УДК 355.3:327.56

https://doi.org/10.52058/3041-1793-2025-10(15)-960-971

Запорожець Тетяна Володимирівна доктор наук з державного управління, доцент, професор кафедри глобальної та національної безпеки, Навчально-науковий інститут публічного управління та державної служби Київського національного університету імені Тараса Шевченка, Київ, https://orcid.org/0000-0003-1914-9481

СТРАТЕГІЧНІ ПІДХОДИ ДО ЗМІЦНЕННЯ НАЦІОНАЛЬНОЇ СТІЙКОСТІ В УМОВАХ ЗОВНІШНІХ ЗАГРОЗ

Анотація. У статті обґрунтовано стратегічні підходи до зміцнення національної стійкості в умовах зовнішніх загроз та окреслено перспективні напрями її розвитку. Доведено, що зміцнення національної стійкості потребує комплексного підходу, що поєднує політичні, економічні, соціальні, інформаційні та безпекові складники, інтеграції ресурсів державних органів, місцевих органів влади, приватного сектору та громадянського суспільства. Визначено ключові принципи її забезпечення: комплексність, інтегрованість та адаптивність. Принцип комплексності забезпечує системний підхід до управління ризиками, взаємодію державних інститутів, бізнесу та громадянського суспільства, а також синхронізацію дій для підтримання політичної та економічної стабільності. Принцип інтегрованості акцентує на багаторівневій координації органів влади різних рівнів, приватного сектору та громадських структур, що підвищує ефективність реагування на гібридні, кібернетичні та інформаційні загрози. Принцип адаптивності забезпечує здатність системи швидко реагувати на трансформацію зовнішніх викликів, прогнозувати потенційні ризики та відновлювати критичні функції держави у кризових ситуаціях. Доведено, що кіберстійкість виступає важливим інтегративним компонентом національної безпеки, що передбачає не лише протидію кібератакам, а й швидке відновлення критичних інформаційних і технологічних систем із застосуванням превентивних та активних оборонних заходів. Визначено роль багаторівневої координації та сценарного планування у підвищенні гнучкості та адаптивності державних систем, що дозволяє проактивно прогнозувати потенційні загрози та забезпечувати ефективне управління кризами. Визначено роль соціальної складової у підвищенні довіри громадян до державних інститутів, розвитку громадянського суспільства та соціальної згуртованості як фундаментальних умов для самоорганізації та партнерства у сфері безпеки. Обґрунтовано, що стратегічні підходи до зміцнення національної стійкості є методологічною основою для побудови динамічної, інтегрованої та адаптивної системи національної безпеки, здатної

протистояти зовнішнім викликам, підтримувати політичну і економічну стабільність та забезпечувати сталий розвиток держави у сучасному мінливому безпековому середовищі.

Ключові слова: національна стійкість, національна безпека, громадянське суспільство, адаптивність, інтегрованість, комплексність, гібридна війна, кібербезпека, управління кризами

Zaporozhets Tetiana Doctor of Science of Public Administration, Associate Professor, Professor of the Department of Global and National Security of Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv, Kyiv, https://orcid.org/0000-0003-1914-9481

STRATEGIC APPROACHES TO STRENGTHENING NATIONAL RESILIENCE IN THE CONTEXT OF EXTERNAL THREATS

Abstract. The article substantiates strategic approaches to enhancing national resilience in the context of external threats and outlines prospective directions for the development of the state security system. It is demonstrated that strengthening national resilience requires a comprehensive approach integrating political, economic, social, informational, and security components, as well as the coordinated use of resources from state authorities, local government bodies, the private sector, and civil society. The key principles ensuring resilience are identified: comprehensiveness, integration, and adaptability. The principle of comprehensiveness provides a systemic approach to risk management, facilitates the interaction of state institutions, business, and civil society, and ensures the synchronization of actions to maintain political and economic stability. The principle of integration emphasizes multi-level coordination among national, regional, and local authorities, the private sector, and public organizations, enhancing the effectiveness of responses to hybrid, cyber, and informational threats. The principle of adaptability ensures the system's capacity to promptly respond to evolving external challenges, anticipate potential risks, and restore critical state functions during crises. It is demonstrated that cyber resilience constitutes a crucial integrative component of national security, encompassing not only counteraction to cyberattacks but also rapid recovery of critical information and technological systems through preventive and active defensive measures. The role of multi-level coordination and scenario-based planning is highlighted in increasing the flexibility and adaptability of state systems, enabling proactive risk forecasting and effective crisis management. The social dimension is emphasized as a fundamental factor in strengthening citizens' trust in state institutions, developing civil society, and promoting social cohesion, which are essential for self-organization and partnership in the security sphere. It is substantiated that strategic approaches to enhancing national resilience serve as a methodological foundation for constructing a dynamic,

integrated, and adaptive national security system capable of countering external threats, maintaining political and economic stability, and ensuring sustainable state development in today's volatile security environment.

Keywords: national resilience, national security, civil society, adaptability, integration, comprehensiveness, hybrid warfare, cybersecurity, crisis management.

Постановка проблеми. Забезпечення національної стійкості є одним із головних напрямів сучасної державної політики безпеки, оскільки від рівня її ефективності залежить здатність держави протидіяти зовнішнім загрозам, зберігати цілісність політичної системи та забезпечувати функціонування критичних соціально-економічних процесів. Особливу актуальність ця проблема набуває в умовах сучасної геополітичної нестабільності, коли держави постають перед комплексними, динамічними та непередбачуваними викликами, що поєднують елементи гібридної війни, конвенційних загроз, інформаційних операцій і кібернетичних атак. Таким чином, актуальність дослідження визначається необхідністю напрацювання комплексних стратегічних підходів до забезпечення національній стійкості, що базуються на сучасних наукових концепціях управління ризиками, системного аналізу та формування інтегрованих моделей протидії сучасним загрозам.

Аналіз останніх досліджень і публікацій свідчить, що проблематика національної стійкості розглядається у кількох змістових площинах. У працях О. Резнікової [1], Я. Лазебника [8] та колективній монографії під ред. Г. Ситника [9] акцентовано увагу на концептуалізації цього феномена як багатовимірної системи, що інтегрує політичні, економічні, соціальні та безпекові складники. Соціально-психологічні та інституційні аспекти висвітлює К. Коростеліна [2], яка доводить значення колективної ідентичності й суспільної згуртованості, М. Каліман [5] та М. Назаров [6] аналізують організаційні й правові механізми забезпечення стійкості та перехід від концепту до практичних моделей. Окрему увагу приділено функціональним вимірам: В. Хаустова та Н. Трушкіна [12] систематизують ризики та загрози національній безпеці. Зарубіжні дослідники фокусуються на питаннях кіберстійкості (М. Ахмед та ін. [10]) та стратегіях кризового менеджменту (К. Мізрак [11]). Вагому роль у формуванні стратегічних орієнтирів відіграють нормативно-правові та політичні документи. Указ Президента України № 479/2021 [7] започаткував створення національної системи стійкості, визначивши її як комплексну інституційну рамку. У документах НАТО щодо цивільної готовності [4] та рішеннях Робочої групи ЄС з протидії гібридним загрозам [3] закріплено підходи до багаторівневої координації у сфері безпеки. Таким чином, сучасний науковий і нормативно-правовий дискурс окреслює національну стійкість як багаторівневу категорію, що поєднує концептуальні засади, інституційні механізми та практичні інструменти забезпечення безпеки. Однак, попри наявність широкого теоретичного підґрунтя та

нормативних орієнтирів, залишається низка невирішених аспектів, зокрема відсутність узгодженого бачення стратегічних підходів до побудови системи національної стійкості та окреслення перспективних напрямів її розвитку.

Мета статті – обґрунтувати стратегічні підходи та окреслити перспективні напрями зміцнення національної стійкості в умовах зовнішніх загроз.

Виклад основного матеріалу. У сучасних умовах ескалації зовнішніх загроз питання вироблення стратегічних підходів до забезпечення національної стійкості набуває особливої ваги. Йдеться не лише про реагування на гібридні чи конвенційні виклики, а й про створення довготривалої основи, здатної підтримувати політичну, економічну та соціальну стабільність у кризових ситуаціях. Вітчизняні та зарубіжні дослідження свідчать про те, що стратегічні рамки стійкості формуються на перетині питань безпеки, управління ризиками та суспільної довіри, а їхня ефективність визначається здатністю до синхронізації державних і громадських ресурсів. Практика НАТО та ЄС, закріплена у відповідних політичних документах, орієнтує на побудову багаторівневих систем, де стійкість розглядається як результат взаємодії державних структур, бізнесу, громадянського суспільства та міжнародних партнерів. Саме тому стратегічний вимір стійкості в українському контексті має розглядатися як цілісна система, спрямована не лише на протидію зовнішнім загрозам, але й на створення умов для відновлення, розвитку та зміцнення державних інститутів у довгостроковій перспективі.

У монографії «Національна стійкість у мінливих умовах безпеки» О.Резнікова зазначає, що досягнення національної стійкості можливе шляхом забезпечення відповідного рівня готовності держави та суспільства до реагування на широкий спектр загроз і небезпек, своєчасного виявлення вразливостей, які послаблюють безпекові можливості, проведення адаптивного управління, ефективного кризового управління та зв’язку на всіх рівнях, створення необхідних резервів і альтернативних стратегій [1]. Опираючись на емпіричні дослідження, К.Коростеліна показує, що національна стійкість формується через мобілізацію соціальних мереж, культурних ресурсів та колективної ідентичності, що дозволяє країні витримувати й відновлюватися в умовах постійних викликів [2].

Звіти НАТО та ЄС комплексно висвітлюють питання посилення національної стійкості у сучасних умовах гібридних загроз. Ці документи ґрунтуються на принципі багаторівневої взаємодії між урядовими структурами, приватним сектором та громадянським суспільством, що забезпечує комплексний та координаційний підхід до зміцнення захисних спроможностей держав. Документ Європейського Союзу, розроблений Горизонтальною робочою групою з питань підвищення стійкості та протидії гібридним загрозам у 2024 році [3], підкреслює, що резильєнтність держави - це не лише спроможність протистояти атакам, але і здатність адаптуватися та відновлюватися у

динамічному середовищі загроз. В документі наголошується на важливості цифрової трансформації як одного з ключових чинників формування стійкості. Цей фактор включає посилення кіберзахисту критичної інфраструктури, розвиток медіаграмотності населення для протидії дезінформації, а також створення умов для взаємодії між державними відомствами і різними секторами суспільства у інформаційній сфері. Акцент робиться на ролі превентивних заходів, зокрема підвищенні ступеня готовності до реагування на ведення гібридної війни, які можуть поєднувати кібернетичні атаки, дезінформаційні кампанії та порушення функціонування критичних систем.

У звіті НАТО «Стійкість, цивільна готовність та стаття 3» (2024) розглядається резильєнтність у контексті Пункту 3 Північноатлантичного договору, який покладає на держави-члени Альянсу обов'язок забезпечувати свою здатність протистояти зовнішнім загрозам. Документ виокремлює сім ключових складових цивільної підготовки, серед яких: безперервність функціонування уряду, стабільність життєво важливих сервісів для населення, міцність комунікаційних і транспортних систем, забезпечення ресурсів харчування та питної води, а також здатність ефективно реагувати на масові надзвичайні ситуації та катастрофи [4]. НАТО наголошує, що хоча основна відповідальність за резильєнтність лежить на самих державах-членах, Альянс надає консультативну підтримку, координує навчання та обмін досвідом, створюючи спеціалізовані команди для реагування на гібридні загрози.

Вказані документи наголошують на необхідності тісної координації між різними рівнями управління між національним урядом, регіональними і місцевими органами, а також інтеграції можливостей приватного сектору і активізації громадянського суспільства. Ця багаторівнева взаємодія формує багатошарову систему безпеки, яка підвищує загальну стійкість до комплексних викликів. Значною мірою її успішність залежить від ефективного використання цифрових технологій для збору та аналізу інформації, поширення правдивих даних і протидії ворожим впливам через інформаційний простір. Крім того, як зазначається у звітних документах, ЄС та НАТО розвивають механізми спільної роботи, такі як спільні робочі групи та стратегічні ініціативи для захисту критичної інфраструктури, обміну інформацією та координації кризових заходів. Особливу увагу приділяють підвищенню кібербезпеки, посиленню енергетичної та транспортної безпеки, а також подоланню залежностей у ланцюгах постачання, що дають потенційну вразливість перед гібридними операціями.

Отже, наукові розробки та документи відображають сучасний багатогранний та інтегрований підхід до підвищення національної стійкості, де цифрова трансформація, міжсекторальна координація і комплексне планування є основними інструментами в протидії сучасним гібридним загрозам. Вони створюють науково і практично обґрунтовану основу для формування стратегій державної та міжнародної безпеки в умовах мінливого глобального середовища.

Стратегічні підходи до формування системи національної стійкості базуються на принципах, які забезпечують її ефективність у складних і мінливих умовах сучасного безпекового середовища. Найважливішими серед них варто виокремити принципи комплексності, інтегрованості та адаптивності, кожен із яких відображає специфіку викликів, з якими стикається держава, та особливості реагування на них.

Принцип *комплексності* у формуванні національної стійкості означає розгляд цього явища як багатовимірного процесу, що включає політичний, економічний, соціальний, інформаційний і безпековий сектори. Це підкреслюють дослідження М. Калімана, який наголошує на необхідності ефективної взаємодії суспільства і держави у різних сферах для подолання криз із мінімальними втратами та швидким відновленням [5]. Комплексність розглядається також як інституціоналізація партнерських стосунків між державними інститутами, громадянським суспільством і бізнесом у сфері безпеки, що стимулює формування взаємодіючих механізмів із залученням широкого кола учасників і ресурсів. М.Назаров наголошує на більш широкому розумінні національної стійкості як комплексної категорії, що не лише включає здатність держави протистояти зовнішнім і внутрішнім загрозам, а й передбачає активну участь громадянського суспільства у забезпеченні національної безпеки. Автор також підкреслює важливість соціальної згуртованості, демократії і довіри як фундаментальних факторів посилення стійкості національної системи [6]. Таким чином, принцип комплексності є ключовим для стратегічного управління національною стійкістю, оскільки він забезпечує системний підхід, який поєднує різні компоненти безпекового середовища в єдину систему.

Принцип *інтегрованості* пов’язаний із необхідністю об’єднання зусиль різних суб’єктів: державних органів, органів місцевого самоврядування, приватного сектору і громадянського суспільства у рамках єдиної системи управління національною стійкістю. У згадуваній монографії О.Резнікової [1] систематизовано основні механізми забезпечення стійкості та наголошено на важливості реалізації багаторівневого організаційного механізму, здатного координувати дії на всіх рівнях, включаючи міжсекторальну взаємодію та адаптивне управління загрозами. Інтегрованість дозволяє не лише об’єднати ресурси, але й забезпечити ефективну комунікацію та оперативність у відповідь на зовнішні виклики

Принцип *адаптивності* забезпечує здатність сучасної системи національної стійкості гнучко реагувати на зміни у безпековому середовищі. У Концепції забезпечення національної системи стійкості, затвердженій Указом Президента України від 27 вересня 2021 року № 479/2021, національна стійкість визначається як здатність держави та суспільства своєчасно ідентифікувати загрози й вразливості, оцінювати ризики для національної безпеки, ефективно реагувати на них, а також швидко і масштабно

відновлюватися після виникнення загроз або надзвичайних ситуацій різного характеру, включно з гібридними загрозами [7]. Концепція визначає, що адаптивність до змін безпекового середовища забезпечується розвиненими системами ідентифікації загроз, управління ризиками, виявлення вразливостей, а також здатністю систем швидко оновлюватися і відновлюватися після кризових ситуацій. Важливе значення надається функціонуванню таких елементів національної системи стійкості, як дієвість державних інститутів і інституційна стійкість, захищеність критичних об'єктів інфраструктури, ефективність систем цивільного захисту і охорони здоров'я, а також фінансово-економічна стабільність.

Вчені підкреслюють, що адаптивність як складова національної стійкості стає особливо важливою в умовах гібридних та мультидоменних загроз, які характеризуються постійною трансформацією і ускладненням свого характеру. Зовнішні виклики характеризуються динамічністю, тому системи безпеки повинні бути гнучкими, що дозволяє своєчасно реагувати на нові реалії, мінімізувати негативні наслідки й ефективно протидіяти складним загрозам [8].

Наукові дослідження доводять, що вказані принципи не існують ізольовано, а взаємодіють і взаємно посилюють одна одну. Комплексний та інтегрований підхід забезпечує стійкість, яка ґрунтується на довірі громадян до інститутів влади, спроможності до самоорганізації та готовності до партнерства у сфері безпеки. Ефективність адаптивного управління обумовлюється потребою систематичного застосування механізмів зворотного зв'язку та навчання, що забезпечують постійне коригування політик і стратегій безпеки [9]. Важливо і те, що ці принципи ґрунтуються також на визначальній ролі суспільної довіри і цивільної підготовленості як основоположних елементів системи національної стійкості. Здатність суспільства до самоорганізації та активної участі у безпекових процесах є необхідною умовою для реалізації комплексних та інтегрованих стратегій управління викликами.

Таким чином, побудова системи національної стійкості вимагає системного поєднання принципів комплексності, інтегрованості та адаптивності. Ці принципи утворюють методологічне підґрунтя, яке сприяє підвищенню ефективності реагування держави та суспільства на зовнішні виклики та створенню стійкої, готової до трансформаційної саморегуляції системи безпеки.

У контексті системного підходу до побудови національної стійкості, що базується на вказаних принципах, особливого значення набуває розробка стратегічних рамок протидії гібридним і конвенційним загрозам. Такий підхід передбачає не лише розуміння багатогранності викликів безпеці, а й створення довгострокових планів, які дозволяють ефективно управляти ризиками та забезпечують гнучкість і стійкість державних систем у часі. Зокрема, стратегічне управління у сфері безпеки розглядається комплексний підхід до

розбудови кіберстійкості як ключового елементу національної безпеки в умовах сучасних зовнішніх загроз, зокрема гібридних атак.

Зарубіжні вчені підкреслюють, що кібербезпека та кібероборона, хоча і є взаємопов'язаними, часто розглядаються окремо в теоретичних і практичних аспектах, що створює певний розрив у формуванні ефективної системи національної стійкості. З їхньої точки зору, кіберстійкість (cyber resilience) охоплює здатність не лише запобігати атакам, але й швидко відновлювати критичні системи після інцидентів, що вимагає інтеграції превентивних заходів із активними оборонними діями. Дослідники відзначають, що в умовах сучасної гібридної війни та мультидоменних загроз, до яких належать інформаційні операції та кібератаки, стратегічне управління має забезпечувати синергію між оперативною кібербезпекою та довгостроковим кіберзахистом. При цьому довгостроковий кіберзахист передбачає підготовку кваліфікованих кадрів, розробку та вдосконалення нормативно-правової бази, створення інтегрованих центрів реагування й впровадження ефективних систем моніторингу. Автори акцентують на тому, що кіберстійкість стає платформою для створення комплексного «щита» національної безпеки, який враховує всі можливі вектори агресії, від зламу комп'ютерних мереж до впливу на суспільну свідомість через інформаційні технології. Особливу увагу приділено зміцненню захисту критичної інфраструктури (енергетичних, транспортних, фінансових систем), що уразливі перед кібернападами і є критичними для функціонування держави. Науковці пропонують поєднати технічні рішення з управлінськими практиками, на основі яких формується гнучка, швидко адаптована система відновлення після атак. Важливою є також теза про необхідність тісної співпраці між різними суб'єктами: державними органами, приватним сектором та науковою спільнотою для обміну інформацією про загрози та кращими практиками реагування. Це відповідає концепції інтегрованої стійкості в національній безпеці, де кібербезпека і кібероборона функціонують у взаємодії з іншими компонентами системи стійкості, такими як інформаційна безпека, економічна стабільність і суспільна згуртованість [10]. Вказане суттєво розширює розуміння ролі кіберкомпоненту у зміцненні національної стійкості та формуванні сучасних моделей захисту у довгостроковій перспективі.

При цьому важливе значення мають моделі управління, орієнтовані на адаптивність і проактивне планування. Вчені підкреслюють, що стратегічне управління у сфері безпеки в умовах зростаючих гібридних і конвенційних загроз має базуватися на формуванні гнучких сценаріїв розвитку подій та систем раннього попередження. Завдяки сценарному плануванню держава здатна проактивно оцінювати потенційні ризики і готувати відповідні варіанти реагування задовго до фактичного виникнення надзвичайних ситуацій. Такий підхід дозволяє управляти поточними кризами, розвивати внутрішній потенціал для якіснішого прогнозування й мінімізації негативних наслідків майбутніх загроз [11].

У цьому контексті важливо звернути увагу на теорії ризиків і загроз національній безпеці, які представлені у роботі В.Хаустової та Н.Трушкіної (2024). Дослідниці аналізують сутність і класифікацію ризиків, відзначаючи, що сучасна безпекова ситуація характеризується не лише традиційними воєнними загрозами, але й економічними, інформаційними, соціальними та технологічними викликами, серед яких особливої уваги заслуговують гібридні загрози. Авторки підкреслюють, що без комплексного підходу до розуміння різноманіття і взаємозв'язку цих загроз ефективне стратегічне управління неможливе. Класифікація загроз, запропонована авторками, охоплює широкий спектр: від деформації економіки й втрати науково-технічного потенціалу до інформаційної безпеки та кібернетичних атак [12]. Такий підхід узгоджується зі сценарним плануванням, допомагаючи виявити ключові вразливості, визначити найбільш імовірні сценарії загроз та своєчасно розробити адекватні відповіді. Таким чином, інтеграція аналізу ризиків і класифікації загроз у процес сценарного планування та розробки систем раннього попередження підсилює адаптивність стратегічного управління. Це створює механізми, які дозволяють державі не лише реагувати на безпосередні виклики, але й готуватися до складних багатовимірних загроз, що постійно трансформуються у сучасному глобалізованому і геополітично напруженому світі.

Як підкреслюється у звітах ЄС та НАТО, формування довгострокових моделей управління національною стійкістю потребує, окрім інтеграції державних інституцій, приватного сектору та громадянського суспільства, також глибокої цифрової трансформації [13]. Це підтверджує необхідність не лише реагувати на конкретні загрози, а й формувати проактивні стратегії розвитку управлінських моделей, які здатні динамічно підлаштовуватися під нові виклики.

Висновки. Вище проведений аналіз дозволяє зробити наступні висновки. Стратегічні підходи до зміцнення національної стійкості в умовах зовнішніх загроз передбачають формування комплексної системи, що інтегрує політичні, економічні, соціальні, інформаційні та безпекові складники та забезпечує системний підхід до оцінки ризиків, управління кризами та формування превентивних механізмів. *Комплексність* у цьому контексті виступає як методологічна основа для синхронізації дій державних інститутів, бізнесу та громадянського суспільства, що дозволяє не лише протидіяти зовнішнім викликам, а й підтримувати стабільність соціально-економічних процесів та політичної системи. *Інтегрованість* системи національної стійкості забезпечує координацію багаторівневих управлінських механізмів, міжсекторальну взаємодію та ефективне використання ресурсів, що критично важливо в умовах гібридних, кібернетичних та інформаційних загроз, оскільки вона дозволяє об'єднати зусилля урядових структур, місцевих органів, приватного сектору та громадянського суспільства у єдину функціональну систему реагування на кризи. *Адаптивність* виступає ключовим фактором

здатності системи швидко і ефективно реагувати на трансформацію зовнішніх загроз, прогнозувати потенційні ризики та забезпечувати відновлення критичних систем після кризових ситуацій, що є особливо актуальним у контексті постійної динаміки гібридних загроз, кібернетичних атак і мультидоменних викликів.

Важливою складовою стратегічного підходу є кіберстійкість, яка розглядається як інтегративний елемент національної безпеки і включає здатність держави не лише протидіяти кібератакам, а й швидко відновлювати критичні інформаційні та технологічні системи, поєднуючи превентивні та активні оборонні заходи, а також інтеграцію цифрових технологій у процеси управління ризиками, моніторингу загроз та забезпечення безпеки критичної інфраструктури. Розвиток сценарного планування та моделей управління кризовими ситуаціями забезпечує проактивне реагування на потенційні загрози, дозволяє оцінювати альтернативні сценарії розвитку подій і формувати довгострокові стратегії управління, що підвищує гнучкість і стійкість державних систем.

Невід'ємним компонентом є соціальна складова, що включає підвищення рівня довіри громадян до інститутів влади, активізацію громадянського суспільства та розвиток соціальної згуртованості, що створює передумови для ефективної самоорганізації та партнерства у сфері безпеки. Ці фактори, поряд із інтеграцією державних і приватних ресурсів та цифровою трансформацією, формують багатошарову систему безпеки, здатну адаптуватися до швидкоплинних змін зовнішнього середовища, мінімізувати негативні наслідки кризових ситуацій та забезпечувати відновлення й розвиток державних інститутів у довгостроковій перспективі. У цьому контексті стратегічні підходи до зміцнення національної стійкості виступають не лише як інструмент реагування на сучасні загрози, а й як методологічна основа для побудови динамічної, інтегрованої та адаптивної системи безпеки, яка здатна протистояти зовнішнім викликам, підтримувати політичну та економічну стабільність і забезпечувати сталий розвиток держави в умовах мінливого безпекового простору.

Література:

1. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 456 с. URL : https://www.marshallcenter.org/sites/default/files/files/2022-04/Reznikova_Resilience_UKR.pdf

2. Korostelina, Karina V. National Resilience to Protracted Violence in Ukraine. *Peace and Conflict Studies*. 2020. Vol. 27: No. 2, Article 4. URL : https://nsuworks.nova.edu/pcs/vol27/iss2/4

3. Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats. 2024. URL : https://data.consilium.europa.eu/doc/document/CM-1107-2024-INIT/en/pdf

4. Resilience, civil preparedness and Article 3. NATO. 2024. URL : https://www.nato.int/cps/uk/natohq/topics_132722.htm?selectedLocale=en

5. Каліман М.Р. Деякі питання вдосконалення процесу забезпечення національної стійкості в Україні. *Юридичний науковий електронний журнал*. 2021. № 3. URL : http://lsej.org.ua/3_2021/51.pdf

6. Назаров М. С. Національна стійкість України: від концептуальних засад до практичної реалізації. *Науковий журнал «Політикус»*. 2020. № 2. URL : http://www.politicus.od.ua/2_2020/11.pdf

7. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : Указ Президента України від 27 вересня 2021 року № 479/2021. URL : https://www.president.gov.ua/documents/4792021-40181

8. Я. Лазебник. Концепція національної стійкості: український контекст. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2024. Випуск 56, с. 223-228. URL : http://fps-visnyk.lnu.lviv.ua/archive/56_2024/27.pdf

9. Концептуальні засади національної стійкості та державна політика врегулювання воєнно-політичних конфліктів: колективна монографія / за заг. ред. Г.П. Ситника; ТОВ «Академпрес». Київ, 2024. 358 с. URL : https://ipacs.knu.ua/pages/dop/391/files/221d1a94-527f-475a-9005-2c66fc64f84e.pdf

10. Md Faisal Ahmed, Abul Hasan Molla, Md Riaj Uddin. Advancing Cyber Resilience: Bridging the Divide Between Cyber Security and Cyber Defense. 2023. International Journal For Multidisciplinary Research. URL : https://www.researchgate.net/publication/377814266_Advancing_Cyber_Resilience_Bridging_the_Divide_Between_Cyber_Security_and_Cyber_Defense

11. Kağan Cenk Mizrak. Crisis Management and Risk Mitigation: Strategies for Effective Response and Resilience. Trends, Challenges, and Practices in Contemporary Strategic Management. 2024. URL : https://www.researchgate.net/publication/378432533_Crisis_Management_and_Risk_Mitigation_Strategies_for_Effective_Response_and_Resilience

12. Хаустова В. Є., Трушкіна Н. В. Ризики та загрози національній безпеці: сутність і класифікація. *Бізнес Інформ*. 2024. № 10. С. 6-22. URL : https://www.business-inform.net/export_pdf/business-inform-2024-10_0-pages-6_22.pdf

13. The resilience of the European Union and NATO in an era of multiple crises. URL : https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-02-28/resilience-european-union-and-nato-era-multiple-crises

References:

1. Reznikova, O. O. (2022). *Natsionalna stiikist v umovakh minlyvoho bezpekovogo seredovyshcha* [National Resilience in a Changing Security Environment]. Kyiv: NISD. Retrieved from: https://www.marshallcenter.org/sites/default/files/files/2022-04/Reznikova_Resilience_UKR.pdf [in Ukrainian].

2. Korostelina, K. V. (2020). National Resilience to Protracted Violence in Ukraine. Peace and Conflict Studies, 27(2), Article 4. Retrieved from: https://nsuworks.nova.edu/pcs/vol27/iss2/4 [in Ukrainian].

3. Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats. (2024). Retrieved from: https://data.consilium.europa.eu/doc/document/CM-1107-2024-INIT/en/pdf

4. NATO. (2024). Resilience, civil preparedness and Article 3. Retrieved from: https://www.nato.int/cps/uk/natohq/topics_132722.htm?selectedLocale=en

5. Kaliman, M. R. (2021). Deyaki pytannya vdoskonalennya protsesu zabezpechennya natsionalnoi stiikosti v Ukraini [Some Issues of Improving the Process of Ensuring National Resilience in Ukraine]. Yurydychnyi naukovyi elektronicnyi zhurnal, 3. Retrieved from: http://lsej.org.ua/3_2021/51.pdf [in Ukrainian].

6. Nazarov, M. S. (2020). Natsionalna stiikist Ukrainy: vid kontseptualnykh zasad do praktychnoyi realizatsii [National Resilience of Ukraine: From Conceptual Foundations to Practical Implementation]. Politykus, 2. Retrieved from: http://www.politicus.od.ua/2_2020/11.pdf [in Ukrainian].

7. Verkhovna Rada of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku «Pro zaprovadzhennia natsionalnoi systemy stiikosti»: Ukaz Prezydenta Ukrainy №479/2021 [On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Introduction of the National Resilience System": Presidential Decree №479/2021]. Retrieved from: . https://www.president.gov.ua/documents/4792021-40181 [in Ukrainian].

8. Lazebnyk, Ya. (2024). Kontseptsiia natsionalnoi stiikosti: ukrainskyi kontekst [The Concept of National Resilience: Ukrainian Context]. Visnyk Lvivskoho universytetu. Seriia filosofsko-politolohichni studii, 56, 223–228. Retrieved from: http://fps-visnyk.lnu.lviv.ua/archive/56_2024/27.pdf [in Ukrainian].

9. Sytnyk, H. P. (Ed.). (2024). Kontseptualni zasady natsionalnoi stiikosti ta derzhavna polityka vriehulyuvannia voienno-politychnykh konfliktiv [Conceptual Foundations of National Resilience and State Policy for Regulation of Military-Political Conflicts]. Kyiv: Akadempress. Retrieved from: https://ipacs.knu.ua/pages/dop/391/files/221d1a94-527f-475a-9005-2c66fc64f84e.pdf [in Ukrainian].

10. Ahmed, M. F., Molla, A. H., & Uddin, M. R. (2023). Advancing Cyber Resilience: Bridging the Divide Between Cyber Security and Cyber Defense. International Journal For Multidisciplinary Research. Retrieved from: https://www.researchgate.net/publication/377814266_Advancing_Cyber_Resilience_Bridging_the_Divide_Between_Cyber_Security_and_Cyber_Defense

11. Mizrak, K. C. (2024). Crisis Management and Risk Mitigation: Strategies for Effective Response and Resilience. Trends, Challenges, and Practices in Contemporary Strategic Management. Retrieved from: https://www.researchgate.net/publication/378432533_Crisis_Management_and_Risk_Mitigation_Strategies_for_Effective_Response_and_Resilience

12. Khaustova, V. E., & Trushkina, N. V. (2024). Ryzyky ta zahrozy natsionalnii bezpetsi: sutnist i klasyfikatsiia [Risks and Threats to National Security: Essence and Classification]. Biznes Inform, 10, 6–22. Retrieved from: https://www.business-inform.net/export_pdf/business-inform-2024-10_0-pages-6_22.pdf [in Ukrainian].

13. The resilience of the European Union and NATO in an era of multiple crises. (2025, February 28). OSW Commentary. Retrieved from: https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-02-28/resilience-european-union-and-nato-era-multiple-crises