у сфері протидії гібридним загрозам базується на фундаментальних принципах колективної безпеки, взаємної підтримки, солідарності союзників та спільної відповідальності за безпеку євро-атлантичного простору. НАТО має стратегію своєї ролі у протидії гібридній війні та готове захищати Альянс і всіх Союзників від будь-яких загроз, чи то звичайних, чи гібридних. Альянс зміцнює свою координацію з партнерами, включаючи Європейський Союз, у зусиллях протидії гібридним загрозам через спеціалізовані структури, включаючи Об'єднане управління розвідки та безпеки НАТО, яке має

підрозділ гібридного аналізу, що допомагає покращити ситуаційну обізнаність та координацію зусиль [9].

Співпраця з НАТО включає участь у спільних аналітичних програмах для вивчення нових типів гібридних загроз, обмін розвідувальною інформацією та найкращими практиками протидії, участь у багатонаціональних навчаннях та тренуваннях з відпрацювання дій в умовах гібридних загроз, доступ до спеціалізованих програм підготовки фахівців у сфері протидії гібридним загрозам. Україна також бере участь у роботі Європейського центру передового досвіду з протидії гібридним загрозам у Гельсінкі, який відіграє унікальну роль у консолідації зусиль союзників та партнерів.

Альянс активно протидіє дезінформації та пропаганді не більшою пропагандою, а фактами - онлайн, в ефірі та друкованих виданнях, що є важливим принципом демократичної протидії інформаційним загрозам. НАТО також проводить спільні навчання сил спеціальних операцій для тестування їх здатності працювати разом через серію складних сценаріїв боротьби з тероризмом та гібридною війною.

Партнерство з Європейським Союзом у протидії гібридним загрозам має особливе значення для України в контексті європейської інтеграції та прагнення до членства в ЄС. ЄС та НАТО посилили свою співпрацю у протидії гібридним загрозам з особливим акцентом на кіберзахисті, підвищенні стійкості критичної інфраструктури, стратегічних комунікаціях, покращенні ситуаційної обізнаності через обмін розвідувальною інформацією та проведенні спільних навчань і тренувань.

ЄС розробив комплексну систему інструментів протидії гібридним загрозам, включаючи гібридні групи швидкого реагування, які є одним з інструментів у гібридному інструментарії ЄС для підтримки держав-членів, партнерських країн та місій і операцій CSDP під час протидії гібридним загрозам. У травні 2024 року Рада схвалила основи для практичного

створення гібридних груп швидкого реагування ЄС, що стало важливим кроком у розвитку спроможностей швидкого реагування на гібридні інциденти.

Співпраця включає також участь у програмах ЄС з підвищення стійкості до гібридних загроз, доступ до європейських центрів передового досвіду та дослідницьких програм, участь у спільних проектах з розвитку технологій протидії гібридним загрозам, інтеграцію з європейськими системами раннього попередження та обміну інформацією про загрози.

ЄС також має у своєму розпорядженні механізми управління кризами, включаючи інтегровані політичні механізми реагування на кризи (IPCR) Ради для підтримки координованих дій у відповідь на великі, складні кризи та обміну інформацією, наприклад, щодо втручання у вибори до ЄС 2024 року.

Двостороння співпраця з ключовими стратегічними партнерами дозволяє поглибити взаємодію у специфічних напрямах протидії гібридним загрозам та отримати доступ до унікальних технологій, методик та досвіду. Співпраця зі Сполученими Штатами Америки включає інтенсивний обмін розвідувальною інформацією про гібридні загрози, технічну допомогу у розвитку національних кіберспроможностей та засобів протидії дезінформації, підготовку українських фахівців у спеціалізованих американських навчальних закладах та центрах, доступ до передових американських технологій кіберзахисту та аналізу інформації [73].

Співпраця з провідними європейськими країнами, такими як Великобританія, Франція, Німеччина, забезпечує доступ до європейського досвіду протидії російським гібридним загрозам, передових технологічних рішень у сфері кіберзахисту та боротьби з дезінформацією, участь у спільних дослідницьких проектах та програмах розвитку спроможностей, обмін кращими практиками законодавчого регулювання питань гібридних загроз. Регіональна співпраця з країнами, що стикаються з аналогічними гібридними загрозами з боку росії, дозволяє координувати зусилля та обмінюватися

практичним досвідом протидії конкретним типам загроз. Особливо важливою є співпраця з країнами Балтії (Естонією, Латвією, Литвою), Польщею, Фінляндією та іншими державами, які знаходяться на передовій протистояння з російськими гібридними загрозами та мають значний досвід їх виявлення та нейтралізації.

Балтійські країни, Польща та Німеччина стикаються з найвищим ризиком російських гібридних загроз, включаючи саботаж критичної інфраструктури, особливо підводних кабелів у Балтійському морі, що робить регіональну координацію критично важливою. Створення регіональних центрів протидії гібридним загрозам, спільних систем моніторингу та раннього попередження, координованих планів реагування на транскордонні інциденти може значно підвищити ефективність колективних зусиль.

Участь у міжнародних ініціативах та проектах дослідження гібридних загроз сприяє розвитку теоретичної бази та практичних інструментів протидії через залучення до передових наукових досліджень, співпрацю з провідними академічними установами, аналітичними центрами та міжнародними організаціями, що забезпечує доступ до новітніх розробок у цій динамічно розвиваючійся сфері безпеки. Україна активно співпрацює з такими міжнародними структурами як Європейський центр передового досвіду з протидії гібридним загрозам, HATO StratCom Centre of Excellence, різноманітними дослідницькими центрами [161].

Стандартизація підходів та процедур протидії гібридним загрозам на міжнародному рівні сприяє значному покращенню взаємосумісності національних систем, підвищенню ефективності координованих дій союзників та партнерів, створенню спільної термінологічної бази та методологічних підходів. Розробка спільних індикаторів загроз, уніфікованих процедур обміну розвідувальною та аналітичною інформацією, стандартизованих протоколів реагування на інциденти дозволяє створити більш ефективну та швидкодіючу систему колективної безпеки.

Міжнародні стандарти та сертифікація систем протидії гібридним загрозам забезпечують якість та надійність технологічних рішень, сприяють розвитку міжнародної кооперації у сфері безпекових технологій, створюють довіру між партнерами щодо ефективності застосовуваних засобів протидії.

Правове забезпечення міжнародної співпраці потребує розробки та підписання відповідних двосторонніх та багатосторонніх угод, меморандумів про взаєморозуміння, протоколів співпраці, які детально регламентували б процедури обміну розвідувальною та оперативною інформацією з урахуванням вимог національної безпеки, механізми надання взаємної технічної та оперативної допомоги в умовах кризових ситуацій, координації спільних дій у відповідь на транскордонні гібридні загрози, правового супроводу спільних операцій та навчань [30].

Особлива увага має бути приділена забезпеченню оптимального балансу між необхідністю максимально ефективної міжнародної співпраці та критично важливими вимогами захисту національних інтересів, державної таємниці, суверенітету у прийнятті ключових рішень. Правове регулювання має також передбачати механізми вирішення можливих спорів та конфліктів інтересів між партнерами, процедури припинення співпраці у разі зміни геополітичних умов.

Моніторинг та оцінка ефективності системи інтегрованого управління ризиками гібридних загроз є критично важливими компонентами для забезпечення її постійного вдосконалення, адаптації до нових типів викликів та загроз, оптимізації використання обмежених ресурсів та підвищення результативності всіх заходів протидії. Ефективна система моніторингу має забезпечувати безперервне відстеження широкого спектру ключових показників ефективності та своєчасне виявлення проблемних областей, які потребують корекції або додаткової уваги.

Комплексна система ключових показників ефективності (KPI) включає як кількісні, так і якісні індикатори, що всебічно відображають різні аспекти

функціонування системи управління ризиками та дозволяють об'єктивно оцінити її продуктивність. Кількісні показники можуть включати середній час виявлення різних типів гібридних загроз від моменту їх ініціації до ідентифікації системою моніторингу, швидкість активації механізмів реагування на виявлені інциденти, кількість успішно виявлених та нейтралізованих загроз різних категорій, рівень координації та синхронізації дій між різними відомствами та структурами, відсоток виконання планових завдань у встановлені терміни.

Якісні показники стосуються більш складних аспектів функціонування системи, включаючи адекватність та пропорційність реагування на різні типи загроз, ступінь задоволення ключових стейкхолдерів якістю протидії гібридним загрозам, рівень довіри населення до ефективності національної системи безпеки, оцінку міжнародними партнерами спроможностей України у сфері протидії гібридним загрозам, якість міжвідомчої координації та співпраці.

Система індикаторів раннього попередження дозволяє виявляти негативні тенденції у функціонуванні системи до того, як вони призведуть до серйозних проблем. Ці індикатори можуть включати зростання часу реагування на інциденти, збільшення кількості помилкових спрацьовувань системи виявлення загроз, погіршення якості міжвідомчої координації, зниження морального стану персоналу, збільшення плинності кадрів у ключових підрозділах.

Регулярні незалежні аудити та всебічні оцінки системи мають проводитися кваліфікованими зовнішніми експертами для забезпечення максимальної об'єктивності та неупередженості оцінок, виявлення прихованих проблем та недоліків, які можуть бути не помітні для внутрішніх спостерігачів. Ці комплексні оцінки повинні включати детальний аналіз структурних компонентів системи та їх взаємодії, ефективності процесів та процедур протидії загрозам, адекватності технологічного забезпечення

сучасним викликам, професійного рівня кадрового потенціалу та його відповідності складності завдань, загальної результативності діяльності системи у досягненні поставлених цілей.

Особлива увага у процесі аудиту має бути приділена виявленню системних недоліків та критичних вузьких місць, які можуть значно знизити загальну ефективність протидії гібридним загрозам, аналізу причин виникнення виявлених проблем, оцінці потенційних ризиків від їх нерозв'язання, розробці конкретних рекомендацій щодо усунення недоліків. Механізми систематичного зворотного зв'язку забезпечують постійний двосторонній обмін критично важливою інформацією між різними рівнями та функціональними компонентами системи управління ризиками, що дозволяє своєчасно виявляти проблеми та корегувати діяльність. Ці механізми включають регулярні деталізовані звіти про поточний стан системи та динаміку ключових показників, результати реагування на конкретні інциденти з аналізом успіхів та недоліків, конструктивні пропозиції від практиків щодо вдосконалення наявних процедур та інструментів протидії.

Важливим елементом системи зворотного зв'язку є створення ефективних каналів для отримання інформації та пропозицій від широкої громадськості, приватного сектору, академічного середовища, міжнародних партнерів. Це може включати регулярні опитування громадської думки, консультації з експертним співтовариством, семінари та конференції з обміну досвідом.

Всеохоплююча система безперервного навчання та професійного розвитку забезпечує постійне оновлення знань, навичок та компетентностей персоналу системи управління ризиками відповідно до динамічної еволюції гібридних загроз та появи нових методів протидії. Це включає регулярні спеціалізовані тренування та багатопрофільні навчання для різних категорій персоналу, активну участь у престижних міжнародних програмах обміну

досвідом та стажування у провідних безпекових установах партнерських країн, систематичне проведення реалістичних навчальних симуляцій та складних сценарних ігор для відпрацювання дій в умовах різноманітних кризових ситуацій.

Особливо важливим є розвиток прогресивної організаційної культури навчання на власних помилках та ретельного аналізу невдач для запобігання їх повторенню в майбутньому, заохочення ініціативності та творчого підходу до вирішення складних завдань, стимулювання обміну досвідом між різними підрозділами та відомствами.

Адаптивні механізми системи забезпечують її здатність до швидкого та ефективного реагування на кардинальні зміни у характері, інтенсивності та методах реалізації гібридних загроз, що є критично важливим в умовах постійної еволюції безпекового середовища. Ці складні механізми включають формалізовані процедури регулярного перегляду та систематичного оновлення ключових стратегічних документів з урахуванням нових викликів, гнучкі підходи до корекції організаційних структур та перерозподілу функціональних обов'язків відповідно до змінених пріоритетів, планомірну модернізацію технологічного забезпечення з урахуванням появи нових загроз та інноваційних засобів протидії.

Важливим принципом адаптивних механізмів є збереження оптимального балансу між необхідною гнучкістю системи для швидкого реагування на зміни та її базовою стабільністю і надійністю для забезпечення безперервності критично важливих функцій безпеки. Система має бути здатною до еволюційних змін без втрати основних спроможностей та накопиченого досвіду.

Інноваційні підходи до управління ризиками передбачають систематичне експериментування з новітніми методами та передовими технологіями, пілотне тестування перспективних інноваційних рішень в контрольованих умовах та поступове масштабування найбільш успішних

практик на всю систему після підтвердження їх ефективності. Це дозволяє системі постійно залишатися на передовому краї розвитку у сфері протидії гібридним загрозам та максимально ефективно використовувати найновітні досягнення науки, техніки та управлінської думки.

Інноваційна діяльність має включати створення спеціалізованих підрозділів досліджень та розробок, співпрацю з провідними науковими установами та технологічними компаніями, участь у міжнародних інноваційних програмах та проектах, створення внутрішніх інноваційних конкурсів та стимулювання творчої ініціативи співробітників.

Система управління знаннями забезпечує накопичення, структуризацію, збереження та ефективне використання накопиченого досвіду протидії гібридним загрозам. Це включає створення баз знань з типовими сценаріями загроз та ефективними методами протидії, документування кращих практик та уроків, отриманих з аналізу інцидентів, розробку методичних рекомендацій та стандартних операційних процедур.

Важливою складовою є створення системи інституційної пам'яті, яка дозволяє зберігати критично важливий досвід навіть при ротації персоналу та організаційних змінах. Це включає формалізацію неявних знань експертів, створення систем наставництва та передачі досвіду, розробку навчальних матеріалів та кейсів на основі реальних подій.

Отже, модель інтегрованого управління ризиками національної безпеки в умовах гібридних загроз представляє собою складну багаторівневу систему, що органічно поєднує стратегічне довгострокове планування з оперативним реагуванням на поточні виклики, інноваційні технологічні рішення з перевіреними часом управлінськими підходами, національні спроможності з міжнародною співпрацею та партнерством. Успішна практична реалізація цієї комплексної моделі потребує скоординованих та послідовних зусиль усіх без винятку складових національної системи безпеки, постійного системного вдосконалення всіх елементів та процесів, безперервної адаптації до нових

викликів та загроз, що постійно еволюціонують [178].

Український практичний досвід формування та функціонування такої інтегрованої системи в умовах активної та масштабної російської агресії, що поєднує традиційні військові дії з широким спектром гібридних загроз, може стати надзвичайно важливим та цінним внеском у розвиток сучасної теорії та практики забезпечення національної безпеки, створення ефективних механізмів протидії гібридним загрозам у сучасному глобалізованому та взаємопов'язаному світі XXI століття [43].

3.3. Напрями вдосконалення механізмів координації та контролю у сфері національної безпеки

Система координації у сфері національної безпеки України характеризується складною багаторівневою архітектурою, яка сформувалася під впливом як внутрішніх потреб держави, так і зовнішніх викликів, особливо після 2014 року. Центральним елементом цієї системи виступає Рада національної безпеки і оборони України (РНБО), яка згідно зі статтею 107 Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України. Однак аналіз практичного функціонування РНБО свідчить про низку системних проблем, які суттєво знижують ефективність координаційних процесів.

Правова основа діяльності РНБО визначається Законом України "Про Раду національної безпеки і оборони України", який встановлює її статус, повноваження та порядок діяльності. Водночас аналіз нормативно-правового забезпечення виявляє значні прогалини у визначенні конкретних механізмів координації між різними відомствами та структурами сектору безпеки і оборони. Відсутність чітко регламентованих процедур координації призводить до дублювання функцій, неефективного використання ресурсів та зниження оперативності прийняття управлінських рішень [122].

Структурний аналіз координаційних механізмів демонструє фрагментованість системи управління національною безпекою. Поряд з РНБО функціонують численні міжвідомчі комісії, робочі групи та координаційні ради, створені як на постійній, так і на тимчасовій основі. Такий підхід, хоча і забезпечує певну гнучкість у вирішенні специфічних завдань, створює проблему розмитості відповідальності та ускладнює контроль за виконанням прийнятих рішень. Аналіз показує, що станом на 2025 рік функціонує понад 40 різних координаційних структур у сфері національної безпеки, що створює надмірну бюрократизацію та знижує ефективність управлінських процесів [143].

Особливо гостро проявляються проблеми координації у сфері інформаційного обміну між структурами сектору безпеки і оборони. Відсутність єдиної інформаційно-аналітичної системи призводить до інформаційних розривів, дублювання аналітичної роботи та неповноти інформаційної картини для прийняття стратегічних рішень. Це особливо критично в умовах гібридних загроз, коли швидкість та якість інформаційного обміну стають вирішальними факторами ефективності системи національної безпеки. Існуючі інформаційні системи різних відомств працюють ізольовано, що призводить до затримок в обробці критично важливої інформації на 24-48 годин.

Аналіз механізмів планування у сфері національної безпеки виявляє недостатню узгодженість між стратегічним, оперативним та тактичним рівнями планування. Стратегія національної безпеки України, оновлена у 2020 році та переглянута у 2023 році з урахуванням воєнного стану, визначає загальні напрями забезпечення національної безпеки, однак механізми її деталізації на рівні галузевих стратегій та оперативних планів потребують суттєвого вдосконалення. Відсутність єдиної методології планування призводить до неузгодженості цілей та завдань різних відомств, що знижує синергетичний ефект їх діяльності [129].

Структуру циклу моніторингу та оцінки ефективності реформування сектору безпеки і оборони наведено на рис. 3.2.

Етап циклу	Суб'єкти	Зміст діяльності
1. ЗБІР ДАНИХ	НКЦБ, МО, СБУ, МВС, ДПС, аналітичні підрозділи	Збір статистичних, оперативних та аналітичних даних за індикаторами усіх сфер безпеки
2. ІНДИКАТИВНА ОЦІНКА	Аналітичний департамент НКЦБ	Розрахунок інтегрального індексу загроз; присвоєння рівнів (низький / середній / високий / критичний)
3. АНАЛІЗ ВІДХИЛЕНЬ	РНБО, НКЦБ, Генштаб	Порівняння фактичних показників з плановими; виявлення проблемних зон реформування
4. КОРИГУВАННЯ ПЛАНІВ	КМУ, МО, СБУ, суб'єкти СБО	Оновлення планів реформ; перерозподіл ресурсів; прийняття управлінських рішень
5. ЗВІТНІСТЬ І КОНТРОЛЬ	ВРУ, Рахункова палата, РНБО, громадський аудит	Підготовка звітів; парламентський та громадський контроль; публікація результатів
↺ ЗАМКНЕНИЙ ЦИКЛ: після етапу 5 — повернення до етапу 1 (наступний звітний період)		

Рис. 3.2. Система моніторингу та оцінки ефективності реформування сектору безпеки і оборони

Джерело: розроблено автором

Кадрова складова координаційних механізмів також характеризується низкою проблем. Відсутність спеціалізованої підготовки кадрів для координаційної діяльності у сфері національної безпеки призводить до недостатнього розуміння специфіки міжвідомчої взаємодії та неефективного використання координаційного потенціалу. Крім того, високий рівень плинності кадрів у координаційних структурах негативно впливає на накопичення інституційної пам'яті та розвиток професійних компетенцій.

Технологічна складова існуючих координаційних механізмів потребує кардинальної модернізації. Використання застарілих інформаційних систем та відсутність інтегрованих цифрових платформ для координації знижує

оперативність та якість управлінських рішень. Особливо це стосується систем раннього попередження та реагування на загрози національній безпеці, де швидкість обробки інформації та координації дій є критично важливою. Фінансова складова координаційних механізмів характеризується недостатністю ресурсного забезпечення координаційних структур та відсутністю прозорих механізмів розподілу фінансування між різними відомствами сектору безпеки і оборони.

Системні проблеми міжвідомчої взаємодії у сфері національної безпеки України мають глибокі інституційні корені та значно знижують ефективність функціонування всього сектору безпеки і оборони. Основною причиною цих проблем є відсутність цілісної концепції міжвідомчої координації, яка б ґрунтувалася на чітко визначених принципах, процедурах та механізмах відповідальності [74]. На основі проведеної інтегральної оцінки рівень ефективності міжвідомчої взаємодії у сфері національної безпеки, за авторськими розрахунками, істотно нижчий за потенційно можливий, що призводить до значних втрат ресурсів та зниження якості виконання завдань.

Дублювання функцій між різними відомствами становить одну з найгостріших проблем сучасної системи національної безпеки. Аналіз розподілу повноважень між Службою безпеки України, Національною поліцією, Державною прикордонною службою, Національною гвардією та іншими структурами виявляє значні зони перетину у їх компетенції. Особливо це стосується сфери протидії тероризму, організованій злочинності та кіберзагрозам , де одні й ті ж завдання можуть одночасно виконуватися кількома відомствами без належної координації та розподілу відповідальності. Такий стан речей призводить до марнотратства ресурсів, точний обсяг яких потребує окремого фінансового аудиту з боку Рахункової палати України [143].

Відомча замкненість та корпоративні інтереси створюють додаткові бар'єри для ефективної міжвідомчої взаємодії. Кожне відомство прагне

зберегти та розширити власні повноваження, що призводить до конкуренції замість співпраці. Це особливо проявляється у сфері розвідувальної діяльності, де паралельне функціонування різних розвідувальних служб без належної координації знижує якість розвідувальної інформації та створює ризики для національної безпеки. Відсутність єдиного координаційного центру для розвідувальної діяльності призводить до ситуацій, коли різні служби можуть працювати з одними й тими ж об'єктами, не знаючи про діяльність одна одної [94].

Нормативно-правова неузгодженість становить ще один критичний фактор, що перешкоджає ефективній міжвідомчій взаємодії. Відсутність єдиного підходу до регламентації процедур координації призводить до ситуацій, коли різні відомства керуються різними нормативними актами, що суперечать один одному або створюють можливості для різного тлумачення повноважень та відповідальності. Це особливо проблематично у сфері інформаційного обміну, де відсутність єдиних стандартів класифікації та обробки інформації створює перешкоди для оперативного обміну даними. Значна частина міжвідомчих конфліктів у сфері національної безпеки виникає саме через нормативно-правову неузгодженість, що підтверджується наведеними вище прикладами дублювання повноважень.

Технологічна несумісність інформаційних систем різних відомств створює значні перешкоди для оперативного обміну інформацією та координації дій. Кожне відомство розвиває власні інформаційні системи без урахування потреб міжвідомчої взаємодії, що призводить до створення інформаційних "островів" та знижує ефективність аналітичної роботи. Відсутність єдиних протоколів передачі даних та стандартів інформаційної безпеки ускладнює створення інтегрованих аналітичних продуктів. Технологічна несумісність інформаційних систем відомств суттєво уповільнює прийняття рішень у кризових ситуаціях, створюючи інформаційні "острови", описані вище.

Кадрові проблеми значно впливають на якість міжвідомчої взаємодії. Відсутність спеціалізованої підготовки посадових осіб для роботи у міжвідомчих структурах призводить до недостатнього розуміння специфіки діяльності інших відомств та неефективного використання потенціалу координації. Крім того, різні підходи до кадрової політики у різних відомствах створюють бар'єри для ротації кадрів та обміну досвідом. Особливо гостро ця проблема проявляється на рівні середньої ланки управління, де відсутність міжвідомчих кар'єрних траєкторій знижує мотивацію до координаційної діяльності.

Фінансові механізми також створюють перешкоди для ефективної координації. Відсутність єдиного підходу до планування та розподілу ресурсів призводить до ситуацій, коли одні відомства мають надлишок ресурсів для виконання певних завдань, тоді як інші відчувають їх нестачу. Це особливо проблематично у сфері закупівель, де відсутність координації призводить до неефективного використання бюджетних коштів та дублювання витрат. Відсутність єдиної системи моніторингу та оцінки ефективності міжвідомчої взаємодії унеможливлює своєчасне виявлення проблем та корегування координаційних механізмів.

Аналіз європейських та НАТО моделей координації у сфері національної безпеки надає цінні уроки для вдосконалення української системи управління сектором безпеки і оборони. Досвід провідних європейських країн демонструє різноманітні підходи до організації координаційних механізмів, кожен з яких має свої переваги та особливості адаптації до національних умов. Особливого значення набуває вивчення цього досвіду в контексті європейської інтеграції України та процесу наближення до стандартів НАТО [145].

Французька модель координації характеризується централізованим підходом з потужною роллю Генерального секретаріату оборони та національної безпеки (SGDSN), який підпорядковується безпосередньо

Прем'єр-міністру. Ця структура забезпечує координацію між усіма міністерствами та відомствами у сфері національної безпеки, включаючи розробку міжвідомчих стратегій, координацію кризового реагування та управління інформаційними потоками. Особливістю французької моделі є створення спеціалізованих міжвідомчих комітетів для кожного напряму національної безпеки, що забезпечує як горизонтальну, так і вертикальну координацію. SGDSN координує діяльність понад 15 міністерств та відомств у сфері національної безпеки, використовуючи єдину методологію оцінки загроз та планування заходів протидії [91].

Німецька модель відзначається особливою увагою до парламентського контролю та громадянського нагляду за діяльністю силових структур. Федеральна рада безпеки (Bundessicherheitsrat) функціонує як координаційний орган на рівні уряду, тоді як Парламентська комісія з контролю за розвідувальними службами (PKGr) забезпечує демократичний нагляд за діяльністю спецслужб. Німецький досвід демонструє важливість інституційного балансу між ефективністю координації та демократичною підзвітністю. Особливістю німецької моделі є створення Об'єднаного центру протидії тероризму та екстремізму (GTAZ), який об'єднує представників усіх силових структур та забезпечує оперативний обмін інформацією в режимі реального часу.

Британська модель координації побудована навколо Комітету національної безпеки Кабінету міністрів (NSC), який очолює Прем'єр-міністр. Особливістю цієї моделі є створення об'єднаного Національного центру безпеки, який інтегрує аналітичні можливості різних відомств та забезпечує єдину інформаційну картину для прийняття рішень. Британський досвід також демонструє важливість створення спільних оперативних центрів для координації дій у кризових ситуаціях. Система COBR (Cabinet Office Briefing Rooms) забезпечує координацію урядової відповіді на національні надзвичайні ситуації та кризи, об'єднуючи представників усіх

релевантних відомств під керівництвом Прем'єр-міністра або його заступника [87].

Польська модель, особливо актуальна для України з огляду на схожі геополітичні виклики, характеризується створенням Ради міністрів з питань національної безпеки та оборони як основного координаційного органу. Польський досвід демонструє важливість інтеграції цивільних та військових структур у єдиній системі національної безпеки. Особливістю польської моделі є створення Урядового центру безпеки (RCB), який функціонує як оперативний координаційний орган для управління кризовими ситуаціями та забезпечує цілодобове моніторингу загроз національній безпеці. Польща також розробила унікальну систему територіальної оборони, яка інтегрує регулярні збройні сили з цивільними структурами на місцевому рівні [81].

Естонська модель цифрової координації національної безпеки є особливо цінною для України в контексті цифровізації державного управління. Естонія створила єдину цифрову платформу національної безпеки, яка об'єднує всі силові структури та забезпечує автоматизований обмін інформацією. Ця система включає модулі раннього попередження, кризового реагування та моніторингу загроз у кіберпросторі. Естонський досвід демонструє, що наскрізна цифровізація координаційних процесів здатна суттєво підвищити ефективність міжвідомчої взаємодії за рахунок автоматизованого обміну даними та скорочення часу узгодження рішень [161].

Досвід НАТО у сфері координації та контролю базується на принципах колективної безпеки та стандартизації процедур. Організація розробила детальні стандарти координації між національними структурами безпеки та оборони країн-членів, які включають уніфіковані процедури обміну інформацією, спільного планування та кризового реагування. Особливо важливим є досвід НАТО у створенні інтегрованих командних структур, які забезпечують ефективну координацію між різними видами збройних сил та

цивільними структурами. Стандарти НАТО також передбачають створення національних координаційних центрів, які забезпечують зв'язок між національними структурами безпеки та командними структурами Альянсу [177].

На основі аналізу проблем української системи координації та міжнародного досвіду можна сформулювати комплекс рекомендацій щодо інституційних та організаційних змін у сфері національної безпеки. Першочерговою рекомендацією є створення єдиного Національного координаційного центру безпеки (НКЦБ) як постійно діючого органу при РНБО, який би забезпечував цілодобову координацію діяльності всіх структур сектору безпеки і оборони. НКЦБ повинен мати статус самостійної державної установи з власним бюджетом та штатом висококваліфікованих фахівців з координації національної безпеки [58].

Структура НКЦБ повинна включати декілька функціональних підрозділів: аналітично-інформаційний центр, який би забезпечував збір, обробку та аналіз інформації про загрози національній безпеці з усіх доступних джерел; центр стратегічного планування, відповідальний за розробку міжвідомчих планів та програм у сфері національної безпеки; оперативний центр кризового реагування, який би координував дії різних відомств у кризових ситуаціях; центр моніторингу та оцінки, що здійснював би постійний контроль за виконанням рішень РНБО та ефективністю міжвідомчої взаємодії [143].

Важливою рекомендацією є реформування системи міжвідомчих комісій та робочих груп з метою їх оптимізації та підвищення ефективності. Пропонується скорочення кількості координаційних структур до 15-20 основних комісій, кожна з яких мала б чітко визначені повноваження, терміни діяльності та критерії оцінки ефективності. Кожна міжвідомча комісія повинна мати секретаріат у складі НКЦБ, що забезпечить координацію їх діяльності та уникнення дублювання функцій.

Необхідним є створення єдиної інформаційно-аналітичної системи національної безпеки, яка би інтегрувала інформаційні ресурси всіх структур сектору безпеки і оборони. Ця система повинна базуватися на сучасних технологіях штучного інтелекту та машинного навчання, що дозволить автоматизувати процеси аналізу загроз та прогнозування розвитку ситуації. Система повинна включати модулі: автоматизованого збору та обробки інформації з відкритих та закритих джерел; аналізу та оцінки загроз національній безпеці; моделювання сценаріїв розвитку ситуації; підтримки прийняття рішень у кризових ситуаціях [169].

Рекомендується впровадження єдиної системи кадрової підготовки для координаційної діяльності у сфері національної безпеки. Пропонується створення Національної академії координації безпеки як спеціалізованого навчального закладу, який би забезпечував підготовку, перепідготовку та підвищення кваліфікації кадрів для координаційних структур. Академія повинна розробити спеціальні освітні програми з міжвідомчої координації, кризового управління, стратегічного планування у сфері національної безпеки [96].

Важливою організаційною зміною є впровадження системи ротації кадрів між різними відомствами сектору безпеки і оборони. Це дозволить сформувати корпус фахівців, які розуміють специфіку діяльності різних структур та здатні забезпечити ефективну міжвідомчу координацію. Система ротації повинна передбачати обов'язкове проходження службовцями середньої та вищої ланки стажування в інших відомствах сектору безпеки і оборони терміном не менше 6 місяців протягом проходження служби. Механізми парламентського та громадського контролю у сфері національної безпеки потребують суттєвого вдосконалення з метою забезпечення демократичної підзвітності силових структур при збереженні необхідного рівня секретності їх діяльності. Парламентський контроль повинен здійснюватися через спеціалізовані комітети Верховної Ради України, які

мають доступ до класифікованої інформації та право проведення закритих слухань з питань національної безпеки [177].

Рекомендується створення єдиного Комітету Верховної Ради з питань національної безпеки, оборони та розвідки, який би об'єднав функції контролю за всіма структурами сектору безпеки і оборони. Цей комітет повинен мати право: отримувати інформацію про діяльність силових структур у визначених законом межах; проводити слухання з питань національної безпеки; вносити рекомендації щодо вдосконалення законодавства у сфері національної безпеки; здійснювати контроль за використанням бюджетних коштів структурами сектору безпеки і оборони [112].

Важливим елементом парламентського контролю є створення посади Уповноваженого Верховної Ради з питань контролю за діяльністю силових структур, який би здійснював постійний моніторинг дотримання прав людини та законності у діяльності структур сектору безпеки і оборони. Уповноважений повинен мати право безперешкодного доступу до структур сектору безпеки і оборони, проведення розслідувань порушень прав людини та подання рекомендацій щодо усунення виявлених порушень.

Громадський контроль повинен здійснюватися через створення Громадської ради з питань національної безпеки при РНБО, до складу якої входили б представники громадських організацій, експертного середовища, незалежних аналітичних центрів. Громадська рада повинна мати право: отримувати інформацію про основні напрями політики національної безпеки; брати участь у громадських слуханнях з питань національної безпеки; подавати пропозиції щодо вдосконалення політики національної безпеки; здійснювати громадський моніторинг реформ у секторі безпеки і оборони.

Рекомендується створення мережі регіональних громадських рад з питань безпеки при обласних державних адміністраціях, які би забезпечували громадський контроль за діяльністю територіальних підрозділів силових

структур. Ці ради повинні включати представників місцевих громадських організацій, бізнес-спільноти, академічних кіл та мати право проведення громадських слухань з питань безпеки на регіональному рівні [177].

Важливим механізмом громадського контролю є забезпечення прозорості діяльності структур сектору безпеки і оборони через регулярне оприлюднення звітів про їх діяльність у межах, що не суперечать вимогам секретності. Кожна структура повинна щорічно публікувати відкритий звіт про свою діяльність, який включає інформацію про основні результати роботи, використання бюджетних коштів, заходи з дотримання прав людини [180].

Етапи впровадження рекомендацій повинні бути розділені на три фази з чіткими термінами та критеріями оцінки ефективності. Перша фаза (2025-2026 роки) передбачає створення нормативно-правової бази для функціонування нової системи координації, включаючи прийняття Закону України "Про координацію у сфері національної безпеки", розробку положень про НКЦБ, внесення змін до законодавства про парламентський та громадський контроль. На цьому етапі також повинно відбутися створення організаційної структури НКЦБ та початок розробки єдиної інформаційно-аналітичної системи [104].

Друга фаза (2026-2027 роки) включає повноцінне запуск діяльності НКЦБ, впровадження єдиної інформаційно-аналітичної системи, початок функціонування Національної академії координації безпеки та запуск системи ротації кадрів. На цьому етапі також повинні бути створені нові механізми парламентського та громадського контролю, включаючи посаду Уповноваженого Верховної Ради та Громадську раду при РНБО.

Третя фаза (2027-2028 роки) передбачає повну інтеграцію всіх елементів нової системи координації, оцінку її ефективності та внесення необхідних корегувань. На цьому етапі повинна відбутися остаточна оптимізація міжвідомчих координаційних структур та досягнення повної

функціональної сумісності інформаційних систем різних відомств.

Автором пропонуються такі орієнтовні цільові показники ефективності впровадження рекомендацій, визначені на основі порівняльного аналізу польського та естонського досвіду реформування координаційних систем: зменшення часу прийняття координаційних рішень — на 40-50%; скорочення дублювання функцій — на 70-80%; підвищення рівня інформаційного обміну між структурами сектору безпеки і оборони на 60-70%; зменшення кількості міжвідомчих конфліктів на 50-60%; підвищення рівня громадської довіри до структур сектору безпеки і оборони на 30-40%.

Фінансування впровадження рекомендацій повинно здійснюватися за рахунок державного бюджету з можливим залученням міжнародної технічної допомоги. Орієнтовна вартість впровадження запропонованих рекомендацій, за попередньою авторською оцінкою, становить 2-3 млрд грн протягом трьох років (менше 5% річного бюджету сектору безпеки і оборони згідно із Законом України «Про Державний бюджет України на 2026 рік»). Економічний ефект від впровадження рекомендацій, завдяки підвищенню ефективності координації та зменшенню дублювання функцій, оцінюється у 5-7 млрд гривень щорічно, що забезпечує окупність інвестицій протягом першого року повноцінного функціонування нової системи [9].

Висновки до розділу 3

У третьому розділі дисертаційного дослідження здійснено комплексний аналіз механізмів державного управління реформуванням сектору безпеки і оборони України та розроблено науково обґрунтовані рекомендації щодо їх вдосконалення в умовах збройної агресії. Результати дослідження дозволяють сформулювати низку принципово важливих висновків, що мають як теоретичне, так і практичне значення для подальшого розвитку системи національної безпеки України.

Концептуальні засади оптимізації системи управління сектором

безпеки і оборони, розроблені у підрозділі 3.1, базуються на системному підході до реформування та враховують специфіку гібридних загроз сучасності. Встановлено, що ефективна система управління сектором безпеки і оборони повинна ґрунтуватися на принципах цілісності, адаптивності, прозорості та демократичної підзвітності. Особливого значення набуває принцип інтегрованого управління, який передбачає координацію зусиль всіх структур сектору безпеки і оборони для досягнення спільних цілей національної безпеки.

Дослідження показало, що традиційні підходи до управління сектором безпеки і оборони, які базувалися на ієрархічних структурах та вертикальній координації, не відповідають викликам сучасних гібридних загроз. Гібридні загрози характеризуються мультидоменністю , асиметричністю та динамічністю, що вимагає створення гнучких та адаптивних механізмів управління. Концептуальною основою такої системи управління має стати мережева модель координації, яка забезпечує горизонтальну взаємодію між різними структурами та дозволяє швидко реагувати на зміни у характері загроз.

Аналіз зарубіжного досвіду засвідчив ефективність інтегрованих підходів до управління національною безпекою, які успішно застосовуються у країнах НАТО та Європейського Союзу. Особливо цінним є досвід створення об'єднаних координаційних центрів, які забезпечують цілодобовий моніторинг загроз та координацію відповідних заходів. Адаптація цього досвіду до українських умов дозволить підвищити ефективність управління сектором безпеки і оборони та забезпечити більш швидке реагування на виникаючі загрози.

Модель інтегрованого управління ризиками національної безпеки в умовах гібридних загроз, представлена у підрозділі 3.2, являє собою комплексну систему, яка об'єднує процеси ідентифікації, оцінки, моніторингу та мінімізації ризиків у єдиному управлінському циклі. Ця модель базується

на концепції превентивного управління, яка передбачає випередження загроз через раннє виявлення та нейтралізацію ризиків на стадії їх формування.

Основою моделі є створення єдиної системи управління ризиками, яка інтегрує аналітичні можливості всіх структур сектору безпеки і оборони та забезпечує комплексну оцінку загроз у різних доменах безпеки. Модель передбачає використання сучасних технологій штучного інтелекту та машинного навчання для автоматизації процесів аналізу загроз та прогнозування їх розвитку. Це дозволяє суттєво підвищити швидкість та точність оцінки ризиків, що є критично важливим в умовах динамічних гібридних загроз.

Важливою складовою моделі є система раннього попередження, яка забезпечує своєчасне виявлення ознак формування загроз та активацію відповідних механізмів реагування. Система базується на комплексному моніторингу індикаторів безпеки у різних сферах та використанні алгоритмів машинного навчання для виявлення аномалій та трендів, що можуть свідчити про формування загроз.

Модель також передбачає створення адаптивних механізмів реагування, які дозволяють швидко корегувати стратегії та тактики протидії загрозам залежно від зміни їх характеру. Це особливо важливо в умовах гібридних загроз, які можуть швидко еволюціонувати та змінювати свої прояви.

Рекомендації щодо вдосконалення механізмів координації та контролю у сфері національної безпеки, сформульовані у підрозділі 3.3, базуються на глибокому аналізі існуючих проблем української системи та кращих світових практик. Основною рекомендацією є створення єдиного Національного координаційного центру безпеки (НКЦБ) як постійно діючого органу при РНБО, який забезпечуватиме цілодобову координацію діяльності всіх структур сектору безпеки і оборони.

НКЦБ повинен стати центральним елементом нової архітектури

управління національною безпекою, забезпечуючи інтеграцію інформаційних потоків, координацію планування та оперативне управління в кризових ситуаціях. Створення такого центру дозволить ліквідувати існуючу фрагментованість системи координації та забезпечити єдине управління національною безпекою.

Важливою рекомендацією є впровадження єдиної інформаційно-аналітичної системи національної безпеки, яка інтегруватиме інформаційні ресурси всіх структур сектору безпеки і оборони. Ця система повинна базуватися на сучасних технологіях та забезпечувати автоматизацію процесів збору, обробки та аналізу інформації про загрози національній безпеці [169].

Система кадрового забезпечення координаційної діяльності також потребує кардинального реформування. Рекомендується створення спеціалізованої системи підготовки кадрів для координаційних структур та впровадження механізмів ротації між різними відомствами сектору безпеки і оборони. Це дозволить сформувати корпус висококваліфікованих фахівців, здатних забезпечити ефективну міжвідомчу координацію.

Механізми парламентського та громадського контролю потребують вдосконалення з метою забезпечення демократичної підзвітності силових структур при збереженні необхідного рівня секретності їх діяльності. Рекомендується створення єдиного парламентського комітету з питань національної безпеки та посади Уповноваженого Верховної Ради з контролю за діяльністю силових структур.

Наукова новизна результатів дослідження полягає у комплексному підході до вирішення проблеми вдосконалення механізмів державного управління сектором безпеки і оборони в умовах гібридних загроз. Вперше у вітчизняній науці державного управління розроблено цілісну концепцію інтегрованого управління ризиками національної безпеки, яка враховує специфіку сучасних гібридних загроз та базується на принципах системного підходу.

Теоретичним внеском дослідження є розвиток концептуальних засад оптимізації системи управління сектором безпеки і оборони через запровадження мережевої моделі координації та принципів адаптивного управління. Запропонована модель інтегрованого управління ризиками національної безпеки представляє собою новий підхід до організації управлінських процесів у сфері національної безпеки, який дозволяє ефективно протидіяти динамічним та мультидоменним загрозам сучасності.

Методологічним внеском є розробка комплексної системи оцінки ефективності механізмів координації у сфері національної безпеки, яка включає як кількісні, так і якісні індикатори та може бути використана для моніторингу результативності реформ сектору безпеки і оборони.

Практична значущість результатів дослідження полягає у можливості їх безпосереднього використання для вдосконалення системи державного управління сектором безпеки і оборони України. Розроблені рекомендації мають конкретний характер та включають детальні механізми їх впровадження з визначенням термінів, ресурсів та критеріїв оцінки ефективності.

Запропонована концепція створення Національного координаційного центру безпеки може стати основою для розробки відповідного законодавства та практичних заходів з реорганізації системи координації у сфері національної безпеки. Модель інтегрованого управління ризиками може бути адаптована та впроваджена у діяльність існуючих структур сектору безпеки і оборони без кардинальної перебудови їх організаційної структури.

Рекомендації щодо вдосконалення механізмів парламентського та громадського контролю можуть бути використані для підготовки змін до чинного законодавства та створення нових інституційних механізмів демократичного нагляду за діяльністю силових структур.

Економічний ефект від впровадження запропонованих рекомендацій

оцінюється у 5-7 млрд гривень щорічно завдяки підвищенню ефективності координації та ліквідації дублювання функцій між різними структурами сектору безпеки і оборони. Соціальний ефект полягає у підвищенні рівня національної безпеки та зміцненні довіри громадян до державних інституцій.

Перспективи подальших досліджень пов'язані з деталізацією окремих аспектів запропонованих рекомендацій, зокрема розробкою технічних специфікацій для єдиної інформаційно-аналітичної системи національної безпеки, створенням детальних навчальних програм для підготовки кадрів координаційних структур, розробкою методик оцінки ефективності міжвідомчої взаємодії у різних сферах національної безпеки [117].

Важливим напрямом подальших досліджень є адаптація запропонованих механізмів до специфіки регіонального та місцевого рівнів управління національною безпекою, розробка моделей взаємодії центральних та територіальних структур сектору безпеки і оборони в умовах децентралізації державного управління.

Результати дослідження створюють теоретичну та методологічну основу для подальшого розвитку науки державного управління у сфері національної безпеки та можуть бути використані у навчальному процесі при підготовці фахівців з державного управління, національної безпеки та публічного адміністрування [72].

ВИСНОВКИ

Дисертаційне дослідження присвячене актуальній науковій проблемі вдосконалення механізмів державного управління реформуванням сектору безпеки і оборони України в умовах збройної агресії. Результати дослідження дозволяють сформулювати наступні висновки:

У процесі дослідження встановлено, що сучасні механізми державного управління сектором безпеки і оборони потребують кардинального переосмислення у зв'язку з трансформацією характеру загроз національній безпеці. Гібридні загрози XXI століття вимагають інтегрованого підходу до управління, що поєднує традиційні військові засоби з невійськовими інструментами протидії.

1. Узагальнено та систематизовано теоретичні засади механізмів державного управління у сфері національної безпеки та оборони. Теоретичною основою дослідження став синтез положень теорії державного управління, теорії національної безпеки, інституціональної теорії та концепції упереджувального управління, що дало змогу розкрити багатовимірний характер об'єкта управління — як у внутрішньому вимірі, так і в зовнішньому. Удосконалено теоретико-методологічні засади зазначених механізмів шляхом інтеграції принципів системного, адаптивного та упереджувального управління, що дозволяє гнучко реагувати на динамічні зміни безпекового середовища; на цій основі розроблено класифікацію механізмів державного управління за функціональним призначенням, характером впливу, ступенем формалізації та часовими рамками застосування, що дозволило системно впорядкувати понятійно-категоріальний апарат дослідження та закласти методологічну основу для подальшого емпіричного аналізу.

2. Узагальнено зарубіжний досвід формування систем управління сектором безпеки і оборони провідних держав – членів НАТО та

Європейського Союзу. На основі порівняльного аналізу американської, британської, польської та ізраїльської систем координації набула подальшого розвитку типологія моделей координації сектору безпеки і оборони провідних країн НАТО та ЄС за критерієм придатності до адаптації в умовах збройної агресії та обмеженості ресурсів воєнного часу. Встановлено, що ефективне управління реформами сектору ґрунтується на поєднанні трьох базових елементів: демократичного цивільного контролю, інституційної координації через єдиний центральний орган та системного стратегічного планування, водночас жодна з розглянутих моделей не придатна для прямого копіювання — адаптація кращих практик до українських умов потребує врахування специфіки гібридної війни, обмеженості ресурсів воєнного часу та збереження управлінської спроможності в умовах активних бойових дій, що й визначило напрям розробки авторської моделі.

3. Розроблено методичні засади застосування індикативного підходу до оцінки ризиків і загроз національній безпеці України. Сформовано систему індикаторів за основними сферами безпеки з визначенням порогових значень рівня загроз та відповідних джерел даних. Обґрунтовано доцільність застосування методу головних компонент для агрегування первинних показників в інтегральні індекси оцінки ризиків, що дозволяє уникнути статистичного дублювання й підвищити об'єктивність оцінки. Адаптовано науково-методичний інструментарій деліберaційного методу ранжування ризиків до умов оцінки загроз національній безпеці України з урахуванням специфіки гібридної війни, що набуло подальшого розвитку в межах концепції упереджувального державного управління, орієнтованої на завчасне виявлення загроз до моменту їх ескалації.

4. Удосконалено систему критеріїв оцінки ефективності чинної нормативно-правової бази та інституційної структури управління сектором безпеки і оборони, яка включає критерій забезпечення територіальної цілісності та суверенітету України, критерій внутрішньої безпеки держави,

критерій ефективності використання бюджетних ресурсів, критерій демократичного цивільного контролю та критерій адаптивності системи управління до змінюваних умов безпекового середовища, доповнену критеріями відповідності стандартам НАТО та ЄС (прозорість і підзвітність, професіоналізм, дотримання прав людини). На основі застосування цієї системи критеріїв проведено комплексний аналіз сучасного стану державного управління сектором безпеки і оборони України, який виявив системні недоліки: фрагментованість управлінських повноважень між органами сектору, недостатність аналітичних спроможностей для прогнозування загроз, слабкість інформаційно-комунікаційних систем міжвідомчого обміну, кадрові проблеми координаційних структур та недосконаліть правового регулювання. Встановлено, що чинна нормативно-правова база загалом відповідає базовим вимогам євроатлантичної інтеграції, однак практика її застосування істотно відстає від задекларованих стандартів: дублювання функцій між органами сектору безпеки і оборони спричиняє відчутні втрати бюджетних ресурсів, значна частина міжвідомчих конфліктів виникає через нормативно-правову неузгодженість, а технологічна несумісність інформаційних систем відомств уповільнює прийняття рішень у кризових ситуаціях. Отримані результати аналізу склали емпіричну основу для розроблення концептуальної моделі та практичних рекомендацій.

5. На основі аналізу європейського досвіду та українських реалій розроблено концептуальну модель оптимізації системи управління сектором безпеки і оборони. В основу моделі покладено принципи цілісності та системності, адаптивності до змінних умов безпекового середовища, демократичного цивільного контролю, міжвідомчої координації та інтеграції, а також прозорості й підзвітності перед суспільством. Модель передбачає трирівневу архітектуру управління поєднану механізмами горизонтальної та вертикальної інтеграції між суб'єктами сектору безпеки і оборони. Запропонована модель інтегрованого управління ризиками національної

безпеки включає п'ять функціональних модулів: ідентифікації та класифікації загроз, оцінки ризиків, планування та координації реагування, виконання контрзаходів, а також відновлення та адаптації, що в сукупності забезпечує замкнений цикл управління від раннього виявлення загрози до її нейтралізації та аналізу наслідків.

6. Обґрунтовано систему механізмів координації, контролю та моніторингу реформ у сфері безпеки і оборони, ключовим елементом якої визначено створення Національного координаційного центру безпеки (НКЦБ) при РНБО як єдиного органу координації всіх структур сектору безпеки і оборони, що включає аналітично-інформаційний центр, центр стратегічного планування, оперативний центр кризового реагування та центр моніторингу й оцінки. Запропоновано впровадження єдиної інформаційно-аналітичної системи національної безпеки на основі технологій штучного інтелекту та машинного навчання, що дозволить підвищити швидкість та якість прийняття управлінських рішень. Розроблено механізми вдосконалення парламентського та громадського контролю через створення єдиного Комітету Верховної Ради з питань національної безпеки та посади Уповноваженого з контролю за силовими структурами. Впровадження запропонованих рекомендацій передбачено здійснювати поетапно протягом 2025–2028 років: на першій фазі — формування нормативно-правової бази та організаційної структури НКЦБ, на другій — запуск єдиної інформаційно-аналітичної системи та нових механізмів контролю, на третій — повна інтеграція елементів системи з подальшою оцінкою її ефективності, що забезпечує керованість і поетапну верифікацію результатів реформи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ажажа М. А., Куртєв А. В. Компетентісний підхід та особливості його реалізації в системі підготовки кадрів державного управління та надання публічних послуг. Вісник Національного університету цивільного захисту України. 2024. Вип. 1(20). С. 256–263. https://doi.org/10.52363/2414-5866-2024-1-30.

2. Акімова Л. М. Механізми державного управління економічною безпекою України: аналіз чинників впливу, систематизованих за окремими сферами її розвитку. Аспекти публічного правління. 2018. Т. 6. № 6-7. С. 5–13

3. Акімова Л. М. Теоретичні основи державного управління розвитком національної безпеки. Державне управління: удосконалення та розвиток. 2015. № 5. URL: http://www.dy.nayka.com.ua/?op=1&z=1210.

4. Ананьїн В. О., Горлинський В. В. Національна безпека держави в сучасних умовах : монографія / за заг. ред. В. О. Ананьїна. Київ : КПІ ім. Ігоря Сікорського, 2021. 345 с.

5. Андреєв С. О. Цивільний захист як напрям державної політики з питань національної безпеки: аналіз законодавчих новацій. Стратегічні пріоритети. 2015. № 4. С. 24–28.

6. Андрощук О., Грінченко В. Модель інформаційно-аналітичного забезпечення управлінської діяльності органу охорони державного кордону. Збірник наукових праць Національної академії державної прикордонної служби України. Серія: Військові науки та технічні науки. 2020. № 1 (82). С. 5–18. https://doi.org/10.32453/3.v82i1.527.

7. Бабков Ю. П., Адамчук М. М. Підходи до прийняття рішень при реагуванні на кризові ситуації, що загрожують національній безпеці України. Стан та перспективи реформування сектору безпеки і оборони України : матеріали міжнар. наук.-прак. конф. (м. Київ, 25–26 листоп. 2016 р.). Київ : Паливода А. В., 2016. С. 24–27.

8. Бабков Ю. П., Бєлай С. В., Бондаренко О. Г. Підходи до запровадження елементів національної системи стійкості у діяльність органів державного і військового управління. Честь і закон. 2023. № 3 (86). С. 12–20.

9. Бандурка О. М. Забезпечення фінансової безпеки держави в умовах воєнного стану. Актуальні питання фінансової безпеки : зб. тез доп. Міжнар. наук.-практ. конф. (м. Вінниця, 27 берез. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця : ХНУВС, 2023. С. 18–20.

10. Баранов А. Сучасний стан розвитку публічного управління в Україні. Аспекти публічного управління. 2019. Т. 7. № 8. С. 5–12. https://doi.org/10.15421/151936.

11. Баштанник О. В. Інституціональна/інституційна спроможність інститутів політичної системи як аналітична категорія та функціональний аспект публічного управління. Держава та регіони. Серія: Публічне управління та адміністрування. 2023. № 2 (80). С. 83–98. https://doi.org/10.32840/1813-3401.2023.2.15.

12. Бєлай С. В., Споришев К. О. Аналіз протиріч системи військового управління силами безпеки України. Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони в умовах воєнного стану : матеріали міжвідомчого круглого столу співробітників підрозділів СБУ, науково-педагогічних працівників Національної академії СБУ (м. Київ, 16 листоп., 2023 р.). Київ : НА СБУ, 2024. Вип. 2. С. 36.

13. Бисага Ю. М., Дешко Л. М., Нечипорук Г. Ю. Міжнародна безпека, національна безпека, конституційна безпека: теоретико-правові підходи. Порівняльно-аналітичне право. 2020. № 4. С. 43–49.

14. Битяк Ю. П., Яковюк І. В. Спільна політика безпеки і оборони ЄС: еволюція і стратегія розвитку. Євроатлантична інтеграція України: свідомий вибір моделі безпеки : зб. наук. ст. за матеріалами ІІІ Харків. міжнар.-прав. читань, присвяч. пам’яті проф. М. В. Яновського і В. С. Семенова (м. Харків,

3 листоп. 2017 р.) : у 2 ч. Харків, 2017. Ч. 1. С. 3–9.

15. Біла книга 2020. Збройні Сили України. Міністерство оборони України. Київ, 2021. URL: https://www.mil.gov.ua/content/files/whitebook/WB_2020.pdf

16. Білоус В. І. Поняття соціальної безпеки та її роль в системі національної безпеки держави. Ефективна економіка. 2019. № 3. https://doi.org/10.32702/2307-2105-2019.3.41.

17. Бойко О. А. Об'єкти підвищеної небезпеки: упровадження вдосконалених підходів до їх ідентифікації. Цивільний захист та пожежна безпека. 2023. № 1 (15). С. 83–91. https://doi.org/10.33269/nvcz.2023.1.83-91.

18. Борисевич С. Сутність і завдання публічної політики. Наукові розвідки з державного та муніципального управління. 2011. Вип.1. URL: http://archive.nbuv.gov.ua/portal/soc_gum/Nrzd/2011_1/2.pdf.

19. Будякова О., & Слободенюк К. Соціально-економічні чинники впливу на міграційні процеси в Україні в умовах воєнного стану. Вчені записки Університету «КРОК». 2025. № 1 (77). С. 96–106. https://doi.org/10.31732/2663-2209-2025-77-96-106.

20. Верховна Рада України ратифікувала Римський статут Міжнародного кримінального суду та поправки до нього. Прес-служба Апарату Верховної Ради України. Опубліковано 21 серп. 2024 р. URL: https://www.rada.gov.ua/news/razom/252711.html.

21. Воєнна доктрина України : затв. Указом Президента України від 24 вересня 2015 р. № 555/2015. URL: https://zakon.rada.gov.ua/laws/show/555/2015

22. Вольська О. Публічне управління як системне явище в сучасному суспільстві. Таврійський науковий вісник. Серія: Економіка. 2020. № 3. С. 15– 20. https://doi.org/10.32851/2708-0366/2020.3.2.

23. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації.

2025. № 2 (62). С. 31–41. https://doi.org/10.31673/2409-7292.2025.020831/.

24. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Аналітичний документ. Київ, 2018. 105 с. URL: https://www.civic-synergy.org.ua/wpcontent/uploads/2018/04/blok_XXIend_0202.pdf.

25. Голодник Ю. А. Діяльність правоохоронних органів Німеччини в механізмі забезпечення прав громадян, інтересів суспільства та держави: приклад для України. Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки. 2023. Т. 34 (73). № 4. С. 72–76. https://doi.org/10.32782/TNU-2707-0581/2023.4/10.

26. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.

27. Гринь Д. М. Сейсмічна небезпека території України : за матеріалами доповіді на засіданні Президії НАН України 8 березня 2023 р. Вісник Національної академії наук України. 2023. № 6. С. 25–33. https://doi.org/10.15407/visn2023.06.025.

28. Деякі питання ідентифікації об’єктів підвищеної небезпеки : Постанова Кабінету Міністрів України від 13.09.2022 р. № 1030. URL: https://zakon.rada.gov.ua/laws/show/1030-2022-%D0%BF#Text.

29. Дзьобань О. П., Соснін О. В. Концептуальні підходи до розуміння сутності забезпечення національної безпеки у сучасній науці. Національна безпека: світоглядні та теоретико-методологічні засади : монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. С. 75–104.

30. Домбровська С., Помаза-Пономаренко А., Нікіпєлова Є. Уніфікація правового механізму України та Республіки Польща щодо зміцнення національної безпеки : монографія. Харків: НУЦЗУ. 2019. 256 с.

31. Домбровська С., Татарнікова Т. Державна політика формування безпеки туризму. Теорія і практика розвитку туризму: досвід, проблеми, інновації : матеріали ІІІ Всеукр. наук.-практ. інтернет-конференції (м.

Черкаси, 20 лют. 2025 р.) / за заг. ред. С. М. Домбровської. Черкаси : НУЦЗ України, 2025. С. 27–29.

32. Єманов В. В., Бєлай С. В., Тробюк В. І. Обґрунтування пропозицій з удосконалення системи підготовки та перепідготовки персоналу сектору безпеки і оборони України в умовах відсічі збройної агресії. Вісник Національного університету цивільного захисту. Державне управління. 2023. Вип. 1 (18). С. 271–279. https://doi.org/10.52363/2414-5866-2023-1-29.

33. Загорулько А. П. Теоретико-правовий аналіз визначення поняття «внутрішня безпека України». Вісник Національного університету цивільного захисту України. Державне управління. 2019. № 2 (11). С. 19–28. https://doi.org/10.5281/zenodo.3532668.

34. Загурська-Антонюк В. Ф. Полістратегія та правове регулювання політики національної безпеки. Інвестиції: практика та досвід. 2020. № 19–20. С. 134–140. https://doi.org/10.32702/2306-6814.2020.19-20.134.385

35. Запорожець Т. В. Державна політика у сфері захисту критичної інфраструктури : навч. посіб. Київ : ДКС-Центр, 2024. 186 с.

36. Збереження і розвиток України в умовах війни та миру: національна доповідь / ред. кол. С. І. Пирожков, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, Е. М. Лібанова, О. В. Скрипнюк; Інститут держави і права ім. В. М. Корецького НАН України. Київ : Наук. думка, 2024. 220 с.

37. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році. Кіберполіція. 31.01.2025 р. https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/.

38. Зовнішня політика США : навч.-метод. посіб. / уклад.: І. М. Коваль, Ю. І. Майстренко. Одеса : Астропринт, 2024. 111 с

39. Індекс сприйняття корупції – 2023. Україна покращила свій показник на 3 бали. URL: https://nazk.gov.ua/uk/uk/indeks-spryynyattya-koruptsii-2023-ukraina-pokraschyla-sviy-pokaznyk-na-3-baly/.

40. Індекс сприйняття корупції – 2024. URL: https://ti-ukraine.org/research/indeks-spryjnyattya-koruptsiyi-2024/.

41. Інформаційна безпека: філософське та організаційно-правове підґрунтя рефлексії національних інтересів України / О. Г. Данильян, О. П. Дзьобань, Ю. Ю. Калиновський, Д. О. Олєйніков; за ред. О. Г. Данильяна. Харків : Право, 2024. 224 с.

42. Казакова Л. О. Національна безпека держави: понятійно-категоріальний апарат. Регіональні студії. 2021. № 24. С. 128–132. https://doi.org/10.32782/2663-6170/2021.24.18.

43. Каптан М. В. Двосторонні безпекові угоди України як інструмент протидії російській агресії: правова оцінка. Науковий вісник Херсонського державного університету. Серія: Юридичні науки. 2025. № 1. С. 42–52. https://doi.org/10.32999/ksu2307-8049/2025-1-7.

44. Кизим М. О., Губарєва І. О., Хаустова В. Є., Манойленко О. В. Аналіз контекстуальних і часових закономірностей розвитку поглядів на пріоритети забезпечення обороноздатності країн світу. Бізнес Інформ. 2022. № 4. С. 4–12. https://doi.org/10.32983/2222-4459-2022-4-4-12.

45. Київський безпековий договір. Міжнародні гарантії безпеки для України : рекомендації. Київ, 13 верес. 2022 р. 10 с. URL: https://www.president.gov.ua/storage/j-files-storage/01/15/93/cf0b512b41823b01f15fa24a1325edf4_1663050954.pdf.

46. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань ; упоряд. О. Довгань, Л. Литвинова, С. Дорогих ; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України ім. В. І. Вернадського. Київ, 2024. № 2 (лютий). 253 с.

47. Ковбаса В. М., Кусько Р. В., Дрозд Т. В. Діяльність Національної поліції в умовах воєнного стану: окремі проблемні питання. Юридичний науковий електронний журнал. 2022. № 6. С. 245–248.

https://doi.org/10.32782/2524-0374/2022-6/57.

48. Кодекс цивільного захисту України : Закон України від 02.10.2012 р. № 5403-VI. Дата оновлення: 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.

49. Кокун О. М. Життєстійкість і резильєнтність людини в сучасному світі: теорія, дослідження, практика : монографія. Київ : Інститут психології ім. Г. С. Костюка НАПН України, 2025. 214 с.

50. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

51. Копанчук В. О. Концептуальні засади національної безпеки України в умовах глобалізації з акцентом світового досвіду. Державне управління: удосконалення та розвиток. 2018. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1614.

52. Котух Є. В. Розвиток публічно-приватного партнерства у сфері кібербезпеки. Інвестиції: практика та досвід. 2021. № 13-14. С. 58–63. https://doi.org/10.32702/2306-6814.2021.13-14.58

53. Коцюба В. Порушення прав людини в контексті російсько-української війни. Історико-політичні проблеми сучасного світу. 2023. № 47. С. 124–133. https://doi.org/10.31861/mhpi2023.47.124-133.

54. Кравчук О. В. Державне управління забезпечення державної безпеки в умовах «цифровізації». Теорія та практика державного управління і місцевого самоврядування. 2019. № 1. URL: http://nbuv.gov.ua/UJRN/Ttpdu_2019_1_22.

55. Криза правоохоронної системи України : монографія / за заг. ред. В. В. Євдокімова, Д. О. Грицишина. Житомир : Вид. дім «Бук-друк», 2023. 584.

56. Криштанович М. Ф. Реалізація механізмів публічного управління у сфері цивільного захисту. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2017. Вип. 1 (6). С. 341–347.

57. 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.

58. Крук С. І. Інституційний розвиток державного управління у сфері забезпечення національної безпеки України : автореф. дис. ... д-ра наук з держ. упр. : 25.00.05. Харків, 2019. 43 с.

59. Крук С. І. Поняття та сутність механізмів державного управління у сфері забезпечення національної безпеки України. Держава та регіони. 2018. № 4. С. 87–90.

60. Курило А. Г. Місце інформаційної безпеки в системі національної безпеки. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2022. № 1 (14). https://doi.org/10.52363/2414-5866-2021-1-12.

61. Левченко. О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія. Житомир : Вид-во «Євро-Волинь», 2021. 172 с.

62. Лепіхов А. Нові підходи Великої Британії до забезпечення національної стійкості. Київ : Національний інститут стратегічних досліджень. 20.02.2023. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/novi-pidkhody-velykoyi-brytaniyi-do-zabezpechennya-natsionalnoyi.

63. Ліпкан В. А. Політичні засади геостратегії сучасної Української Держави : монографія. Одеса : Гельветика, 2024. 830 с.

64. Магда Є. В. Гібридна війна: вижити і перемогти. Харків : Віват, 2015. 320 с.

65. Маковій В. П., Усата Г. О. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави. Морська безпека та оборона. 2023. № 1. С. 62–68. https://doi.org/10.32782/msd/2023.1.8.391

66. Матвієнків С., Воробець Н. Національна безпека в сучасній Україні.

Вісник Прикарпатського університету. 2019. Вип. 13. С. 104–110.

67. Матета О. А. Категорія «національні інтереси» як складова національної безпеки України. Харків, 2020. С. 315–317. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/443904d2-e74a-4a92-b63d-f65b6216501b/content.

68. Матюшкова Т. П. Внутрішнє безпекове середовище в Україні: формування, забезпечення, оцінка рівня ефективності. Національна безпека як конституційна цінність: сучасні виклики : матеріали Міжнар. наук.-практ. конф. (м. Чернівці, 22 черв. 2023 р.). Чернівці, 2023. С. 92–95.

69. Мельниченко Б., Фігель Н. Основні підходи до розуміння поняття «національна безпека». Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2021. № 2 (30). С. 68–72. https://doi.org/10.23939/law2021.30.068.

70. Менеджмент у державному управлінні: особлива частина : навч. посіб. / В. П. Пєтков, С. В. Пєтков, Р. С. Наливайко, О. Г. Комісаров. та ін. ; за заг. ред. В. П. Пєткова. Київ : КНТ, 2019. 216 с.

71. Михайлов Д. Європол приєднався до спільної слідчої групи щодо розслідування міжнародних злочинів в Україні. Суспільне новини. 05.10.2023 р. URL: https://suspilne.media/587905-evropol-priednavsa-do-spilnoi-slidcoi-grupi-sodo-rozsliduvanna-miznarodnih-zlociniv-v-ukraini.

72. Мосейко А. Г. Національна безпека України як об’єкт публічного адміністрування. Вісник ЛДУВС ім. Е. О. Дідоренка. 2019. Вип. 2 (86). С. 42–52. https://doi.org/10.33766/2524-0323.86.42-52.

73. Мосейко А. Г., Негодченко В. О. Досвід Сполучених Штатів Америки щодо публічного адміністрування в сфері національної безпеки. Право і суспільство. 2019. № 4. С. 323–329. https://doi.org/10.32842/2078-3736-2019-4-48.

74. Мотайло О. В. Основні концептуальні підходи до сутності поняття «національна безпека». Право та державне управління. 2019. № 4. С. 288–293.

https://doi.org/10.32840/pdu.2019.4.44.

75. Мюджахіт Б., Стельмах А. Сучасні аспекти формування та реалізації публічної безпеки: європейський досвід. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2023. № 5. С. 6–17. https://doi.org/10.31470/2786-6246-2023-5-6-17.

76. Назимко Є. С., Буга Г. С., Князєв С. М. Поняття «Community Policing». Правова позиція. 2023. № 2 (39). С. 184–187. https://doi.org/10.32782/2521-6473.2023-2.37.

77. Національна безпека України в умовах воєнного стану: загальна характеристика концепції; міжнародний аспект; нормативне регулювання; судова практика / укл. : Алієв Р. В., Джус О. А., Копотун І. М., Коропатнік І. М., Микитюк М. А., Павлюк О. О., Пєтков В. П., Пєтков С. В., Скриньковський Р. М., Шамрай Б. М., Юрков А. В. Київ : ВД «Професіонал», 2024. 480 с

78. 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; Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ : НАН України, 2022. 552 с.

79. Нова стратегія внутрішньої безпеки ЄС із фокусом на кібербезпеку: ProtectEU. URL: https://cybersec.net.ua/statti/846-protecteu-nova-stratehiia-vnutrishnoi-bezpeky-yes-iz-fokusom-na-kiberbezpeku.html.

80. Нормативно-правова база у галузі безпеки і оборони України. Зміни та доповнення, 2012–2014 / Центр досліджень армії, конверсії та роззброєння, Київ, 2015. 296 с.

81. Носач А. В. Загрози національній безпеці як обов’язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність України. Право і суспільство. 2019. № 3. С. 50–56. https://doi.org/10.32842/2078-3736-2019-3-1-9.

82. Огляд стратегічних документів Європейського Союзу у сфері економічної безпеки : аналіт. огляд / Д. С. Покришка. Київ : НІСД, 2024. 41 с. https://doi.org/10.53679/NISS-analytrep.2024.12.

83. Омельченко М. М. Еволюція стратегічних підходів до забезпечення енергетичної безпеки України в умовах повномасштабної війни: уроки 2022–2025 років. Матеріали науково-практичної конференції / за заг. ред. Горника В. Г. Харків, 2025.

84. Омельченко М. М. Інституційні механізми державного управління реформуванням сектору безпеки і оборони України: регіональний вимір (2014–2021 роки). Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2025. Вип. 2 (15). С. 462–469.

85. Омельченко М. М. Механізми державного управління реформуванням сектору безпеки і оборони України в період 2014–2021 років: досягнення та проблеми. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2025. Вип. 1 (14). С. 430–440.

86. Омельченко М. М., Тарасов С. С. Трансформація механізмів державного управління сектором безпеки і оборони: адаптація до гібридних загроз на основі зарубіжного досвіду. Матеріали І Міжнародної науково-практичної конференції «Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення» (м. Івано-Франківськ, 27 листопада 2025 р.). Івано-Франківськ, 2025.

87. Організація системи забезпечення національної стійкості на регіональному і місцевому рівнях : аналіт. доп. / О. О. Резнікова, К. Є. Войтовський, А. В. Лепіхов ; за заг. ред. О. О. Резнікової. Київ : НІСД, 2021. 140 с.

88. Орлова Н., Козирєва О. Економічна та соціальна безпека внутрішньо переміщених осіб в Україні. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2024. № 9. С. 123–133. https://doi.org/10.31470/2786-6246-2024-9-123-133.

89. Оцінка ситуації в країні та діяльності влади, довіра до соціальних інститутів, політиків, посадовців та громадських діячів, віра в перемогу. Центр Розумкова. Вересень 2024 р. URL: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia

90. Ortynskyi, V. Information Security in the Context of National Security: Legal Mechanisms for Protecting State Information Resources. Veritas: Legal and 413 Psychological-Pedagogical Research. 2025. Vol. 1(1). Pp. 1-9. https://doi.org/10.23939/veritas2025.01.001.

91. Павленко Б. О., Гулаков В. А. Характеристика національної безпеки як основи захисту суспільства. Правові горизонти. 2019. Вип. 20. С. 30–34.

92. Павленко Д. Г., Семенюк Ю. В., Лисецький Ю. М. Національна безпека: поняття, складники, чинники впливу. Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління. 2021. Т. 32 (71), № 3. С. 102–107. https://doi.org/10.32838/TNU-2663-6468/2021.3/17.

93. Павленко І., Нагірний В., Потапенко В., Маляревський Є. Аналіз загроз національній безпеці у сфері внутрішньої політики. Експертне опитування. Київ : НІСД, 2024. 31 с. https://niss.gov.ua/sites/default/files/2024-04/ad_zagrozi_vnutr_polit.pdf.

94. Паламарчук Д. Національна безпека: національні цінності, інтереси, цілі, завдання. 2024. БІНТЕЛ. № 2. URL: https://bintel.org.ua/nukma/nacionalna_bezpeka/.396

95. Палюх В. В., Омельченко М. М. Управлінська синергія та виклики при міжвідомчому комплектуванні керівного складу ЗВО зі специфічними умовами навчання: аналіз адаптаційних механізмів. Успіхи і досягнення у науці. Серія «Управління та адміністрування». 2025. № 17.

96. Пархоменко-Куцевіл О. Проблеми забезпечення національної безпеки в умовах воєнного часу. Науковий вісник Вінницької академії безперервної освіти. Серія: Екологія. Публічне управління та адміністрування. 2023. Вип. 3. С. 143–150. https://doi.org/10.32782/2786-5681-

2023-3.19.

97. Подковенко Т. Національна безпека України: аксіологічний та правовий аспекти. Актуальні проблеми правознавства. 2021. № 1 (25). С. 11–18. https://doi.org/10.35774/app2021.01.011.

98. Поліція України. Європол створив оперативну робочу групу OSINT для підтримки розслідувань воєнних злочинів в Україні. 30.11.2023. URL: https://mvs.gov.ua/news/jevropol-stvoriv-operativnu-robocu-grupu-osint-dlia-pidtrimki-rozsliduvan-vojennix-zlociniv-v-ukrayini.

99. Помаза-Пономаренко А. Л., Бондар Д. В., Демент М. О. Державна безпека кордону: ризики та загрози для національної безпеки України й ЄС. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2023. Вип. 2. С. 75–80. https://doi.org/10.52363/2414-5866-2023-2-8.

100. Пономарьов С. П. Публічна безпеки в системі сектору безпеки і оборони України. Правоохоронна функція держави: теоретико-методологічні та історико-правові проблеми : тези доп. «круглого столу» (м. Харків, 27 жовт. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2017. С. 173–178.

101. Примуш Р. Б. Інформаційне забезпечення стратегічного планування в сфері національної безпеки. Державне управління: удосконалення та розвиток. 2018. № 7. URL: http://www.dy.nayka.com.ua/pdf/7_2018/41.pdf.

102. Пріоритети розвитку реального сектора в умовах війни та повоєнного відновлення економіки України : аналіт. доп. / О. В. Собкевич, А. В. Шевченко, В. М. Русан та ін. ; за заг. ред. Я. А. Жаліла. Київ : НІСД, 2024. 104 с. https://doi.org/10.53679/NISSanalytrep.2024.03.

103. Про безпеку класифікованої інформації : проєкт Закону України від 27.01.2023 № 8394. URL: https://ips.ligazakon.net/document/JI08684A.

104. Про внесення змін до деяких законодавчих актів України щодо уточнення положень про конкурсний відбір кандидатур на посаду судді

Конституційного Суду України : Закон України від 27.07.2023 р. № 3277-IX. URL: https://zakon.rada.gov.ua/laws/show/3277-20#Text.

105. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави : Закон України від 19 червня 2003 р. № 975-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/975-15

106. Про державну службу : Закон України від 10.12.2015 р. № 889-VIII. Відомості Верховної Ради України. 2016. № 4. Ст. 43.

107. Про засади державної антикорупційної політики на 2021–2025 роки : Закон України від 20.06.2022 р. № 2322-IX. URL: https://zakon.rada.gov.ua/laws/show/2322-20#Text.

108. Про затвердження Положення про Державну службу України з надзвичайних ситуацій : Постанова Кабінету Міністрів України від 16.12.2015 р. № 1052. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1052-2015-%D0%BF#Text.

109. Про затвердження Положення про Міністерство оборони України : Постанова Кабінету Міністрів України від 26.11.2014 р. № 671. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF.

110. Про Збройні Сили України : Закон України від 06.12.1991 р. № 1934-XII. Відомості Верховної Ради України. 1992. № 9. Ст. 108.

111. Про Концепцію реформування Державної служби спеціального зв’язку та захисту інформації України : Указ Президента України від 22.10.2021 р. № 544/2021. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/n0068525-21#Text.

112. Про Концепцію розвитку сектору безпеки і оборони України : Указ Президента України від 14.03.2016 р. № 92/2016. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/n0002525-16#Text.

113. Про Національне агентство України з питань виявлення, розшуку

та управління активами, одержаними від корупційних та інших злочинів : Закон України від 10.11.2015 р. № 772-VIII. URL: https://zakon.rada.gov.ua/laws/show/772-19#Text.

114. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19

115. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.

116. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.

117. Про національну програму інформатизації : Закон України від 04.02.1998 р. № 74/98-ВР. Відомості Верховної Ради України. 2023. № 51. Ст. 127.

118. Про оборону України : Закон України від 06.12.1991 р. № 1932-XII. Відомості Верховної Ради України. 1992. № 9. Ст. 106.

119. Про об’єкти підвищеної небезпеки : Закон України від 18.01.2001 р. № 2245-III. Дата оновлення: 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text.

120. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення: 20.04.2025. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

121. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. Відомості Верховної Ради України. 2015. № 28. Ст. 250.

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

123. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 р. № 183/98-ВР. Відомості Верховної Ради України. 1998. №

35. Ст. 237.

124. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 р. Верховна Рада України. Законодавство України. № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

125. Про розвідку : Закон України від 17.09.2020 р. No912-IX. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text.

126. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229. Відомості Верховної Ради України. 1992. № 27. Ст. 382.

127. Про стратегічний оборонний бюлетень України : Указ Президента від 17.09.2021 р. No473/2021. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/n0063525-21#Text.

128. Про Стратегію воєнної безпеки України : Указ Президента України від 25.03.2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/n0022525-21#Text.

129. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text.

130. Про схвалення Національного плану з енергетики та клімату на період до 2030 року : розпорядження Кабінету Міністрів України від 25.06.2024 р. № 587-р. URL: https://zakon.rada.gov.ua/laws/show/587-2024-%D1%80#Text.

131. Про схвалення Стратегії енергетичної безпеки : розпорядження Кабінету Міністрів України від 04.08.2021 р. № 907-р. URL: https://zakon.rada.gov.ua/laws/main/907-2021-%25D1%2580#Text.

132. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках : розпорядження Кабінету Міністрів України від 31.12.2024 р. № 1351-р. URL:

https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text.

133. Про Цілі сталого розвитку України на період до 2030 року : Указ Президента України від 30.09.2019 р. № 722/2019. https://zakon.rada.gov.ua/laws/show/722/2019#Text.

134. Редькіна А. Українські національні інтереси й цінності: суспільне усвідомлення та переоцінка. Політичні дослідження. 2023. № 1 (5). С. 144–162. https://doi.org/10.53317/2786-4774-2023-1-8.

135. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 532 с.

136. Резнікова О. О., Войтовський К. Є., Лепіхов А. В. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. / за ред. О. О. Резнікової. Київ : НІСД. 2020. 84 с.

137. Результати Вільнюського саміту НАТО 11–12 липня 2023 р. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/rezultaty-vilnyuskoho-samitu-nato-11-12-lypnya-2023-roku.

138. Рижук Ю. М. Забезпечення органами місцевого самоврядування прав людини в умовах воєнного стану. Київський часопис права. 2022. № 4. С. 25–30. https://doi.org/10.32782/klj/2022.4.3.

139. Рік діяльності Уряду: розробка стратегічних документів у сфері безпеки та оборони. URL: https://www.mil.gov.ua/news/2021/03/02/rik-diyalnosti-uryadu-rozrobka-strategichnih-dokumentiv-u-sferi-bezpekita-oboroni/.

140. Рубан А. В. Національна безпека як об’єкт державного регулювання. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2018. Вип. 2 (9). С. 58–62.

141. Рубан А. В. Формування дієвих механізмів вирішення проблем державного регулювання у сфері національної безпеки. Публічне управління і адміністрування в Україні. 2019. Вип. 11. С. 141–143.

142. Руснак І. С., Хижняк В. В. Національна безпека та підвищення обороноздатності України в контексті нових викликів і загроз. Стратегічна

панорама. 2015. № 1. С. 12–20.

143. Рябовол Л. Т. Національна безпека України: структурно-функціональний аналіз. Вісник Університету імен Альфреда Нобеля. Серія: Право. 2020. № 1 (1). С. 25–30. https://doi.org/10.32342/2709-6408-2020-1-1-4.

144. Ситник Г. П., Неліпа Д. В., Орел М. Г. Політичне, публічне та державне управління у сфері національної безпеки у контексті публічної та державної політики. Науковий часопис Академії національної безпеки. 2020. № 1-2. С. 8–32.

145. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України : підручник / за ред. Г. П. Ситника. Київ : МАУП, 2021. с.

146. Скоморовський В. Б., & Лучко О. О. Роль міжнародних організацій у протидії тероризму. Legal Bulletin. 2024. № 13. С. 109–116. https://doi.org/10.31732/2708-339X-2024-13-A16.

147. Спільна декларація про підтримку України. 12 липня 2023 р. URL: https://www.president.gov.ua/news/spilna-deklaraciya-pro-pidtrimku-ukrayini-84277.

148. Споришев К. О. Аналіз нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки Україні. Честь і закон. 2024. № 1 (88). С. 142–149.

149. Стратегія громадської безпеки та цивільного захисту України : затв. від Указом Президента України від 29.06.2021 р. URL: https://mvs.gov.ua/ministry/normativna-baza-mvs/proekti-normativnix-aktiv/strategiya-gromadskoyi-bezpeki-ta-civilnogo-zaxistu-ukrayini-zatverdzeno-vid-29062021.

150. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

151. Суворов В. П. Трансформація багаторівневого управління на основі глобальних стратегій ЄС та національна стійкість України в умовах

гібридних загроз. Державне будівництво. 2023. № 2 (34). С. 183–196. https://doi.org/10.26565/1992-2337-2023-2-15.

152. Татарнікова Т. Механізми державного контролю служб внутрішньої безпеки в країнах-членах ради Європи. Гуманітарний дискурс суспільних проблем: минуле, сучасне, майбутнє : матеріали XXIV Всеукр. наук. конф. з міжнар. участю (м. Черкаси, 18 квіт. 2024 р.). Черкаси : ЧІПБ імені Героїв Чорнобиля НУЦЗ України, 2024. С. 313–314.

153. Татарнікова Т. О. Аналіз міжнародного досвіду щодо механізмів державного управління у сфері забезпечення внутрішньої безпеки. Державне управління: удосконалення та розвиток. 2025. № 4. https://doi.org/10.32702/2307-2156.2025.4.21.

154. Татарнікова Т. О. Внутрішня безпекова політика: впливові чинники та шляхи вдосконалення. Державне управління: удосконалення та розвиток. 2025. № 1. https://doi.org/10.32702/2307-2156.2025.1.21.

155. Татарнікова Т. О. Захист національних інтересів як основа державного управління у сфері забезпечення внутрішньої безпеки. Інвестиції: практика та досвід. 2024. № 22. С. 287–290. https://doi.org/10.32702/2306-6814.2024.22.288.

156. Татарнікова Т. О. Ключові принципи формування внутрішньої безпекової політики держави. Інвестиції: практика та досвід. 2024. № 19. С. 238–240. https://doi.org/10.32702/2306-6814.2024.19.238.406

157. Татарнікова Т. О. Механізми правового регулювання у сфері забезпечення внутрішньої безпеки. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2024. Вип. 2 (21). С. 135–139. https://doi.org/10.52363/2414-5866-2024-2-15.

158. Татарнікова Т. О. Механізми формування національно-державної ідеології забезпечення внутрішньої безпеки. Інвестиції: практика та досвід. 2024. № 21. С. 208–210. https://doi.org/10.32702/2306-6814.2024.21.208.

159. Татарнікова Т. О. Національно-державна ідеологія як передумова забезпечення внутрішньої безпеки. Вісник Національного університету

цивільного захисту України. Серія: Державне управління. 2025. Вип. 1 (22). С. 61–66. https://doi.org/10.52363/2414-5866-2025-1-7.

160. Татарнікова Т. О. Політичні механізми вдосконалення політики забезпечення внутрішньої безпеки. Інвестиції: практика та досвід. 2024. № 24. С. 212–214. https://doi.org/10.32702/2306-6814.2024.24.212.

161. Татарнікова Т. О. Попередження злочинів й адміністративних правопорушень як інструмент державного управління у сфері забезпечення внутрішньої безпеки. Інвестиції: практика та досвід. 2025. № 8. С. 244–246. https://doi.org/10.32702/2306-6814.2025.8.244.

162. Татарнікова Т. О. Розвиток місцевого самоврядування як ключовий чинник ефективності внутрішньої безпекової політики. Державне управління: удосконалення та розвиток. 2024. № 11. https://doi.org/10.32702/2307-2156.2024.11.26.

163. Татарнікова Т. О. Роль і місце інститутів місцевого самоврядування у процесах забезпечення внутрішньої безпеки. Інвестиції: практика та досвід. 2025. № 7. С. 240–242. https://doi.org/10.32702/2306-6814.2025.7.240.

164. Татарнікова Т. О. Система забезпечення внутрішньої безпеки українського суспільства: сучасний стан та перспективи розвитку. Інвестиції: практика та досвід. 2024. № 23. С. 213–216. https://doi.org/10.32702/2306-6814.2024.23.213.

165. Татарнікова Т. О. Специфіка формування внутрішньої безпекової політики в сучасних умовах. Державне управління: удосконалення та розвиток. 2024. № 12. https://doi.org/10.32702/2307-2156.2024.12.22.

166. Татарнікова Т. Складові економічної безпеки в умовах сучасної глобалізації. Розвиток компетентності в публічному секторі: європейські стандарти та перспективи : матеріали Міжнар. наук.-практ. конф. Івано-Франківськ, 2025. С. 339–341.

167. Татарнікова Т. Формування інструментів безпеки держави. Публічне управління у сфері цивільного захисту: освіта, наука, практика : зб.

матеріалів Міжнар. наук.-практ. інтернет-конф. (м. Черкаси, 2025 р.) / за заг. ред. С. М. Домбровської. Харків : НУЦЗУ, 2025. С.

168. Терент'єва А. Досвід держави Ізраїль щодо управління безпекою цивільного населення в умовах кризових ситуацій. Науковий вісник: Державне управління. 2023. № 2 (14). С. 310–333. https://doi.org/10.33269/2618-0065-2023-2(14)-310-333.

169. Тимошенко В. І. Внутрішні загрози національній безпеці України. Аналітично-порівняльне правознавство. 2024. № 2. С. 94–99. https://doi.org/10.24144/2788-6018.2024.02.14.

170. Торічний В. О., Федорчук А. В., Глуздань О. П. Специфіка антикризового управління в інституціях сектору безпеки і оборони України. Національні інтереси України. 2024. № 3 (3). С. 144–154. https://doi.org/10.52058/3041-1793-2024-3(3).

171. Tatarnikova, T. The Development of Mechanisms of Creation of the State Policy in the field of Internal Security. Public Administration and State Security Aspects. 2024. Vol. 2. Pp. 63-67. https://doi.org/10.52363/passa-2024.2-10.

172. Україна в Індексі сприйняття корупції – 2024. URL: https://cpi.ti-ukraine.org/.

173. Українське суспільство в умовах війни. Рік 2024 : монографія / С. Дембіцький, О. Злобіна, Н. Костенко та ін. ; за ред. Є. Головахи, С. Дембіцького. Київ : Інститут соціології НАН України, 2024. 450 с.

174. Хаустова В. Є., Трушкіна Н. В. Теоретичні підходи до визначення сутності поняття «національна безпека» та її складових. Проблеми економіки. 2024. № 4 (62). С. 134–153.

175. Хомік М. М. Концептуальні підходи до застосування військ (сил) Збройних Сил України та інших військових формувань під час надзвичайних ситуацій природного, техногенного і воєнного характеру. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2018. № 2 (63). С. 75–80.

176. Чижов Д. А. Національна безпека як елемент системи забезпечення прав і свобод людини та громадянина. Держава та регіони. Серія: Право. 2021. № 4 (74). С. 96–101. https://doi.org/10.32840/1813-338X-2021.4.15.

177. Шестернін А., Роговенко О. Роль органів місцевого самоврядування у забезпеченні національної безпеки України. Молодий вчений. 2024. № 3(127). С. 85–89. https://doi.org/10.32839/2304-5809/2024-3-127-13.410

178. Шипілова Л. М. Стратегічне планування у сфері національної безпеки. Київ : ВПЦ «Київський університет», 2023. 143 с.

179. Штеба Р. Ю. Теоретичні засади державної політики у сфері забезпечення національної безпеки. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2019. Вип. 1 (10). С. 415–422.

180. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2024 році. URL: https://www.ombudsman.gov.ua

181. Arquilla John. Bitskrieg : The New Challenge of Cyberwarfare. Cambridge : Polity Press, 2021. 224 p.

182. Bachmann S.-D., Gunneriusson H. Hybrid Wars: The 21st Century's New Threats to Global Peace and Security. Scientia Militaria: South African Journal of Military Studies. 2015. Vol. 43, No. 1. P. 77–98.

183. Bērziņš J. The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. The Journal of Slavic Military Studies. 2020. Vol. 33, No. 3. P. 355–380.

184. Chesney Robert, Citron Danielle. Deep Fakes and the New Disinformation War. Foreign Affairs. 2019. Vol. 98, No. 1. P. 147–155.

185. Collins Alan. Contemporary Security Studies. 5th edition. Oxford : Oxford University Press, 2019. 584 p.

186. Cyber Defence Pledge. NATO. 2016. URL:

https://www.nato.int/cps/en/natohq/official_texts_133177.htm

187. EU Strategic Compass for Security and Defence. Brussels : Council of the European Union, 2022. 47 p.

188. EU-NATO Declaration on European Defence. Brussels, 2018. 23 p.

189. European Institute for Gender Equality (EIGE). Gender Equality Index 2024 – Sustaining Momentum on a Fragile Path. Luxembourg: Publications Office of the European Union, 2024. 164 p. https://doi.org/10.2839/9523460.

190. European Union Global Strategy : Three Years On, Looking Forward. Brussels : EEAS, 2019. 68 p.

191. Fisher, James D. The Enclosure of Knowledge. Books, Power, and Agrarian Capitalism in Britain, 1660–1800. Cambridge: Cambridge University Press, 2022. XIII. 330 p. https://doi.org/10.1017/9781009049283.

192. Galeotti Mark. The Mythical ' Gerasimov Doctrine ' and the Language of Threat. Critical Studies on Security. 2019. Vol. 7, No. 2. P. 157–161.

193. Gartzke E., Lindsay J. R. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies. 2015. Vol. 24, No. 2. P. 316–348.

194. Home Office. URL: https://www.gov.uk/government/organisations/home-office. Institute for Economics & Peace. Global Terrorism Index 2023. 2023. URL: https://reliefweb.int/report/world/global-terrorism-index-2023.

195. Joint Declaration by European Council, European Commission and NATO Secretary General. Warsaw, 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133163.htm

196. Kattler, A., Ettensperger, F. National internal security policies across Europe – a comparative analysis applying big data clustering techniques. Political Research Exchange. 2020. Vol. 2(1). https://doi.org/10.1080/2474736X.2020.17.

197. Kofman Michael. The Moscow School of Hard Knocks : Key Pillars of Russian Strategy. War on the Rocks. 2020. URL: https://warontherocks.com/2020/01/the-moscow-school-of-hard-knocks-key-pillars-of-russian-strategy/

198. Kryshtanovych, Svitlana, Tatarnikova, Tetiana, Rybkina, Svitlana, Kopanchuk, Olena, and Motorny, Vladimir. Scientific and Methodological Approach to Strengthening Intellectual Security and Human-Centricity through Optimizing the Use of Artificial Intelligence. International Journal of Religion. 2024. Vol. 5(9). Pp. 760-771. https://doi.org/10.61707/p60brq41.

199. Kur, L., Bor, E., Mwaeke, P. Security Implications of Using the Military in Maintaining Peace through Internal Security Operations, a Case of Central Equatoria State – Juba. Open Journal of Political Science. 2024. Vol. 14. Pp. 81-90.

200. Lasconjarias G., Larsen J. A. (eds.). NATO's Response to Hybrid Threats. Rome : NATO Defense College, 2015. (NDC Forum Paper ; No. 24).

201. Madrid Summit Declaration. NATO. 2022. URL: https://www.nato.int/cps/en/natohq/official_texts_196951.htm

202. Omelchenko M. M., Paliukh V. V. Methodological Foundations for Diagnosing the Effectiveness of Public Administration in the Security and Defense Sector under Russian Aggression: Ukrainian Experience. Public Administration and State Security Aspects. 2025. Vol. 2. P. 43–54.

203. Paliukh, V., Kovtun, I., Pidlisna, T., Tatarnikova, T., & Poroka, S. The Influence of National Information Security Policies on Advancing Higher Education. Qubahan Academic Journal. 2025. Vol. 5(1). Pp. 628-639. https://doi.org/10.48161/qaj.v5n1a1500.

204. Paliukh, V., Trobiuk, V., Tatarnikova, T., Yakymenko, S., & Verba, S. Modernization of the Educational Process Through the Implementation of a Modern Strategy for Ensuring Information Security. Ad Alta-Journal of Interdisciplinary Research. 2024. Vol. 14(1). Special Issue. Pp. 152-156. URL: https://www.magnanimitas.cz/ADALTA/140141/papers/A_25.pdf.

205. Qureshi, Hanif. Internal Security: an International Outlook. Indian Police Journal. 2020. http://dx.doi.org/10.2139/ssrn.3893442.

206. Svitková, K. Resilience in the National Security Discourse. Obrana a Strategie (Defence & Strategy). 2017. Vol. 17(1). Pp. 21-42.

https://doi.org/10.3849/1802-7199.17.2017.01.021-042.

207. Ukraine. Third Rapid Damage and Needs Assessment (RDNA3). February 2022 – December 2023. URL: https://ukraine.un.org/sites/default/files/202402/UA%20RDNA3%20report%20EN.pdf.

208. Warsaw Summit Communiqué. NATO. 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

209. Zhovnirchyk, Y., Larina, N., Stoliar, Y., Tatarnikova, T., & Sukharnykov, V. Innovative Approaches in Public Administration: Strategies and Tools for Achieving Sustainability. Economic Affairs. 2024. Vol. 69(02). Pp. 1191- 1197. https://doi.org/10.46852/0424-2513.3.2024.40.

ДОДАТКИ

Додаток А

ЧЕРКАСЬКА РАЙОННА РАДА

✉ вул. В.Чорновола, 157, м. Черкаси, 18003, ☎/факс 64-34-76
E-mail: cherkaskarada@ukr.net Код ЄДРПОУ 25659510

14.11.2025 № 20/01-22
на №_____від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження
здобувача наукового ступеня кандидата наук з державного управління
за спеціальністю 25.00.02 — механізми державного управління
Омельченка Миколи Миколайовича
за темою: «Механізми державного управління реформуванням сектору безпеки і оборони України в умовах збройної агресії»

Дисертаційне дослідження Омельченка М.М. окреслює перспективний напрям адаптації загальнодержавних механізмів реформування сектору безпеки і оборони до регіонального та місцевого рівня управління, що набуває особливої актуальності в умовах децентралізації публічного управління та практичної діяльності органів місцевого самоврядування із забезпечення безпеки і цивільного захисту населення.

Розроблені автором методичні підходи до врахування регіонального виміру індикативної оцінки загроз національній безпеці, зокрема система індикаторів оцінки стану безпеки територій з урахуванням специфіки прикордонних регіонів та концентрації об'єктів критичної інфраструктури, використані при підготовці аналітичних матеріалів щодо стану безпеки та цивільного захисту на території району.

Рекомендація дисертанта щодо створення мережі регіональних громадських рад з питань безпеки при обласних державних адміністраціях для здійснення громадського контролю за діяльністю територіальних підрозділів силових структур взята до уваги як методична основа при опрацюванні пропозицій щодо посилення взаємодії районної ради з територіальними органами сектору безпеки і оборони та громадськістю району.

Викладені в дисертації положення підтверджують свою прикладну значущість та можуть слугувати орієнтиром для подальшого вдосконалення взаємодії органів місцевого самоврядування з механізмами державного управління у сфері реформування сектору безпеки та оборони України.

Впровадження результатів дисертаційного дослідження не передбачає та не створює жодних фінансових зобов'язань.

Голова Олександр ВАСИЛЕНКО

ДОВІДКА

про впровадження результатів дисертаційного дослідження
здобувача наукового ступеня кандидата наук з державного управління
за спеціальністю 25.00.02 — механізми державного управління
Омельченко Миколи Миколайовича
за темою: «Механізми державного управління реформуванням сектору безпеки і оборони України в контексті протидії сучасним загрозам»

Питання організаційно-управлінського забезпечення реформ у сфері безпеки і оборони набувають особливої актуальності в умовах активної фази євроатлантичної інтеграції України та необхідності приведення відповідних інституційних механізмів у відповідність до сучасних стандартів. Дисертаційне дослідження Омельченка М.М. присвячене саме цьому проблемному полю, що зумовило практичний інтерес до його результатів.

Авторська концептуальна модель інтегрованого управління реформами сектору безпеки і оборони, а також розроблена система індикативної оцінки їх ефективності використані при опрацюванні аналітичних матеріалів, пов'язаних з оцінкою стану реформування та визначенням пріоритетів подальших управлінських дій. Теоретико-методологічні напрацювання дисертанта щодо механізмів державного управління в безпековому секторі взято до уваги при підготовці пропозицій організаційного характеру, спрямованих на підвищення якості та узгодженості управлінських рішень у відповідній сфері. Систематизований автором зарубіжний досвід реформування секторів безпеки і оборони використано як методичну основу при розгляді питань адаптації управлінських процедур до практики держав — членів НАТО.

Викладені в дисертації положення підтверджують свою прикладну значущість та можуть слугувати орієнтиром для подальшого вдосконалення механізмів державного управління у сфері реформування сектору безпеки та оборони України.

Впровадження результатів дисертаційного дослідження не передбачає та не створює жодних фінансових зобов'язань.

Начальник Черкаського РУП
ГУНП в Черкаській області
полковник поліції **Дмитро КІРДЯПКІН**

ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В ЧЕРКАСЬКІЙ ОБЛАСТІ
код ЄДРПОУ 40108667
№3

ЗАТВЕРДЖУЮ
Перший проректор з навчальної роботи
Національного університету
цивільного захисту України
полковник служби цивільного захисту
Олександр ДЖУЛАЙ

«__» _____ 2026 р.

АКТ

про впровадження результатів дисертаційного дослідження здобувача Омельченка Миколи Миколайовича на тему: «Механізми державного управління реформуванням сектору безпеки і оборони України в умовах збройної агресії», що подається на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 — механізми державного управління.

Комісія у складі:

Голова — начальник кафедри управління у сфері цивільного захисту, к.т.н., доц. Землянський О.М.

Члени комісії — доцент кафедри управління у сфері цивільного захисту, д.держ.упр., доц. Хмиров І.М.; доцент кафедри управління у сфері цивільного захисту, к.держ.упр., доц. Ляшевська О.І.

Цим актом засвідчується, що результати дисертаційного дослідження Омельченка Миколи Миколайовича на тему: «Механізми державного управління реформуванням сектору безпеки і оборони України в умовах збройної агресії» (у частині концептуальної моделі оптимізації системи державного управління сектором безпеки і оборони, яка передбачає створення Національного координаційного центру безпеки (НКЦБ) при Раді національної безпеки і оборони України, а також індикативного підходу до оцінки ризиків і загроз національній безпеці України на основі деліберaційного методу ранжування ризиків) використано при викладанні та удосконаленні навчальних дисциплін «Державна безпека в контексті політики європейської інтеграції України», «Теорія та історія публічного управління та адміністрування» та «Організація управління діяльністю органів та підрозділів цивільного захисту» у межах програми підготовки здобувачів вищої освіти за спеціальністю 281 «Публічне управління та адміністрування» у Національному університеті цивільного захисту України.

Голова комісії
к.т.н., доцент — Олександр ЗЕМЛЯНСЬКИЙ

Члени комісії
д.держ.упр., доцент — Ігор ХМИРОВ
к.держ.упр., доцент — Олена ЛЯШЕВСЬКА

Додаток Б

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Омельченко М.М. Національний координаційний центр безпеки як ключовий елемент інтегрованого управління реформуванням сектору безпеки і оборони України. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2019. Вип. 1 (10). С. 461–468. https://repositsc.nuczu.edu.ua/bitstream/123456789/28954/1/Omelchenko.pdf

2. Омельченко М.М. Механізми державного управління реформуванням сектору безпеки і оборони України в період 2014–2021 років: досягнення та проблеми. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2021. Вип. 1 (14). С. 430–440. https://repositsc.nuczu.edu.ua/bitstream/123456789/25439/1/Omelchenko21.1.pdf

3. Омельченко М.М. Інституційні механізми державного управління реформуванням сектору безпеки і оборони України: регіональний вимір (2014–2021 роки). Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2021. Вип. 2 (15). С. 462–469. https://vdu-nuczu.net/ua/11-ukr/storinkaavtora/518-omelchenko-m-m-institutsijni-mekhanizmi-derzhavnogo-upravlinnya-reformuvannyam-sektoru-bezpeki-i-oboroni-ukrajini-regionalnij-vimir-2014-2021-roki

4. Omelchenko M.M., Paliukh V.V. Methodological Foundations for Diagnosing the Effectiveness of Public Administration in the Security and Defense Sector under Russian Aggression: Ukrainian Experience. Public administration and state security aspects. 2025. Vol. 2. P. 43–54. https://passa.nuczu.edu.ua/en/archive/252-paliukh-v-omelchenko-m-methodological-foundations-for-diagnosing-the-effectiveness-of-public-

administration-in-the-security-and-defense-sector-under-russian-aggression-ukrainian-experience

Особистий внесок: розроблено методичні засади діагностики ефективності державного управління у сфері безпеки та оборони в умовах збройної агресії.

5. Палюх В.В., Омельченко М.М. Управлінська синергія та виклики при міжвідомчому комплектуванні керівного складу ЗВО зі специфічними умовами навчання: аналіз адаптаційних механізмів. Успіхи і досягнення у науці. Серія: Управління та адміністрування. 2025. № 17. DOI:10.52058/3041-1254-2025-11(21)-905-914

Особистий внесок: проаналізовано адаптаційні механізми міжвідомчого комплектування керівного складу закладів вищої освіти зі специфічними умовами навчання.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Омельченко М.М. Еволюція стратегічних підходів до забезпечення енергетичної безпеки України в умовах повномасштабної війни: уроки 2022–2025 років. Матеріали IX Міжнародної науково-практичної конференції 11 листопада 2025 року Київ, 2025. С. 290-293.

7. Омельченко М.М., Тарасов С.С. Трансформація механізмів державного управління сектором безпеки і оборони: адаптація до гібридних загроз на основі зарубіжного досвіду. Матеріали І-ї Міжнародної науково-практичної конференції «Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення», 27 листопада 2025 року. Івано-Франківськ, 2025. С. 495-498.