https://doi.org/10.31891/2307-5740-2025-344-4-4
УДК: 351.751; 355.45(477)

АВГУСТИН Руслан
Західноукраїнський національний університет
https://orcid.org/0000-0003-3101-7107
e-mail: avgustyn@ukr.net

RESILIENCE-GOVERNANCE ЯК ІНСТРУМЕНТ СТІЙКОСТІ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У статті досліджується концепція resilience-governance як інструмент забезпечення стійкості публічного управління у сфері національної безпеки України в умовах гібридних загроз і затяжної стратегічної нестабільності. Обґрунтовано необхідність трансформації традиційної бюрократичної моделі управління шляхом впровадження гнучких, антикризових та мережевих підходів, які дозволяють забезпечити адаптивність, координацію та оперативність у реагуванні на багатовимірні виклики. У межах дослідження проаналізовано міжнародний досвід, національні нормативно-правові засади та практичні інституційні зрушення, що формують передумови для запровадження resilience-моделі в управлінську практику. Запропоновано цілісну концептуальну модель resilience-governance, яка інтегрує функції цифрової трансформації, суспільної мобілізації, стратегічної аналітики та інституційної стійкості. Результати дослідження можуть бути використані при розробці стратегій реформування державного управління, побудові національних систем безпеки та створенні ефективних механізмів реагування на гібридні загрози.

Ключові слова: публічне управління; національна безпека; стійкість; resilience-governance; гібридні загрози; цифрова трансформація; стратегічна аналітика; інституційна модернізація.

AVHUSTYN Ruslan
West Ukrainian National University

RESILIENCE-GOVERNANCE AS A TOOL FOR ENHANCING THE STABILITY OF PUBLIC ADMINISTRATION IN THE NATIONAL SECURITY SECTOR OF UKRAINE

The article delves into the critical concept of resilience-governance as a foundational tool for ensuring the sustainability and effectiveness of public administration within Ukraine's national security sector. This is particularly crucial in the face of ongoing hybrid threats and protracted strategic instability, which challenge traditional bureaucratic models. The study argues that the conventional, rigid administrative structures are ill-equipped to handle the complex, multi-faceted nature of modern security challenges. Therefore, it is imperative to transform these models by adopting flexible, crisis-oriented, and network-based approaches. This paradigm shift is not merely about reacting to threats but about building an inherent capacity for adaptability, coordination, and responsiveness to a dynamic and unpredictable environment. The research provides a comprehensive analysis of the prerequisites for implementing a resilience-based governance model. It scrutinizes international experience and best practices, examining how various nations have successfully integrated resilience principles into their security frameworks. Concurrently, the study conducts a detailed review of Ukraine's national legal frameworks, identifying both existing provisions that support this transformation and areas that require reform. It also investigates practical institutional shifts already underway, such as the decentralization of decision-making and the integration of new technologies, which lay the groundwork for a more resilient system.

At the core of the article is the proposal of a comprehensive conceptual model of resilience-governance. This model is not a monolithic structure but an integrated system comprising several key functions. It emphasizes the pivotal role of digital transformation, not just as a technological upgrade, but as a means to enhance data sharing, situational awareness, and the speed of response. The model also highlights the importance of civic mobilization and engagement, recognizing that national security is a collective effort that extends beyond state institutions. By fostering collaboration with civil society, volunteer groups, and the private sector, the state can tap into a vast reservoir of resources and expertise.

Furthermore, the model integrates strategic analytics as a core function. This involves leveraging advanced data analysis and forecasting to anticipate threats, identify vulnerabilities, and inform proactive policy decisions rather than simply reacting to events. Finally, the concept of institutional resilience is central, focusing on building the internal robustness of government bodies. This includes fostering a culture of continuous learning, cross-functional collaboration, and adaptive leadership.

The findings and proposed model offer significant practical utility. The results of the study are intended to serve as a valuable resource for policymakers, government officials, and researchers involved in the development of public administration reform strategies. They provide concrete recommendations for strengthening national security systems and establishing effective mechanisms for responding to the nuanced and ever-evolving landscape of hybrid threats. This work underscores the need for a forward-looking, agile, and inclusive approach to governance that can not only withstand shocks but also emerge stronger from periods of profound instability.

Keywords: public administration; national security; resilience; resilience-governance; hybrid threats; digital transformation; strategic analytics; institutional modernization.

Стаття надійшла до редакції / Received 12.07.2025
Прийнята до друку / Accepted 02.08.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасна безпекова ситуація в Україні засвідчує обмежену ефективність традиційних моделей публічного управління в умовах системних загроз державності, зумовлених повномасштабною військовою

агресією, інформаційним тиском, кіберзлочинністю, енергетичною нестабільністю та гуманітарними викликами. Поступова трансформація природи загроз – від класичних до гібридних – актуалізує потребу переосмислення підходів до державного управління у сфері національної безпеки. Зростаюча складність та динамічність криз вимагає переходу від адміністративно-ієрархічного управління до адаптивної, багаторівневої та стійкої моделі, здатної забезпечити інтеграцію секторів безпеки, кризове прогнозування, швидке реагування та координацію зусиль усіх учасників безпекового середовища.

Водночас, попри наявність стратегічних документів у сфері безпеки, таких як Стратегія національної безпеки України, Стратегія воєнної безпеки, Стратегія кібербезпеки тощо, їх практична реалізація стикається з низкою викликів: відсутність належної міжвідомчої взаємодії, недостатня нормативна підтримка горизонтальних зв'язків між ЦОВВ і регіонами, обмежене використання аналітичних інструментів при ухваленні рішень, нерівномірна цифрова трансформація публічних інституцій. Підвищення спроможності держави ефективно управляти в умовах високої невизначеності та багатовекторних загроз передбачає формування нової управлінської логіки, яка базується на стійкості (resilience), взаємодії, відкритості та цифровій мобільності.

У цьому контексті постає науково-практичне завдання – розробити концептуальну модель публічного управління, яка враховуватиме сучасні виклики, інституційну спроможність, суспільну мобілізацію та технологічні можливості для забезпечення комплексної відповіді на гібридні загрози. Відповідь на це завдання передбачає синтез теоретичних підходів, практичних кейсів, стратегічного аналізу й адаптацію міжнародного досвіду до українських реалій.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Актуальність застосування resilience-підходу в системі публічного управління національною безпекою України висвітлюється як у працях вітчизняних учених, так і в аналітичних звітах провідних міжнародних організацій. У межах українського академічного дискурсу інституційна спроможність публічної влади в умовах політичних криз і гібридної війни детально проаналізована в монографії «Інституційна (не)спроможність держави в Україні», підготовленій колективом Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України [11]. У цьому дослідженні обґрунтовано, що одним із головних чинників нестійкості державного управління є дефіцит горизонтальної взаємодії, формалізму у прийнятті рішень і відсутність механізмів адаптації до багатофакторних загроз. Водночас у межах аналітичної доповіді «Пастки інституційної спроможності у системі державної влади в Україні» [12] авторський колектив під керівництвом Г. Зеленько вказує на глибокі структурні деформації в управлінській системі, які не дозволяють реалізувати навіть наявні інструменти безпекової політики. На міжнародному рівні вагоме місце у формуванні концепції resilience-governance займають напрацювання Організації економічного співробітництва та розвитку (OECD). У звіті «More Resilient Public Administrations after COVID-19» [3] представлено систематизовану модель розвитку публічного сектору, що орієнтується на цифрову адаптивність, інституційну гнучкість і здатність до управління непередбачуваними загрозами. Аналітики наголошують, що основними ознаками стійкої адміністрації є здатність до самонавчання, стратегічної комунікації та міжрівневої координації. Ці ж принципи підтримує звіт CEPA «Resilience, Reconstruction, Recovery: The Path Ahead for Ukraine» [4], у якому конкретизовано пріоритети для України в умовах постконфліктного управління – це створення ситуаційних центрів, побудова цифрової інфраструктури безпеки та інституціоналізація співпраці між владою та громадянським суспільством. Цікавою є позиція аналітичного центру CIDOB, викладена у записці «Hybrid Resilience in Insecure Times» [5], де розглядається новітній тип стійкості, що формується не лише інституціями, а й громадянським суспільством. Автори підкреслюють, що саме взаємозалежність формальних і неформальних інституцій, зокрема волонтерських ініціатив та цифрових спільнот, створює основу гібридної резильєнтності. Дослідження цього типу відкривають шлях до концептуального поєднання державної стійкості та суспільної мобілізації в межах публічної політики безпеки. На регіональному рівні трансформація управлінських підходів у сфері національної безпеки не може бути реалізована без впровадження стандартів захисту критичної інфраструктури. Європейська Комісія в Директиві CER [10] зобов'язує держави-члени запровадити принципи багаторівневої координації, інституційну готовність і мінімальні стандарти оперативного реагування, що можуть бути адаптовані до українського безпекового контексту. В Україні зусилля в кіберсфері координуються Національним координаційним центром кібербезпеки при РНБО, який у своєму щорічному звіті [9] фіксує зростання кількості цільових атак на органи державної влади. Центр наголошує на необхідності посилення цифрової стійкості органів публічної влади, розвитку ситуаційно-аналітичних центрів та запровадження механізмів автоматизованого обміну даними в режимі реального часу. Соціальний вимір стійкості висвітлює Програма розвитку ООН в Україні (UNDP Ukraine), яка у Community Resilience Framework [8] аналізує можливості активізації громад задля попередження або подолання наслідків надзвичайних ситуацій. Зокрема, наголошується на важливості довіри, локального лідерства, відкритих цифрових платформ і підтримки горизонтальних мереж безпеки. У цьому ж напрямі Transparency International Ukraine [7] ідентифікує ризики процедурної непрозорості, які підривають спроможність публічної влади до ефективного управління в умовах воєнного стану. Таким чином, огляд актуальних досліджень і публікацій свідчить про зростаючу роль

resilience-парадигми як нової управлінської логіки, що поєднує антикризову стійкість, цифрову трансформацію, міжвідомчу інтеграцію та суспільну мобілізацію. У той же час, окреслюється потреба у створенні єдиної інтегрованої моделі resilience-governance, яка забезпечувала б не лише реакцію на загрози, а й стабільність та передбачуваність публічного управління в умовах стратегічної нестабільності. .

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Незважаючи на значну кількість досліджень у сферах публічного управління, безпекових студій, цифрової трансформації та кризового менеджменту, низка концептуальних і прикладних аспектів управлінської стійкості в умовах гібридних загроз залишається недостатньо висвітленою. Передусім йдеться про відсутність цілісної моделі публічного управління, яка б інтегрувала механізми антикризового реагування, цифрову інтеграцію, аналітичну підтримку прийняття рішень та залучення громадян до процесів безпекового управління. Існуючі наукові підходи часто залишаються фрагментарними, орієнтованими на окремі інституційні або функціональні елементи, без належної уваги до синергії між ключовими суб'єктами управління – державою, бізнесом, громадянським суспільством та безпековими структурами.

Недостатньо розробленими залишаються також інструменти оцінки інституційної спроможності до забезпечення безперервного функціонування органів влади в умовах системних ризиків та багаторівневих загроз. У науковій літературі бракує уніфікованих індикаторів управлінської стійкості, які могли б бути адаптовані до національної системи стратегічного моніторингу й оцінювання. Практично не дослідженими є також цифрові рішення для безпеки громад, алгоритми швидкої координації між волонтерськими ініціативами та державними структурами, а також моделі інституціоналізації стратегічної комунікації як складової публічного управління в умовах стратегічної нестабільності.

Відтак, актуалізується потреба у формуванні багаторівневої, адаптивної та аналітично підкріпленої управлінської моделі, що дозволить підвищити ефективність публічної влади в умовах гібридних загроз, забезпечити інтегрованість державних і громадських безпекових зусиль та підвищити рівень суспільної консолідації. Саме цим нерозв'язаним аспектам – синтезу стійкості, цифрової трансформації, громадянської мобілізації та управлінської аналітики – присвячено дану статтю.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є теоретичне обґрунтування та практичне моделювання resilience-governance як інструменту забезпечення управлінської стійкості у сфері національної безпеки України в умовах гібридних загроз і затяжної стратегічної нестабільності. У межах поставленої мети передбачено аналіз сучасного стану публічного управління у сфері безпеки, виявлення чинників інституційної вразливості, порівняльну оцінку управлінської спроможності регіонів, а також розроблення концептуальної моделі resilience-governance, що поєднує функції цифрової трансформації, громадянської мобілізації, стратегічної аналітики та міжвідомчої координації. Особливу увагу приділено інтеграції елементів антикризового управління, стратегічної комунікації та прозорості прийняття рішень у процесах забезпечення національної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Публічне управління у сфері національної безпеки розглядається як складова загальної системи державного управління, що забезпечує здатність держави ефективно реагувати на внутрішні та зовнішні загрози, підтримувати стабільність, територіальну цілісність, політичну незалежність та правопорядок у суспільстві. Водночас, на відміну від класичних адміністративних функцій, безпекове управління має інтегративний характер, що передбачає міжгалузеву координацію, швидку адаптацію до змін зовнішнього середовища, а також високий рівень стратегічного передбачення. У цьому контексті публічне управління у сфері національної безпеки функціонує не лише як система управлінських впливів, але й як інституційна інфраструктура, що формує стійкість держави в умовах криз.

Методологічною основою дослідження виступає системний підхід, який дозволяє розглядати публічне управління як багаторівневу та динамічну систему взаємодії інституцій, процедур, правових норм і управлінських практик, що функціонують у політичному, безпековому, економічному та соціальному середовищі. У межах цього підходу національна безпека визначається як цілісний об'єкт публічного управління, що охоплює не лише оборонну сферу, але й питання інформаційної, кібернетичної, економічної, енергетичної, екологічної, соціальної та гуманітарної безпеки.

Окреме значення у структурі дослідження має концепція resilience (стійкості), що активно використовується в країнах НАТО та ЄС. Ця концепція базується на здатності держави та суспільства адаптуватися до несподіваних шоків, підтримувати функціонування основних інституцій під час кризи та швидко відновлюватися після неї. У публічному управлінні це означає запровадження таких інструментів як кризове управління, стратегічне планування, сценарний аналіз, управління ризиками та превентивне прогнозування.

Для цілей порівняльного аналізу можна використати таблицю 1, яка ілюструє відмінності між класичним адміністративним управлінням та безпеково-орієнтованим публічним управлінням:

Таблиця 1.

Відмінності між класичним публічним управлінням та управлінням у сфері національної безпеки

Ознака	Класичне публічне управління	Управління у сфері національної безпеки
Основна функція	Адміністративне забезпечення	Реагування на загрози та захист держави
Характер середовища	Відносно стабільне	Нестабільне, динамічне, кризове
Механізми впливу	Нормативно-правові	Кризові, превентивні, міжвідомчі
Основна мета	Соціальне обслуговування	Безпекова стійкість і захист державності
Домінуючий тип управлінських дій	Планово-організаційний	Антикризовий, оперативно-реактивний
Ключові інституції	ЦОВВ, ОМС	СБУ, ЗСУ, РНБО, МВС, ОВА, ТРО
Взаємодія з громадськістю	Через адміністративні процедури	Через мобілізацію, волонтерство, участь у безпеці
Орієнтація на результат	Вирішення соціальних потреб	Збереження державності, національної єдності

Джерело: узагальнено автором на основі [1], [2].

Як свідчать дані таблиці 1, публічне управління у сфері національної безпеки дедалі більше орієнтується на використання управлінських інструментів, які не є типовими для класичної бюрократичної моделі, що свідчить про поступову трансформацію управлінських практик у бік гнучкості, міждисциплінарності та адаптивності. Така трансформація вимагає не лише зміни інституційних структур, але й нових підходів до управлінської культури, орієнтованої на ризик-мислення, інформаційно-аналітичну підтримку прийняття рішень та динамічну модель управління, що передбачає постійний моніторинг загроз і оновлення сценаріїв дій.

У науковому вимірі публічне управління у сфері національної безпеки розглядається як синтез двох категорій: «governance» – управління багатьма учасниками процесу з делегуванням функцій, і «security management» – забезпечення безперервного захисту критично важливих систем. Українські реалії вимагають гібридної моделі, що поєднує нормативне регулювання, політичне лідерство, технологічну модернізацію, стратегічну комунікацію та громадянську мобілізацію.

Сучасний стан управлінських механізмів забезпечення національної безпеки в Україні формувався під впливом зовнішньої збройної агресії, внутрішньої політичної турбулентності, кризових економічних процесів та зростаючих очікувань суспільства щодо ефективності державного реагування. Після початку російсько-української війни у 2014 році та особливо після повномасштабного вторгнення у 2022 році, система публічного управління була змушена перейти до мобілізаційної логіки, яка передбачає швидке ухвалення рішень, координацію зусиль на національному, регіональному та місцевому рівнях, а також залучення позаурядових суб'єктів до безпекових процесів. Така ситуація оголила як сильні, так і слабкі сторони української моделі безпекового управління, потребуючи системного перегляду її ефективності.

На законодавчому рівні держава забезпечила базу для функціонування управлінських інституцій у сфері безпеки, ухваливши низку ключових документів, зокрема: Закон України «Про національну безпеку» (2018), Стратегію національної безпеки України (2020), Стратегію воєнної безпеки (2021), Стратегію кібербезпеки (2021), а також нову редакцію Закону України «Про основи національного спротиву» (2025). Ці документи засвідчили відхід від вузького секторального розуміння безпеки на користь системного, міжвідомчого підходу, який охоплює сфери оборони, безпеки, правопорядку, дипломатії, інформації, кіберпростору та критичної інфраструктури.

Однак практична реалізація цих стратегій демонструє неоднорідність результатів. Одним із ключових викликів залишається координація між ЦОВВ, місцевими адміністраціями, сектором безпеки та оборони, а також із громадянським суспільством. Часто відсутність чітких механізмів горизонтальної взаємодії призводить до дублювання функцій, неефективного використання ресурсів або сповільнення реагування на загрози. Зокрема, це спостерігалося у перші місяці повномасштабного вторгнення, коли територіальна оборона, гуманітарна логістика та місцеві органи влади не мали уніфікованого алгоритму взаємодії.

У сфері цифрового управління безпекою позитивним кейсом є впровадження систем «Дія», «ЄДокумент», «Розвідка.Інфо», аналітичних платформ СБУ, НГУ та РНБО, а також створення інформаційно-аналітичних центрів при ОВА. Проте, стан інтеграції цих систем залишається недостатнім – відсутність єдиного центру управління цифровими потоками ускладнює стратегічне управління інформаційною безпекою.

Окремо слід відзначити нерівномірність функціональної спроможності регіонів. У табличному вигляді це можна представити як порівняльну характеристику управлінської реакції у різних областях у період 2022–2023 років – таблиця 2.

Наведені дані свідчать про необхідність підвищення рівня стандартизації управлінських рішень та цифрової трансформації у сфері безпеки на регіональному рівні. Також актуальною залишається проблема кадрового забезпечення – як в управлінських структурах, так і в оперативних підрозділах, що формують першу лінію реагування на кризові ситуації. Потребує перегляду система підготовки та професійного розвитку фахівців з безпекового управління, яка має враховувати компетентнісний підхід, знання міжнародного гуманітарного права, кризового менеджменту, кіберзахисту та комунікаційної безпеки.

Таблиця 2.

Рівень управлінської спроможності регіонів України до реагування на безпекові загрози у 2022–2023 рр.

Область	Швидкість реагування	Наявність координаційного штабу	Залучення громадськості	Цифрові інструменти	Оцінка стійкості (1–5)
Київська	Висока	Так	Високий рівень	Високий	5
Дніпропетровська	Висока	Так	Середній рівень	Середній	4
Львівська	Середня	Так	Високий рівень	Високий	4
Харківська	Висока	Частково	Низький рівень	Середній	3
Чернівецька	Низька	Ні	Слабке залучення	Низький	2
Одеська	Середня	Частково	Середній рівень	Слабкий	3

Джерело: сформовано за [13]

Загалом аналіз сучасного стану дозволяє стверджувати, що Україна має стратегічний каркас безпекового управління, однак його ефективна реалізація гальмується недостатньою інтеграцією, інституційною інерцією, нестачею аналітичної підтримки прийняття рішень та обмеженим доступом до оперативної інформації на місцевому рівні.

Функціонування системи публічного управління у сфері національної безпеки України перебуває на перехресті глибоких трансформаційних процесів, які супроводжуються необхідністю інтеграції традиційних моделей управління з новітніми викликами гібридного типу. Станом на сьогодні інституційна архітектура безпеки визначається як багаторівнева, динамічна та поліцентрична, проте в межах її реалізації все ще спостерігається фрагментованість та обмежена здатність до міжвідомчого синтезу. Основу безпекового сектору складають такі суб'єкти як Президент України, Верховна Рада України, Кабінет Міністрів, Рада національної безпеки і оборони, Міністерство оборони, Служба безпеки України, Міністерство внутрішніх справ, Національна гвардія, розвідувальні органи, органи місцевого самоврядування та територіальні громади, проте відсутність чітких механізмів взаємодії між ними у реальному часі обмежує ефективність реагування на комплексні загрози.

Незважаючи на наявність Стратегії національної безпеки України (2020), яка заклала фундамент «всеосяжної безпеки» (comprehensive security), інституційні бар'єри зумовлюють обмежений рівень синергії у прийнятті управлінських рішень. Як показує практика, в умовах загострення ситуації основні управлінські важелі переміщуються у сферу надзвичайного адміністрування – через режим воєнного стану, надзвичайні повноваження військових адміністрацій, оперативні рішення РНБО. Такий підхід ефективний у короткостроковій перспективі, однак обмежений у здатності до стратегічного планування та адаптації до тривалих форм конфлікту.

Особливої уваги заслуговує функціонування системи територіальної оборони, яка після 2022 року набула нової ролі у структурі публічного безпекового управління. З одного боку, ТРО стала дієвим інструментом протидії агресії та локальної стабілізації безпекової ситуації, з іншого – управлінські механізми, які визначають її фінансування, логістику, кадрове забезпечення та інтеграцію в систему ЦОВВ, залишаються неуніфікованими, що призводить до розбалансування між регіонами. Визначальною проблемою є відсутність усталених протоколів дій між ТРО, військовими комендатурами, місцевими адміністраціями та іншими службами реагування.

Іншим викликом є низький рівень адаптації органів державної влади до роботи в умовах інформаційної війни та кіберзагроз. Попри прийняття Стратегії кібербезпеки України (2021), система управління реагуванням на кібератаки залишається розпорошеною, а механізми оперативного інформування між держструктурами не є достатньо надійними. Зокрема, у період 2022–2023 років були зафіксовані спроби дезорганізувати роботу ОМС, вивести з ладу системи «Дія», атакувати державні реєстри, однак відсутність чітких алгоритмів комунікації між кіберпідрозділами Мінцифри, СБУ, НГУ, НКЦК (Національного координаційного центру кібербезпеки) ускладнювала своєчасну локалізацію ризиків.

Аналіз також виявляє дисбаланс між інституційною відповідальністю та реальним ресурсним забезпеченням безпекових функцій на місцях. Органи місцевого самоврядування, які отримали значну частину повноважень з координації гуманітарної допомоги, евакуації населення, взаємодії з волонтерами, досі не мають чітко закріплених бюджетних ліній та нормативних регламентів для здійснення цих повноважень у межах правового поля. Часто в екстрених умовах органи ОМС змушені діяти поза рамками нормативів, що формує потенційні корупційні ризики та правову невизначеність.

Для подальшого удосконалення управлінських механізмів важливим є врахування міжнародного досвіду, зокрема моделей безпекового управління Ізраїлю, Литви, Польщі, Фінляндії, які за останні роки продемонстрували ефективність у протидії гібридним загрозам. Спільною рисою цих країн є впровадження принципу whole-of-government approach – підходу «всією владою», коли безпека є інтегрованою функцією усіх державних інституцій, включно з органами охорони здоров'я, освіти, місцевого самоврядування, IT-сектору та приватного бізнесу. Для України перспективним є формування аналітичного центру (national fusion center), що забезпечуватиме обмін інформацією між секторами безпеки у реальному часі та слугуватиме платформою для інтегрованого управлінського реагування.

На цьому тлі особливої ваги набуває підготовка професійних кадрів, здатних працювати на стику державного управління, безпеки, кризової комунікації, гуманітарного менеджменту та цифрової трансформації. Потреба у створенні багаторівневої системи підготовки кадрів для сектору безпеки з акцентом на антикризове управління, лідерство в умовах невизначеності, практики стратегічної комунікації та інформаційної гігієни, є однією з ключових умов підвищення ефективності безпекового управління на рівні регіонів і центрів прийняття рішень.

Таким чином, поточний стан управлінських механізмів безпеки в Україні демонструє тенденцію до еволюційного розвитку, що вимагає пришвидшення процесів цифрової інтеграції, стандартизації протоколів взаємодії, інституційної гнучкості та формування культури стратегічного управління, в якій національна безпека постає не як окрема функція, а як наскрізна координата всієї публічної політики.

В умовах сучасних загроз, які мають гібридний, системний і пролонгований характер, публічне управління у сфері національної безпеки має змінити свою концептуальну основу. Замість домінування реактивного адміністрування, орієнтованого на усунення наслідків криз, необхідним є перехід до моделі управління, що забезпечує передбачення, запобігання, адаптацію, швидке відновлення та соціальну згуртованість. Саме тому resilience-підхід – як концепція управлінської стійкості – виходить на передній план у сучасному державному управлінні. Його імплементація дозволяє перетворити фрагментовану ієрархічну систему в інтегровану, адаптивну й інноваційно спроможну модель, що базується на довірі, відкритості, технологічній гнучкості та соціальній мобілізації.

Важливо не лише визначити цільовий орієнтир такої трансформації, але й окреслити системні напрями змін, які повинні охоплювати як інституційний каркас, так і інформаційну інфраструктуру, а також соціальний компонент безпеки. Трансформація публічного управління у зазначеному векторі повинна розглядатися як багаторівнева реформа, яка охоплює центральні органи влади, регіональні адміністрації, місцеве самоврядування та громадянське суспільство у форматі партнерської взаємодії.

Інституційна модернізація публічного управління крізь призму resilience-підходу. Концепт resilience-стійкості – в сучасному управлінському дискурсі передбачає здатність інституцій адаптуватися, ефективно функціонувати під впливом зовнішніх шоків і швидко відновлюватися після них. У сфері національної безпеки та публічного управління це означає перехід від реактивного до проактивного управління, в основі якого – запобігання кризам, а не лише ліквідація їхніх наслідків. Для України, яка перебуває в умовах війни, застосування resilience-підходу передбачає кардинальну модернізацію управлінських структур на рівні держави, регіонів і громад із фокусом на стійкість інституцій, гнучкість адміністративних процедур, горизонтальну координацію та обов'язкове врахування ризиків у процесі планування.

Один із першочергових напрямів інституційної трансформації полягає у створенні міжвідомчих координаційних центрів безпекової стійкості (Resilience Coordination Units), що будуть діяти при ОДА/ОВА та мати мандат на аналітичну оцінку загроз, комунікацію з громадськістю, управління ресурсами у надзвичайних ситуаціях та підтримку кіберінфраструктури. Такі структури повинні стати центрами тяжіння для інтеграції функцій ЦОВВ, служб ДСНС, СБУ, Міноборони, ТРО, а також приватного сектору, який має доступ до стратегічних комунікацій, енергетики, цифрових технологій. У цьому контексті держава повинна стимулювати моделі public-private partnership (PPP) у безпековій сфері – зокрема, у напрямі захисту критичної інфраструктури, зберігання даних, створення резервів.

Реформування потребує і сама нормативно-правова основа управління. Чинне законодавство України значною мірою зорієнтоване на централізовану вертикаль, тоді як виклики сучасної війни вимагають посилення горизонтальних управлінських спроможностей, делегування повноважень, гнучких бюджетних механізмів та правових норм, що дозволяють приймати рішення в умовах високої невизначеності. Наприклад, доцільним є впровадження спеціального законодавства про «управлінську стійкість» (Resilience Governance Act), що закріпить базові вимоги до процедур безперервності роботи органів публічної влади, їхньої IT-інфраструктури, захисту персоналу, документів та систем критичного реагування.

У контексті інституційної модернізації одним із індикаторів прогресу може стати рівень готовності до управлінського відновлення після кризи. У таблиці 3 подано порівняння критеріїв інституційної стійкості.

Таблиця 3.

Ознаки інституційної стійкості в системі публічного управління

Критерій	Слабка система	Стійка система
Наявність плану безперервності	Відсутній або формальний	Актуалізований, багаторівневий
Залучення громадськості	Епізодичне, декларативне	Системне, зворотний зв'язок
Інформаційна аналітика	Ручне, фрагментарне	Системне, з аналітичною підтримкою
Кадрова стабільність	Текучість кадрів, слабка мотивація	Кваліфікований, вмотивований персонал
Цифрові резерви	Відсутні	Архівування, хмарні копії
Рівень міжвідомчої взаємодії	Слабкий, конфліктний	Інституалізована координація

Джерело: сформовано на основі [12]

Цифрова трансформація та аналітичне забезпечення управління національною безпекою. Одним із найпотужніших важелів формування стійкої моделі управління є цифровізація, яка не лише автоматизує рутинні процеси, а й відкриває нові горизонти для стратегічного управління, прогнозування ризиків,

моделювання сценаріїв і прийняття рішень на основі даних. В умовах гібридної війни держава має спиратися не на інтуїтивну логіку реагування, а на data-driven governance – управління, засноване на постійній обробці, аналізі та візуалізації даних з відкритих і закритих джерел.

Ключовим кроком у цьому напрямі має стати впровадження Національної інтегрованої платформи безпекових даних, що акумулюватиме дані з сектору оборони, поліції, кіберпростору, органів місцевого самоврядування, гуманітарного сектору, геоінформаційних систем. На її базі доцільно формувати ситуаційні аналітичні центри при Кабінеті Міністрів і ОВА, здатні щоденно генерувати візуалізовані карти загроз, пропонувати сценарні моделі розвитку ситуації, оцінювати індекси вразливості громад. Такі аналітичні центри мають тісно співпрацювати з науковими установами, зокрема Інститутом стратегічних досліджень, Центром кібербезпеки, профільними кафедрами ВНЗ.

Цифрова стійкість передбачає не лише створення нових ІТ-рішень, а й побудову багаторівневої інфраструктури безпеки, включно з хмарними резервними системами, протоколами кіберзахисту, захищеними каналами зв'язку, механізмами швидкого відновлення систем після атаки. Зокрема, у системах «Дія», «Трембіта», «Безпечне місто», «ЄЗахист» має бути закладено резервне адміністрування, мультиканальність та інтеграція з платформами кіберспостереження. Такі елементи повинні стати обов'язковими для всіх органів виконавчої влади.

На цьому етапі також слід впровадити показники цифрової безпекової готовності територіальних громад, аналогічно до індексу цифрової трансформації. Це дозволить визначати найбільш вразливі ОТГ, надавати їм технічну допомогу, а також спрямовувати ресурси у пріоритетні зони. Цифровізація має бути не самоціллю, а інструментом забезпечення національної стійкості.

Інтеграція суспільства, громадянської безпеки та стратегічної комунікації в єдину модель управлінської стійкості. У сучасній парадигмі національної безпеки держави вже недостатньо мати лише ефективні інституції або добре оснащені силові структури – фундаментом стійкої безпекової системи стає суспільство, його мобілізована спроможність, адаптивність до загроз, довіра до влади та здатність до самоорганізації. Це зумовлює необхідність інтеграції громадянської складової у систему публічного управління, що має реалізовуватися не на рівні декларацій, а як системний управлінський інструмент – *громадянська безпека* (civil security) як частина всеосяжної безпеки (comprehensive security).

Однією з найсильніших рис українського суспільства, продемонстрованих у 2022–2024 роках, стала мережевість волонтерського руху, горизонтальна мобілізація громад, участь бізнесу, університетів і неурядових організацій у безпекових процесах. Проте формально система публічного управління здебільшого не включає ці суб'єкти до структурованої моделі взаємодії. Зокрема, відсутні чіткі протоколи реагування, нормативна база взаємодії з волонтерськими фондами, механізми верифікації допомоги, координації логістичних ланцюгів у надзвичайних ситуаціях. Це призводить до дублювання функцій, неефективного витрачання ресурсів та, в окремих випадках, – навіть до паралельного управління поза державною юрисдикцією.

Для формування стійкого публічного управління у сфері безпеки необхідним є інституційне оформлення громадянської компоненти у вигляді:

– центрів безпеки громади,

– місцевих кризових координаційних рад,

– мережевих штабів самозахисту,

– програм підготовки громадян до реагування на НС (на кшталт «громадянської оборони»).

При цьому на рівні громади має бути реалізовано комплексну модель «community resilience», яка включає: захист критичної інфраструктури, кібергігієну, комунікаційну безпеку, психологічну готовність, підтримку вразливих категорій населення, готовність до евакуації. Держава, у свою чергу, повинна надати місцевому самоврядуванню інструменти бюджетної гнучкості, резервних фондів, а також доступ до єдиної цифрової платформи реагування.

Окремий, стратегічно важливий елемент – *стратегічна комунікація*. Саме комунікація визначає ступінь довіри до влади, мобілізаційний потенціал суспільства, стійкість до дезінформації. У цьому контексті стратегічна комунікація є не лише інформаційною політикою, а частиною управління безпековою поведінкою громадян. Держава має переходити від реактивної інформаційної роботи (спростування фейків) до проактивного формування спільної інформаційної реальності, яка базується на прозорості дій, поясненні рішень, постійному зворотному зв'язку.

Варто впроваджувати *стратегії ризик-комунікацій*, що широко застосовуються в управлінні надзвичайними ситуаціями в ЄС. Вони дозволяють структурувати інформаційні потоки, підготувати населення до ризиків, знизити паніку в кризовий момент, утримати соціальну єдність. Дієвим прикладом є спільні кампанії органів влади та незалежних медіа з підготовки до блекаутів, кібератак чи біологічних загроз. Стратегічна комунікація має бути інтегрована у загальну систему державного управління як окремий функціональний модуль, з виділенням відповідальних осіб на рівні міністерств, ОДА, військових адміністрацій, а також посиленням аналітичної підтримки для ідентифікації інформаційних загроз.

Окрему увагу варто приділити формуванню культури безпеки серед населення. Це – процес довготривалий, але критично важливий. Школа, ЗВО, соціальні медіа, інститути соціального виховання

мають формувати розуміння того, що безпека – це не лише справа армії чи поліції, а відповідальність кожного. Державна політика має передбачати програми з розвитку критичного мислення, протидії маніпуляціям, цифрової грамотності, а також поширення знань про механізми участі у безпеці.

Таким чином, публічне управління майбутнього має базуватись на *трикутнику стійкості: інституції – цифрова інфраструктура – мобілізоване суспільство.* Лише за умов інтеграції цих елементів, прозорості рішень, відкритості даних і постійної взаємодії з громадянами держава зможе вистояти перед гібридними загрозами та сформувати ефективну систему управління національною безпекою у поствоєнний період.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Результати проведеного дослідження підтвердили, що сучасна модель публічного управління у сфері національної безпеки України не відповідає рівню складності та динамічності актуальних загроз. Умови повномасштабної війни, ескалація гібридних викликів, зростання кіберризиків, інформаційних впливів та уразливості критичної інфраструктури актуалізують потребу переходу від фрагментованих реактивних механізмів до цілісної системи управління, яка спирається на принципи управлінської стійкості. Концепція resilience-governance, обґрунтована в статті, репрезентує інноваційну управлінську парадигму, що поєднує інституційну адаптивність, цифрову трансформацію, стратегічне аналітичне забезпечення, міжвідомчу координацію та залучення громадянського суспільства до процесів безпекового управління.

Обґрунтовано, що фундаментальними напрямами трансформації виступають: модернізація управлінських структур через створення кризових координаційних центрів та функціональних рад безпеки; розвиток цифрових інфраструктур управління, заснованих на аналітичних платформах та даних реального часу; формування моделі громадянської безпеки як постійного елементу публічної політики; упровадження стратегічної комунікації як механізму зміцнення суспільної довіри та управлінської легітимності в умовах невизначеності. Запропонована в дослідженні трирівнева модель resilience-governance синтезує інституційну модернізацію, цифрову трансформацію та суспільну інтеграцію в єдину концепцію стійкого управління.

Водночас напрацьовані у дослідженні результати відкривають перспективи для подальших наукових розвідок, зокрема: розроблення системи прикладних індикаторів вимірювання управлінської стійкості на різних рівнях; моделювання сценаріїв реагування органів влади на багатовимірні кризові події; дослідження механізмів інституціоналізації громадянської участі у безпекових процесах на місцевому рівні; вивчення архітектури цифрових платформ як інфраструктурного підґрунтя resilience-підходу. Особливу цінність становитиме емпіричний аналіз пілотних ініціатив з апробації resilience-governance у регіонах України та вивчення можливостей імплементації кращих міжнародних практик адаптивного та антикризового управління в українському безпековому контексті.

Література

1. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 р. № 392/2020 [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/3922020-35037

2. Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 р. № 447/2021 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021

3. OECD. More Resilient Public Administrations after COVID-19: Lessons from using the CAF 2020. OECD Public Governance Policy Papers, No. 29. Paris: OECD Publishing, 2023. 32 p. [Електронний ресурс]. – Режим доступу: https://www.oecd.org/publications/more-resilient-public-administrations-after-covid-19-4d50e035-en.htm

4. CEPA. Resilience, Reconstruction, Recovery: The Path Ahead for Ukraine. Center for European Policy Analysis, April 2024. 21 p. [Електронний ресурс]. – Режим доступу: https://cepa.org/wp-content/uploads/2024/04/Ukraine-Resilience-Reconstruction-Recovery.pdf

5. Hybrid Resilience in Insecure Times: Russia's War and Ukrainian Society. CIDOB Notes Internacionals, № 281. Barcelona: CIDOB, 2023. 8 p. [Електронний ресурс]. – Режим доступу: https://www.cidob.org/en/publications/publication_series/notes_internacionals/281/hybrid_resilience_in_insecure_times

6. Szücs G., Báger G. Multi-level Public Administration in the Context of Hybrid Threats. 2022. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/367139758

7. Ризики корупції в умовах воєнного стану: аналітична доповідь / кол. авт. – Київ: Transparency International Україна, 2023. 40 с. [Електронний ресурс]. – Режим доступу: https://ti-ukraine.org/research

8. Community Resilience Framework. UNDP Ukraine, 2022. 24 p. [Електронний ресурс]. – Режим доступу: https://www.undp.org/ukraine/publications/community-resilience

9. Огляд стану кіберзахисту державного сектору України у 2023 році / Національний координаційний центр кібербезпеки при РНБО України. – Київ: НКЦК, 2023. 36 с. [Електронний ресурс]. – Режим доступу: https://ncscc.gov.ua

10. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the

Resilience of Critical Entities. Official Journal of the European Union. L 333, 27.12.2022, p. 164–196. [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557

11. Інституційна (не)спроможність держави в Україні: як розірвати замкнене коло: монографія / за заг. ред. Г. І. Зеленько. – Київ: ІПіЕнД ім. І. Ф. Кураса НАН України, 2025. 180 с. [Електронний ресурс]. – Режим доступу: https://ipiend.gov.ua/wp-content/uploads/2025/04/Instytutsijna-spromozhnist-derzhavy.pdf

12. Пастки інституційної спроможності у системі державної влади в Україні: аналітична доповідь / кол. авт.: Галина Зеленько (кер., наук. ред.) та ін. – Київ: ІПіЕнД ім. І. Ф. Кураса НАН України, 2025. 64 с. [Електронний ресурс]. – Режим доступу: https://ipiend.gov.ua/wp-content/uploads/2025/01/Zapyska_Pastky-spromozhnosti.pdf

13. Суходоля О. М. Формування системи освіти, підготовки та перепідготовки персоналу у сфері захисту критичної інфраструктури: аналітична доповідь. – Київ: НІСД, 2025. 92 с. [Електронний ресурс]. – Режим доступу: https://doi.org/10.53679/NISS-analytrep.2025.01

References

1. Strategiia natsionalnoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 14 veresnia 2020 r. № 392/2020 [Electronic resource]. – Available at: https://www.president.gov.ua/documents/3922020-35037

2. Strategiia kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 26 serpnia 2021 r. № 447/2021 [Electronic resource]. – Available at: https://zakon.rada.gov.ua/laws/show/447/2021

3. OECD. More Resilient Public Administrations after COVID-19: Lessons from using the CAF 2020. OECD Public Governance Policy Papers, No. 29. Paris: OECD Publishing, 2023. 32 p. Available at: https://www.oecd.org/publications/more-resilient-public-administrations-after-covid-19-4d50e035-en.htm

4. CEPA. Resilience, Reconstruction, Recovery: The Path Ahead for Ukraine. Center for European Policy Analysis, April 2024. 21 p. Available at: https://cepa.org/wp-content/uploads/2024/04/Ukraine-Resilience-Reconstruction-Recovery.pdf

5. Hybrid Resilience in Insecure Times: Russia's War and Ukrainian Society. CIDOB Notes Internacionals, № 281. Barcelona: CIDOB, 2023. 8 p. Available at: https://www.cidob.org/en/publications/publication_series/notes_internacionals/281/hybrid_resilience_in_insecure_times

6. Szücs G., Báger G. Multi-level Public Administration in the Context of Hybrid Threats. 2022. Available at: https://www.researchgate.net/publication/367139758

7. Ryzyky koruptsii v umovakh voiennoho stanu: analitychna dopovid / kol. avt. – Kyiv: Transparency International Ukraine, 2023. 40 p. Available at: https://ti-ukraine.org/research

8. Community Resilience Framework. UNDP Ukraine, 2022. 24 p. Available at: https://www.undp.org/ukraine/publications/community-resilience

9. Ohliad stanu kiberzakhystu derzhavnoho sektoru Ukrainy u 2023 rotsi / Natsionalnyi koordynatsiinyi tsentr kiberbezpeky pry RNBO Ukrainy. – Kyiv: NKTsK, 2023. 36 p. Available at: https://ncscc.gov.ua

10. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities. Official Journal of the European Union. L 333, 27.12.2022, p. 164–196. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557

11. Instytutsijna (ne)spromozhnist derzhavy v Ukraini: yak rozirvaty zamknene kolo: monohrafiia / za zah. red. H. I. Zelenko. – Kyiv: IPIEND im. I. F. Kurasa NAN Ukrainy, 2025. 180 p. Available at: https://ipiend.gov.ua/wp-content/uploads/2025/04/Instytutsijna-spromozhnist-derzhavy.pdf

12. Pastky instytutsijnoi spromozhnosti u systemi derzhavnoi vlady v Ukraini: analitychna dopovid / kol. avt.: Halyna Zelenko (ker., nauk. red.) ta in. – Kyiv: IPIEND im. I. F. Kurasa NAN Ukrainy, 2025. 64 p. Available at: https://ipiend.gov.ua/wp-content/uploads/2025/01/Zapyska_Pastky-spromozhnosti.pdf

13. Sukhodolia O. M. Formuvannia systemy osvity, pidhotovky ta perepidhotovky personalu u sferi zakhystu krytychnoi infrastruktury: analitychna dopovid′. – Kyiv: NISD, 2025. 92 s. [Elektronnyi resurs]. – Rezhym dostupu: https://doi.org/10.53679/NISS-analytrep.2025.01