

УДК 35.351

DOI <https://doi.org/10.51547/ppp.dp.ua/2025.2.5>

Міщенко Дмитро Анатолійович,

доктор наук з державного управління, професор,

професор кафедри маркетингу

Університету митної справи та фінансів

ORCID ID: 0000-0003-0278-7209

Міщенко Людмила Олександрівна,

доцент кафедри економіки та менеджменту

ЗВО ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»

ORCID ID: 0000-0002-0163-0763

МОДЕРНІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ ЯК ІНСТРУМЕНТУ НЕЙТРАЛІЗАЦІЇ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

MODERNIZATION OF PUBLIC ADMINISTRATION AS A TOOL FOR NEUTRALIZING THREATS TO NATIONAL SECURITY

У статті досліджується проблематика модернізації публічного управління в Україні в умовах зростаючих та динамічних загроз національній безпеці. Аналізуються ключові виклики, що постають перед системою державного управління, зокрема гібридна агресія, кіберзагрози, економічна нестабільність, екологічні ризики та інформаційні війни. Акцентовується увага на необхідності трансформації традиційних підходів до управління, інтеграції інноваційних технологій та розробки адаптивних механізмів реагування на кризові ситуації. Розглядаються сучасні міжнародні практики та стандарти, що можуть бути імplementовані в українському контексті для підвищення ефективності та гнучкості публічного сектору. Обґрунтовується важливість розвитку інституційної спроможності, посилення координації між державними органами, залучення громадянського суспільства та міжнародних партнерів до процесів формування та реалізації державної політики у сфері національної безпеки. Пропонуються конкретні напрями модернізації, включаючи цифровізацію державних послуг, впровадження систем ризик-менеджменту, посилення аналітичної складової та розвиток кадрового потенціалу. Стаття підкреслює, що успішна модернізація публічного управління є критично важливою для забезпечення стійкості держави, її здатності протистояти сучасним загрозам та ефективно захищати національні інтереси в умовах глобальних трансформацій. Особлива увага приділяється питанню підвищення довіри суспільства до державних інституцій та забезпечення прозорості у прийнятті управлінських рішень, що є запорукою успішної реалізації стратегічних завдань у сфері національної безпеки.

Ключові слова: публічне управління, національна безпека, модернізація, національні інтереси, кібербезпека, цифровізація, стійкість, ризик-менеджмент, інституційна спроможність.

This article explores the modernization of public administration in Ukraine amidst escalating and dynamic national security threats. It analyzes key challenges facing the public governance system, including hybrid aggression, cyber threats, economic instability, environmental risks, and information warfare. The paper emphasizes the necessity of transforming traditional governance approaches, integrating innovative technologies, and developing adaptive mechanisms for crisis response. Contemporary international practices and standards that can be implemented in the Ukrainian context to enhance the public sector's efficiency and flexibility are examined. The study substantiates the importance of developing institutional capacity, strengthening coordination among state bodies, and engaging civil society and international partners in shaping and implementing national security policies. Specific directions for modernization are proposed, including the digitalization of public services, implementation of risk management systems, strengthening analytical capabilities, and developing human resources. The article underscores that successful modernization of public administration is crucial for ensuring state resilience, its ability to withstand contemporary threats, and effectively protect national interests in an era of global transformations. Special attention is paid to the issue of increasing public trust in state institutions and ensuring transparency in administrative decision-making, which is a prerequisite for the successful implementation of strategic tasks in the field of national security.

Key words: public administration, national security, modernization, national interests, cybersecurity, digitalization, resilience, risk management, institutional capacity.

Вступ. У сучасних умовах багатовимірних викликів, що постають перед Україною, особливої актуальності набуває проблема забезпечення національної безпеки. Гібридна агресія, інформаційні війни, кіберзагрози, економічна нестабільність та екологічні ризики формують нову архітектуру загроз, які суттєво впливають на стабільність функціонування держави. У цих умовах зростає потреба в ефективному, гнучкому та адаптивному публічному управлінні, здатному своєчасно реагувати на динамічні зміни безпекового середовища.

Традиційні підходи до державного управління виявили свою обмеженість у протистоянні новітнім загрозам. Недостатня інституційна спроможність, фрагментарність управлінських процесів, низький рівень довіри громадян до органів влади та відсутність ефективної координації між ключовими суб'єктами публічної політики суттєво ускладнюють забезпечення національної безпеки. Це зумовлює потребу в системній модернізації публічного управління як ключового інструменту формування державної стійкості.

Проблематика модернізації публічного управління в контексті загроз національній безпеці активно досліджується як українськими, так і зарубіжними науковцями. Зокрема, В. Божко [1] обґрунтовує концептуальні основи нового публічного менеджменту, Н. Гавриш [2] акцентує увагу на адаптивності управлінських рішень в умовах гібридних загроз, а А. Гончарук [3] аналізує стійкість держави в контексті безпекових конфліктів. Значний внесок у дослідження довіри до публічного управління та належного урядування зробили Д. Журавльов [4] і Л. Чернець [11]. М. Кіндзерська [5] та В. Ковальчук [6] акцентують на важливості цифровізації та демократичного контролю в системі управління. Проте незважаючи на наявність наукових напрацювань, комплексне бачення модернізації публічного управління як системного інструменту нейтралізації загроз національній безпеці залишається недостатньо розробленим.

Метою статті є дослідження потенціалу модернізації публічного управління як ефективного інструменту забезпечення національної безпеки України, визначення стратегічних напрямів трансформації управлінських практик із врахуванням міжнародного досвіду, сучасних технологій та потреб стійкого розвитку держави.

Результати дослідження. Сучасні виклики вимагають переосмислення традиційних підходів до теоретичних засад публічного управління, його модернізації та інтеграції нових концепцій для забезпечення стійкості держави.

Публічне управління в сучасному розумінні є складною, динамічною системою, що охоплює процеси формування, реалізації та контролю державної політики на всіх рівнях. У контексті національної безпеки його сутність трансформується, набуваючи оборонного та превентивного характеру. Це не просто ефективне надання послуг чи раціональне використання ресурсів, а здатність держави адаптуватися до загроз, захищати життєво важливі інтереси суспільства та держави, забезпечувати її суверенітет і територіальну цілісність.

Сутність публічного управління в контексті національної безпеки характеризується такими особливостями:

- комплексний характер, адже публічне управління у сфері національної безпеки виходить за межі виключно військової чи правоохоронної діяльності. Воно охоплює економічний, соціальний, екологічний, інформаційний, культурний та інші виміри безпеки. Це вимагає інтегрованого підходу, координації дій різних державних органів, приватного сектору та громадянського суспільства;

- стратегічна орієнтованість: управління безпекою не може бути лише реактивним. Воно має ґрунтуватися на довгострокових стратегіях, прогнозуванні загроз та розробці превентивних заходів. Це передбачає формування чіткого бачення майбутнього та визначення пріоритетів у сфері безпеки;

- адаптивність та гнучкість: в умовах швидких змін та гібридних загроз публічне управління повинно бути здатним швидко адаптуватися до нових викликів. Це вимагає гнучких структур, оперативних механізмів прийняття рішень та можливості швидкого перерозподілу ресурсів;

- легітимність та довіра: ефективність публічного управління у сфері безпеки значною мірою залежить від довіри суспільства до державних інституцій. Прозорість, підзвітність, верховенство права та участь громадян у процесах прийняття рішень є критично важливими для забезпечення легітимності та підтримки державної політики безпеки [1,4].

Серед основних принципів публічного управління в контексті національної безпеки слід особливо виділити наступні: принцип національного інтересу, передбачає, що всі управлінські рішення та дії повинні бути спрямовані на захист та реалізацію національних інтересів України, визначених відповідними стратегічними документами; принцип верховенства права, адже діяльність усіх суб'єктів публічного управління повинна здійснюватися виключно в межах та у спосіб, визначений

Конституцією та законами України, з дотриманням прав і свобод людини; велика роль належить також принципу системності, який передбачає, що національна безпека розглядається як єдина система, де всі елементи взаємопов'язані. Управління має бути системним, враховуючи взаємодію всіх компонентів безпекового середовища. Принцип комплексності наголошує на тому, що вирішення проблем національної безпеки вимагає комплексного підходу, що об'єднує політичні, економічні, соціальні, військові, екологічні, інформаційні та інші інструменти; згідно принципу превентивності пріоритет надається запобіганню загрозам та їх нейтралізації на ранніх стадіях, а не лише реагуванню на вже існуючі кризи; в сучасних умовах надзвичайно важливим є принцип інноваційності, що вимагає застосування новітніх технологій, управлінських практик та підходів для підвищення ефективності системи безпеки; в умовах громадянського суспільства вкрай важливим є принцип відкритості та прозорості, що передбачає забезпечення доступу до інформації (з урахуванням обмежень, пов'язаних з державною таємницею), громадський контроль за діяльністю органів влади у сфері безпеки, залучення експертів та громадськості; нарешті принцип безперервності передбачає забезпечення постійного моніторингу загроз, аналізу ситуації та коригування управлінських рішень у сфері безпеки [7].

Отже, модернізація державного управління – це неперервний процес адаптації системи управління до мінливих умов внутрішнього та зовнішнього середовища, що спрямований на підвищення її ефективності, гнучкості та здатності вирішувати складні завдання. У контексті національної безпеки модернізація набуває особливого значення, оскільки вона є запорукою виживання та розвитку держави. Сучасна наука і практика виокремлюють кілька ключових концептуальних підходів:

1. Концепція «Нового публічного менеджменту» (New Public Management – NPM): Хоча NPM виникла раніше (1980-ті – 1990-ті роки), її елементи, такі як орієнтація на результати, ефективність, ощадливість, конкуренція та децентралізація, залишаються актуальними для модернізації управління безпекою. NPM пропагує перенесення принципів бізнес-управління в публічний сектор, що може сприяти більш раціональному використанню ресурсів та підвищенню операційної ефективності в оборонному та безпековому секторах. Однак, її слабкі сторони, такі як ризик надмірної комерціалізації та втрати фокусу на суспільних інтересах, потребують зваженого застосування.

2. Концепція «Належного урядування» (Good Governance). Цей підхід акцентує увагу на якості управління, підзвітності, прозорості, участі громадян, верховенстві права, ефективності та справедливості. Для національної безпеки це означає створення міцних інститутів, які здатні протистояти корупції, забезпечувати права людини та викликати довіру громадян. Належне урядування є фундаментом для стійкості держави та її здатності мобілізувати ресурси для відбиття загроз.

3. Концепція «Ціннісно-орієнтованого публічного управління» (Public Value Management): На відміну від NPM, що фокусується на ефективності та результатах, цей підхід ставить у центр уваги створення суспільної цінності. Це означає, що управлінські рішення мають не лише відповідати критеріям ефективності, а й приносити відчутну користь суспільству, покращувати якість життя громадян, сприяти їхній безпеці та добробуту. Для безпекового сектору це вимагає переосмислення показників ефективності від кількості проведених операцій до рівня безпеки та задоволеності громадян.

4. Концепція «Цифрового урядування» (Digital Governance / E-Governance). Сучасні технології відіграють ключову роль у модернізації, цифрове урядування передбачає використання інформаційно-комунікаційних технологій для покращення надання публічних послуг, оптимізації внутрішніх процесів управління, підвищення прозорості та залучення громадян. У сфері безпеки це стосується кіберзахисту, аналізу великих даних для прогнозування загроз, швидкої комунікації та координації дій.

5. Концепція «Стратегічного публічного управління» (Strategic Public Management): Цей підхід зосереджується на здатності держави до довгострокового планування, формування стратегій та їх ефективної реалізації. В умовах національної безпеки це передбачає розробку та виконання комплексних стратегій національної безпеки, оборони, економічного розвитку, що враховують потенційні загрози та можливості.

6. Концепція «Стійкого публічного управління» (Resilient Public Administration). Особливо актуальна в умовах криз та конфліктів. Цей підхід наголошує на здатності системи управління витримувати шоки, швидко відновлюватися та адаптуватися до нових умов. Це включає розробку планів безперервності діяльності, створення резервних систем та гнучких механізмів реагування на надзвичайні ситуації [8, 9].

Інституційне середовище є сукупністю формальних (закони, правила, процедури, державні органи) та неформальних (традиції, цінності,

норми поведінки) правил, що регулюють взаємодію між суб'єктами публічного управління та суспільством. Його якість та спроможність є визначальними для ефективності функціонування системи національної безпеки.

Інституції визначають рамки, в яких функціонують державні органи, силові структури, приватний сектор та громадянське суспільство у сфері безпеки. Чіткі, прозорі та стабільні правила зменшують невизначеність, сприяють передбачуваності дій та знижують корупційні ризики. Ефективні інституції створюють механізми для горизонтальної та вертикальної координації між різними відомствами (наприклад, РНБО, міжвідомчі комісії), що є критично важливим для протидії гібридним загрозам, які вимагають скоординованих дій у різних сферах. Сильне інституційне середовище передбачає наявність незалежних механізмів контролю (парламентський контроль, громадський контроль, судовий нагляд) за діяльністю органів безпеки та оборони. Це запобігає зловживанням владою, підвищує довіру суспільства та забезпечує легітимність дій держави [6].

Інституції повинні бути здатними до саморозвитку та адаптації до нових викликів. Це означає регулярний перегляд та оновлення законодавства, інституційних структур, впровадження нових технологій та управлінських практик. Інституційне середовище має стимулювати інновації у сфері безпеки, а не бути гальмом для них. Добре функціонуючі інституції є менш вразливими до зовнішнього втручання, дезінформації та маніпуляцій, що є важливою складовою гібридної війни. Вони забезпечують інституційну пам'ять та стабільність у кризових ситуаціях.

Інституційне середовище визначає ефективність мобілізації та розподілу ресурсів (фінансових, людських, матеріальних) для потреб національної безпеки. Це включає бюджетні процеси, процедури закупівель, управління майном.

Стійкість держави (*resilience of the state*) є ключовою концепцією в сучасній теорії безпеки та публічного управління. Вона визначається як здатність держави та суспільства протистояти зовнішнім та внутрішнім шокам, швидко відновлюватися після них та адаптуватися до нових умов, зберігаючи при цьому свої основні функції та цілі. Публічне управління є центральним елементом у формуванні та підтримці цієї стійкості [3].

Ефективне публічне управління розробляє, впроваджує та коригує національні стратегії стійкості, що охоплюють всі сфери життя суспільства – економічну, соціальну, екологічну, інформаційну, військову. Це включає розробку планів

безперервності діяльності для всіх критично важливих секторів.

Публічне управління відповідає за ідентифікацію, оцінку та управління ризиками, що загрожують національній безпеці. Це включає створення систем раннього попередження, розробку протоколів кризового реагування, формування та підготовку відповідних підрозділів (Державна служба з надзвичайних ситуацій, правоохоронні органи, медичні служби).

Стійкість держави значною мірою залежить від згуртованості суспільства. Публічне управління, через комунікаційні стратегії, освітні програми та залучення громадян до прийняття рішень, сприяє формуванню довіри, патріотизму та готовності суспільства до спільних дій у кризових ситуаціях. Сюди також належить боротьба з дезінформацією та спробами штучної поляризації суспільства.

Сильна економіка є основою стійкості держави. Публічне управління відповідає за формування сприятливого інвестиційного клімату, підтримку стратегічно важливих галузей, забезпечення енергетичної незалежності та диверсифікації ринків, що знижує вразливість до зовнішніх шоків.

Спроможні та гнучкі інституції публічного управління є основою стійкості. Вони повинні мати здатність швидко змінювати свою структуру та функції у відповідь на нові загрози, перерозподіляти ресурси та оперативно приймати рішення. В сучасних умовах це передбачає розвиток цифрових платформ для забезпечення безперервності функціонування урядових структур [5].

Публічне управління відіграє ключову роль у формуванні та підтримці міжнародних альянсів та партнерств, які є важливим елементом стійкості держави. Взаємодія з міжнародними організаціями (ООН, НАТО, ЄС) та країнами-партнерами сприяє обміну досвідом, доступу до ресурсів та колективній безпеці.

Таким чином, модернізація публічного управління є невід'ємною частиною стратегії підвищення стійкості України до сучасних загроз національній безпеці. Вона вимагає не лише технічних удосконалень, а й фундаментальних змін у філософії управління, орієнтації на цінності, гнучкості та постійну адаптацію до мінливого безпекового середовища.

З 2022 року кардинально змінилося безпекове середовище, виявилися нові вразливості та загрози, які вже існуючі. Це вимагає від системи публічного управління кардинальних трансформацій та адаптації.

Аналіз основних видів загроз засвідчує, що серед них можна виділити військові, гібридні,

кібернетичні, економічні, інформаційні, екологічні, соціальні.

Найбільш очевидною та деструктивною загрозою наразі є масштабні бойові дії, ракетні та артилерійські обстріли, повітряні атаки на критичну інфраструктуру та населені пункти. Така ситуація вимагає переходу до режиму функціонування в умовах воєнного стану, централізації управління, мобілізації ресурсів, оперативного прийняття рішень, забезпечення безперервності функціонування органів влади, ефективного цивільного захисту та управління евакуаційними процесами. Значно зростає роль військових адміністрацій та координаційних центрів [10].

Гібридні загрози являють собою комплекс скоординованих дій, що поєднують військові та невійськові, явні та приховані методи, спрямовані на дестабілізацію держави, підлив її суверенітету та територіальної цілісності без застосування традиційних воєнних дій у відкритій формі (або паралельно з ними). Гібридні загрози можуть проявлятися через використання нерегулярних військових формувань, інформаційно-психологічні операції, кібератаки, економічний тиск, провокування внутрішніх конфліктів, використання енергетичного шантажу. Вони розмивають межі між миром і війною, ускладнюють ідентифікацію агресора, вимагають міжвідомчої координації, створення центрів протидії дезінформації, розвитку стратегічних комунікацій та підвищення стійкості суспільства. Потребують інтегрованих підходів до оцінки ризиків та формування адаптивних відповідей [11].

В сучасних умовах особливої уваги потребують також кібернетичні загрози, що можуть полягати в атаках на критичну інформаційну інфраструктуру (енергетична, фінансова, транспортна, телекомунікаційна), державні реєстри, системи управління, сайти державних органів; бути спрямовані на викрадення даних, шпигунство, руйнування систем. Такі атаки підривають довіру до державних інститутів, порушують функціонування життєво важливих систем, можуть паралізувати управлінські процеси. Вимагають розробки національних стратегій кібербезпеки, створення кібервійськ, навчання фахівців, впровадження сучасних систем захисту інформації, забезпечення кібергігієни державних службовців.

Економічні загрози, такі як блокада морських шляхів, руйнування виробничих потужностей, втрата ринків збуту, енергетичний шантаж, інфляція, падіння ВВП, відтік інвестицій, зростання зовнішнього боргу, криза на ринку праці, вимагають розробки та реалізації програм економічного

відновлення, підтримки бізнесу, забезпечення макроекономічної стабільності, пошуку нових джерел фінансування, ефективного управління міжнародною допомогою. Потребують гнучкого регулювання та антикризових заходів.

Інформаційні загрози, що знаходять прояв у вигляді дезінформації, пропаганди, фейкових новин, психологічних операцій, спрямовані на підлив суспільної довіри, створення паніки, розкол суспільства, маніпуляцію громадською думкою. Вони ускладнюють формування єдиного інформаційного простору, підривають авторитет влади, дезорієнтують громадян. Вимагають розвитку стратегічних комунікацій, медіаграмотності населення, спроможності швидко спростовувати фейки, захисту національного інформаційного простору.

Такі негативні чинники, як забруднення територій внаслідок бойових дій (міни, вибухи, руйнування промислових об'єктів), руйнування екосистем, ядерна загроза, техногенні катастрофи належать до екологічних загроз та вимагають розробки та реалізації програм ліквідації наслідків екологічних катастроф, розмінування, відновлення природного середовища, моніторингу радіаційної та хімічної безпеки. Потребують посилення екологічного контролю та міжнародної співпраці у цій сфері.

Масова міграція та внутрішньо переміщені особи, гуманітарні кризи, зростання безробіття, зниження рівня життя, психологічні травми населення, загострення соціальної напруги, погіршення доступу до медичних послуг становлять прояви соціальних загроз та вимагають ефективної соціальної політики, підтримки вразливих груп населення, забезпечення житлом, медичною та психологічною допомогою, адаптації ветеранів, реінтеграції ВПО.

Вплив загроз на публічне управління є багатовимірним: прямі атаки можуть вивести з ладу системи зв'язку, інфраструктуру, що паралізує роботу органів влади; війна та кризові ситуації вимагають колосальних фінансових, людських та матеріальних ресурсів, що призводить до їхнього дефіциту в інших сферах; непередбачуваність ситуації, швидкі зміни, втрата зв'язку можуть знижувати якість управлінських рішень та ускладнювати їх реалізацію; працівники органів влади перебувають під постійним стресом, що впливає на їхню працездатність та психологічний стан; загрози вимагають відмови від бюрократичних процедур, переходу до більш гнучких та оперативних моделей управління; в умовах надзвичайного стану та швидкого розподілу ресурсів зростають ризики

корупції, що підриває довіру до влади та її ефективність; довгострокове планування стає майже неможливим, що змушує переходити до короткострокових та адаптивних планів.

Традиційні, ієрархічні та бюрократичні моделі публічного управління виявилися недостатньо ефективними в умовах сучасних загроз:

- довгі ланцюги прийняття рішень, надмірна регуляція та повільність у впровадженні змін не дозволяють оперативно реагувати на динамічні загрози;

- жорстка структура та функціональні обмеження перешкоджають швидкому перерозподілу ресурсів та зміні пріоритетів;

- залежність від єдиних центрів прийняття рішень робить систему вразливою до деструктивних впливів;

- слабка міжвідомча координація, де кожен орган працює автономно, унеможливує комплексну відповідь на гібридні загрози;

- фокус на процесах, а не на реальних результатах, призводить до неефективного використання ресурсів у кризових умовах;

- переважно реактивний підхід до проблем замість їх прогнозування та запобігання [2].

Зважаючи на визначені загрози національній безпеці, модернізація публічного управління в Україні має бути системною, комплексною та спрямованою на підвищення його адаптивності, стійкості та ефективності у протидії сучасним загрозам. Серед основних напрямів нейтралізації загроз національним інтересам України в сучасних умовах можна запропонувати:

1. Цифровізація та використання інноваційних технологій, зокрема впровадження електронного урядування та електронних послуг – прискорення розвитку платформи «Дія», розширення переліку послуг, інтеграція реєстрів. Це забезпечує безперервність надання послуг навіть в умовах руйнувань, зменшує корупцію та підвищує прозорість. Слід також більш активно впроваджувати технології Big Data, штучного інтелекту для аналізу та прогнозування загроз, застосувати аналітичні системи для моніторингу соціальних мереж, кіберпростору, економічних показників для раннього виявлення загроз та прийняття обґрунтованих рішень. Наприклад, використання ШІ для аналізу великих обсягів розвідувальної інформації. Вимагає щільної уваги подальша розбудова систем кіберзахисту критичної інфраструктури: посилення захисту державних інформаційних ресурсів, енергетичних, транспортних та фінансових систем. Створення національного центру кібербезпеки, регулярні аудити та тестування сис-

тем, навчання персоналу. Застосування технологій блокчейн для забезпечення незмінності даних. Нарешті впровадження геоінформаційних систем для оперативного моніторингу ситуації на фронті, оцінки руйнувань, планування відновлення, управління ресурсами в надзвичайних ситуаціях.

2. Посилення інституційної спроможності та координації, що передбачає оптимізацію структури та функцій державних органів – перегляд повноважень та відповідальності, усунення дублювання функцій, створення гнучких міжвідомчих робочих груп та штабів для швидкого реагування. Децентралізація повноважень з одночасним посиленням контролю. Нагальним питанням залишається також формування ефективних механізмів міжвідомчої координації та взаємодії, тобто створення єдиних центрів прийняття рішень у кризових ситуаціях, чіткі протоколи взаємодії між різними органами державної влади. Регулярні спільні навчання та тренінги. Актуальним завданням у сфері нейтралізації загроз національній безпеці є подальший розвиток державно-приватного партнерства у сфері безпеки, залучення приватних компаній (ІТ-сектор, оборонна промисловість, логістика) до розробки та впровадження інноваційних рішень для безпеки та оборони, формування довіри та взаємовигідних умов співпраці.

3. Управління ризиками та кризове реагування на базі впровадження систем ризик-менеджменту в публічному управлінні. Це вимагає розробки методологій ідентифікації, оцінки, моніторингу та управління ризиками на всіх рівнях державного управління. Включення ризиків національної безпеки в бюджетні процеси та стратегічне планування. Необхідним є складання та відпрацювання планів кризового реагування, детальних сценаріїв дій у разі виникнення різних типів загроз (військових, кібернетичних, техногенних), чітке визначення ролей та відповідальності, регулярні навчання для перевірки ефективності планів. З метою формування резервів та ресурсів для протидії загрозам обов'язковим є створення державних матеріальних резервів, резервів палива, медикаментів, обладнання, розробка механізмів швидкого залучення фінансових та людських ресурсів у кризових умовах.

4. Розвиток кадрового потенціалу та професіоналізація – підготовка та перепідготовка державних службовців з акцентом на безпекові аспекти має бути невід'ємною складовою процесу нейтралізації загроз національним інтересам України та передбачати включення в навчальні програми елементів національної безпеки, кризового управ-

ління, кібербезпеки, стратегічних комунікацій, розвиток аналітичних навичок та критичного мислення. Формування культури безпеки та відповідальності має сприяти підвищенню свідомості державних службовців щодо важливості безпечових питань, формуванню етичних стандартів та відповідальності за прийняті рішення, допомагати боротьбі з корупцією. Важливим у цьому аспекті є також запровадження системи мотивації та відбору професіоналів, залучення кваліфікованих кадрів, створення конкурентних умов праці та кар'єрного зростання.

5. Залучення громадянського суспільства та налагодження міжнародної співпраці – не можна забувати про роль громадських організацій у формуванні та контролі політики безпеки, залучення експертів та активістів до розробки законопроектів, моніторингу реалізації державної політики, громадського контролю за сектором безпеки та оборони має надзвичайно велике значення. Також і посилення співпраці з міжнародними партнерами та організаціями сприятиме обміну досвідом, розширить можливості для участі у спільних навчаннях, отриманні експертної та фінансової допомоги, імплементації стандартів ЄС у сфері публічного управління та безпеки.

Висновки. Впровадження запропонованих напрямів модернізації публічного управління як інструменту нейтралізації загроз національній безпеці матиме низку позитивних результатів серед яких можна виокремити: підвищення ефективності та оперативності, система управління стане більш гнучкою, здатною швидко реагувати на виклики та ефективно використовувати ресурси; зміцнення стійкості держави, здатності протистояти зовнішнім та внутрішнім шокам, швидко відновлювати функції після кризових ситуацій; підвищення довіри суспільства, адже прозорість, підзвітність та орієнтація на потреби громадян сприятимуть зростанню довіри до державних інституцій; зниження корупційних ризиків, особливо з врахуванням цифровізації та прозорості процесів, що зменшує можливості для корупції; інтеграція в європейський простір, імплементація міжнародних стандартів у сфері публічного управління наблизить Україну до ЄС; покращення міжнародного іміджу – демонстрація здатності до ефективного управління та розвитку навіть в умовах війни підвищить інвестиційну привабливість та політичну підтримку; розвиток людського капіталу сприятиме підвищенню

кваліфікації та професіоналізму державних службовців.

Незважаючи на очевидні переваги, процес модернізації публічного управління як інструменту нейтралізації загроз національній безпеці може стикнутися з низкою значних перешкод таких як: опір змінам через інерцію системи, небажання частини державних службовців змінювати усталені практики, страх втратити повноваження чи «тіньові» доходи; обмежені бюджетні ресурси в умовах війни, висока вартість впровадження нових технологій та навчання; відтік фахівців через війну, низька привабливість державної служби, дефіцит знань та навичок у сфері сучасного управління; корупція; недосконалість законодавчої бази; зовнішні деструктивні впливи.

З метою подолання вказаних перешкод необхідно забезпечити чітке розуміння у суспільстві загалом та серед державних службовців зокрема переваг реформ, навчання та перекваліфікації персоналу, зміни системи мотивації (заохочення до інновацій), жорсткого контролю за виконанням реформ та застосування санкцій за саботаж; оптимізація витрат, пріоритизація напрямків модернізації, залучення міжнародної технічної та фінансової допомоги, використання грантових програм, пошук можливостей для державно-приватного партнерства дозволить залучити додаткові фінансові ресурси у процес модернізації публічного управління як інструменту нейтралізації загроз національній безпеці; розробка ефективних програм підготовки та перепідготовки, підвищення престижу державної служби, створення умов для повернення та залучення кваліфікованих спеціалістів (особливо з IT-сфери), програми менторства сприятиме вирішенню кадрової проблеми у сфері публічного управління; з метою подолання корупції слід і далі сприяти формуванню у суспільстві нульової толерантності до цього явища, посилювати антикорупційне законодавство та забезпечувати його неухильне виконання, широко впроваджувати цифровізацію процесів для мінімізації людського фактору, застосовувати незалежний аудит, забезпечувати прозорість у прийнятті рішень та витрачання бюджетних коштів; систематичний перегляд та оновлення нормативно-правової бази, швидке прийняття законів, що сприяють реформам, їх гармонізація з європейськими стандартами сприятимуть тому, що чинне законодавство відповідатиме сучасним викликам та потребам модернізації.

REFERENCES:

1. Bozhko, V. M. (2021). Novyi publichnyi menedzhment: Sutnist ta mozhlyvosti zastosuvannya v Ukraini [New public management: Essence and possibilities of application in Ukraine]. *Publichne upravlinnia: teoriia ta praktyka*, (1), 45–53.

2. Havrysh, N. V. (2022). Adaptivnist publichnoho upravlinnia v umovakh hibrydnukh zahroz: Ukrainnyi kontekst [Adaptability of public administration under hybrid threats: Ukrainian context]. Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Serii: Derzhavne upravlinnia, (2), 78–85.
3. Honcharuk, A. V. (2023). Kontsepsiia stiikosti derzhavy u konteksti hibrydnukh konfliktiv [The concept of state resilience in the context of hybrid conflicts]. Stratehichni priorytety, (3), 112–120.
4. Zhuravliov, D. O. (2024). Dovira do publichnoho upravlinnia yak faktor natsionalnoi bezpeky [Trust in public administration as a factor of national security]. Naukovi zapysky NaUKMA. Politolohiia, (5), 150–158.
5. Kindzerska, M. I. (2022). Tsyfrove uriaduvannia yak instrument modernizatsii publichnoho upravlinnia v Ukraini [Digital governance as a tool for modernization of public administration in Ukraine]. Derzhavne upravlinnia ta mistseve samovriaduvannia, (4), 67–75.
6. Kovalchuk, V. I. (2023). Rol instytutsii u zabezpechenni demokratychnoho kontroliu nad sektorom bezpeky i oborony [The role of institutions in ensuring democratic control over the security and defense sector]. Publichne upravlinnia ta administruvannia, (1), 89–97.
7. Kulchytskyi, O. V. (2024). Ekonomichna bezpeka yak osnova natsionalnoi stiikosti: upravlinskyi aspekt [Economic security as the basis of national resilience: The managerial aspect]. Ekonomika ta derzhava, (2), 34–42.
8. Pashko, O. M. (2022). Tsinnisno-orientovane publichne upravlinnia: vid teorii do praktyky [Value-oriented public administration: From theory to practice]. Visnyk Akademii upravlinnia, (1), 56–64.
9. Prokopenko, I. V. (2023). Stratehichne planuvannia u sferi natsionalnoi bezpeky: vyklyky ta perspektyvy [Strategic planning in the field of national security: Challenges and prospects]. Publichne uriaduvannia, (3), 201–209.
10. Stepanenko, R. O. (2024). Zabezpechennia bezperervnosti derzhavnoho upravlinnia v umovakh viiny: teoretychni aspekty [Ensuring the continuity of public administration in wartime: Theoretical aspects]. Visnyk derzhavnoi sluzhby Ukrainy, (1), 115–123.
11. Chernets, L. V. (2023). Nalezhne uriaduvannia yak osnova formuvannia stiikoi systemy natsionalnoi bezpeky Ukrainy [Good governance as a foundation for building a resilient national security system in Ukraine]. Derzhava i pravo. Yurydychni i politychni nauky, (97), 210–218.