*УДК 351.86:355.45(477)*

*https://doi.org/10.52058/2786-6300-2025-9(39)-276-288*

**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, м. Київ, https://orcid.org/0000-0003-1914-9481

# ЗАГРОЗИ НАЦІОНАЛЬНІЙ СТІЙКОСТІ ТА ІНСТРУМЕНТИ ЇХ ПРОТИДІЇ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ БЕЗПЕКИ

**Анотація.** У статті досліджено багатовимірний характер загроз національній стійкості в умовах сучасних безпекових викликів, що виходять за межі традиційних військових загроз і охоплюють інформаційні, гібридні та стратегічні ризики. Визначено, що ці загрози мають складну структуру, яка поєднує політичні, економічні, соціальні, інформаційні та культурні компоненти, що створює нове середовище безпеки з асиметричними викликами. Встановлено, що інформаційні загрози, зокрема масштабні дезінформаційні кампанії, становлять особливу загрозу для демократичних інститутів і соціальної єдності, що особливо актуально для України в умовах російської агресії. Показано, що гібридні загрози виступають комплексним поєднанням військових, політичних, інформаційних і кібернетичних інструментів, які активно застосовуються для підриву функціонування держави зсередини. Окреслено значення стратегічних ризиків, що включають інституційну слабкість, нерівність у ресурсах, демографічні дисбаланси та фінансову нестабільність, як основних детермінант вразливості національної системи. Обґрунтовано, що саме інтеграція фінансової складової з соціальними й інституційними факторами є необхідною передумовою збалансованої стійкості. Визначено інструменти протидії загрозам, серед яких ключовими є стратегічні комунікації, інформаційна безпека та організаційно-правові механізми. Встановлено їхню роль у формуванні суспільного дискурсу, захисті інформаційного простору та забезпеченні нормативно-правового поля для реагування на загрози. Показано, що успішна протидія вимагає системного підходу з інтеграцією європейських стандартів і практик, що створюють умови для колективної безпеки та ефективної координації. Зроблено висновок, що національна стійкість у XXI столітті проявляється у здатності держави та суспільства адаптуватися та відновлювати стабільність у умовах багатовекторних викликів. Для України це означає необхідність комплексного поєднання політичних, правових, соціальних і технологічних заходів задля ефективної відповіді на сучасні виклики безпеки.

**Ключові слова:** національна стійкість, національна безпека, адаптивність, гібридні загрози, інформаційна безпека, стратегічні комунікації, організаційно-правові механізми, фінансові інструменти, системний підхід, Україна, європейська інтеграція, кібербезпека, кризове управління.

**Zaporozhets Tetiana Volodymyrivna** 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

## THREATS TO NATIONAL RESILIENCE AND TOOLS TO COUNTER THEM IN THE CONDITIONS OF MODERN SECURITY CHALLENGES

**Abstract:** The article explores the multidimensional nature of threats to national resilience under modern security challenges, which go beyond traditional military threats and encompass informational, hybrid, and strategic risks. It is determined that these threats possess a complex structure combining political, economic, social, informational, and cultural components, thereby shaping a new security environment characterized by asymmetric challenges. The study establishes that informational threats, particularly large-scale disinformation campaigns, pose a significant danger to democratic institutions and social cohesion, which is especially relevant for Ukraine in the context of Russian aggression. It demonstrates that hybrid threats represent a comprehensive combination of military, political, informational, and cyber instruments actively employed to undermine the state from within. The article outlines the significance of strategic risks—including institutional weakness, resource inequality, demographic imbalances, and financial instability—as the main determinants of national vulnerability. It substantiates that integrating the financial dimension with social and institutional factors is a necessary precondition for balanced resilience. The research identifies tools for countering threats, with strategic communications, information security, and organizational-legal mechanisms being key among them. Their role is highlighted in shaping public discourse, protecting the information space, and ensuring the regulatory framework for responding to threats. The analysis shows that effective counteraction requires a systemic approach with the integration of European standards and practices, which create the conditions for collective security and effective coordination. It concludes that national resilience in the 21st century is manifested in the state's and society's ability to adapt and restore stability amid multidimensional challenges. For Ukraine, this implies the necessity of a comprehensive combination of political, legal, social, and technological measures to ensure an effective response to contemporary security challenges.

**Key words:** national resilience, national security, adaptability, hybrid threats, information security, strategic communications, organizational and legal mechanisms, financial instruments, systemic approach, Ukraine, European integration, cybersecurity, crisis management

**Постановка проблеми.** Національна стійкість у сучасному світі постає як інтегральний показник здатності держави протидіяти багатовимірним викликам безпеки та забезпечувати стабільність суспільно-політичної системи, економіки й культурно-ціннісного середовища. Особливої актуальності національна стійкість набуває в умовах глобальних трансформацій, гібридних загроз і зростання ролі інформаційного простору як ключового чинника впливу на національну безпеку. Сучасні війни та конфлікти характеризуються не лише застосуванням військової сили, але й активним використанням інформаційно-психологічних операцій, стратегічних маніпуляцій та кібератак, що спрямовані на підрив соціальної єдності, довіри до інститутів влади та спроможності держави реагувати на кризові ситуації.

У цьому контексті дослідження загроз національній стійкості та визначення ефективних інструментів їх протидії є вкрай важливими для формування цілісної системи державної політики у сфері безпеки. Актуальність статті зумовлена також необхідністю виокремлення та наукового обґрунтування класифікації сучасних загроз національній стійкості; визначення комплексу інструментів їх подолання; формування концептуальної основи для розбудови стійкої державної системи реагування на багатовимірні виклики безпеки.

**Аналіз останніх досліджень і публікацій.** Актуальні дослідження національної стійкості концентруються переважно на вивченні стратегічних комунікацій як ключового механізму протидії гібридним загрозам. Д. Казмірук [5] визначає їх інструментом нейтралізації інформаційно-психологічного впливу противника та мобілізації суспільної єдності. У працях А. Благодарного та О. Кононця [6] стратегічні комунікації розглядаються як невід'ємний елемент сектору безпеки й оборони, що забезпечує синергію між державними інституціями та суспільством. Методологічну й практичну основу цього напряму системно висвітлено у посібнику під редакцією О. Давліканової та Л. Компанцевої [7], де наголошено на необхідності інтеграції комунікацій у загальнодержавну політику. У міжнародних наукових і аналітичних джерелах загрози національній стійкості розглядаються насамперед крізь призму структурних і глобальних ризиків. Світовий звіт про розвиток 2022 року [3] акцентує на фінансовій вразливості як ключовій детермінанті затяжних криз, що безпосередньо підриває здатність держав протидіяти шокам. У Доповіді про людський розвиток 2021-2022 років окреслено концепцію «нового комплексу невизначеності», сформованого поєднанням пандемічних, воєнних, кліматичних та соціально-політичних

факторів [4]. Попри це, актуальним залишається завдання створення системної класифікації загроз та вироблення ефективних механізмів імплементації міжнародних і європейських стандартів у національну політику. Саме їх інтеграція виступає ключовою передумовою підвищення стійкості України в умовах сучасних викликів безпеки.

**Мета статті** – проаналізувати ключові загрози національній стійкості в умовах сучасних викликів безпеки та окреслити інституційні, правові й організаційні інструменти їх протидії з урахуванням міжнародного та європейського досвіду.

**Виклад основного матеріалу.** Загрози національній стійкості в умовах сучасних викликів безпеки становлять надскладний і багатовимірний феномен, що потребує глибокого системного аналізу. Їх природа значно виходить за межі традиційних військових чинників, охоплюючи тривалі інформаційні, гібридні та стратегічні ризики, що формують новітнє середовище безпеки. У цьому контексті важливим є усвідомлення асиметричного, багатогранного та комплексного характеру цих загроз, які поєднують у собі компоненти політичної, економічної, соціальної, інформаційної та культурної сфер. Такий підхід є важливим для переходу від традиційних моделей безпеки до концепції національної стійкості, яка акцентує увагу на здатності держави та суспільства адаптуватися та відновлюватися під тиском багатовекторних викликів.

Інформаційні загрози в сучасному світі посідають роль однієї з найбільш швидкоплинних і руйнівних форм небезпеки. Вони здатні миттєво поширюватися через цифрові канали, формуючи тривалий когнітивний і психологічний вплив на суспільство. Як зазначає Європейська Комісія в «Плані дій щодо боротьби з дезінформацією» (2018), інформаційні маніпуляції у вигляді дезінформації є безпосередньою загрозою функціонуванню демократичних інститутів, знижуючи довіру до влади, послаблюючи соціальну згуртованість і підриваючи демократичні процеси [1].

В українських умовах ця загроза набула особливої актуальності після початку російської військової агресії, що супроводжується масштабними кампаніями дезінформації, спрямованими на делегітимізацію держави на міжнародній арені та послаблення внутрішньої єдності.

Водночас загрози інформаційного характеру рідко діють ізольовано, вони інтегруються у широкий спектр гібридних загроз. У наукових працях під гібридними загрозами розуміють комплексне поєднання військових, політичних, економічних, кібернетичних та інформаційних інструментів, застосованих синхронізовано для досягнення стратегічних цілей агресора. НАТО визначає гібридні загрози як форму діяльності, що підриває функціонування держави зсередини, використовуючи вразливості суспільства та політичної системи [2].

Для України гібридні загрози проявляються через поєднання збройної агресії з кібератаками, енергетичним шантажем, інформаційним впливом та

підтримкою внутрішньої дестабілізації. Таке багатовекторне втручання створює передумови для «каскадних криз», коли одна сфера ураження провокує деструктивні процеси в інших, що ускладнює здатність держави до забезпечення національної стійкості.

Окрему увагу слід приділити стратегічним ризикам, які охоплюють тривалі структурні фактори вразливості держави. Тут мова йде про інституційну слабкість, нерівність у доступі до ресурсів, демографічні дисбаланси, відтік кваліфікованих кадрів та інші фундаментальні виклики, які зумовлюють довгострокову вразливість національної системи. Ці ризики створюють передумови для послаблення функціонування державних інститутів, підривають ефективність управління та загалом знижують спроможність країни запобігати і реагувати на зовнішні й внутрішні виклики.

Вказаний комплекс проблем безпосередньо пов'язаний із фінансовою стабільністю, яка є також важливим фактором формування загальної національної стійкості. З огляду на роль фінансових ресурсів у забезпеченні безперебійного функціонування держави, їх стан і механізми управління ними мають вирішальне значення для пом'якшення структурних ризиків.

Згідно зі «**Світовою доповіддю про розвиток 2022: фінанси для справедливого відновлення»** (World Development Report, WDR) [3], фінансові аспекти виступають визначальним фактором у формуванні структурних ризиків для держави, оскільки саме вони опосередковують як швидкість виходу з кризових станів, так і можливість переходу до інклюзивного розвитку. Ігнорування цих аспектів, як наголошує Світовий банк, здатне перетворити локальні шоки на затяжні кризові процеси, що блокують економічне зростання, обмежують доступ до кредитних ресурсів і створюють передумови для соціальної нестабільності. Такий підхід співвідноситься з положеннями «Доповіді про людський розвиток 2021-2022: невизначені часи, непевні життя: формування нашого майбутнього у світі трансформацій» (Human Development Report 2021-22, HDR), у якій підкреслюється, що сучасний світ опинився у стані «нового комплексу невизначеності» [4], який не зводиться до звичних «циклічних шоків», а має нашарований і взаємопов'язаний характер. Документ виокремлює три взаємодіючі напрями невизначеності, що підсилюють одна одну та перетворюють окремі збурення на системні кризи:

– *небезпечні планетарні зміни*: кліматичні трансформації, деградація біорізноманіття, нові зоонози множать екологічні ризики та розширюють соціальну вразливість, насамперед у країнах і групах з нижчими доходами, де спроможність до адаптації обмежена;

– *суспільні трансформації*, які є необхідними для пом'якшення планетарних тисків і використання потенціалу нових технологій (декарбонізація енергетики, переоблаштування агропродовольчих систем, цифрові зрушення), несуть

перехідні ризики: від перерозподілу зайнятості та доходів до дезорієнтації інститутів, які не встигають за темпом змін;

– *інтенсифікована поляризація* (політична, соціальна, інформаційна), підсилена способами використання цифрових технологій і середовищ, підриває довіру, ускладнює колективні дії й перетворює одноразові шоки на тривалі ланцюгові кризи через блокування компромісів і солідарних рішень.

У підсумку утворюється середовище «накладених ризиків», у якому шоки нашаровуються замість того, щоб згасати: війна, пандемія, кліматичні зміни швидко трансформуються у глобальну кризу вартості життя, продовжуючи розривати ланцюги постачання, розгойдувати ціни на енергоносії та продукти харчування. Саме це, за HDR, пояснює безпрецедентне падіння глобального Індексу людського розвитку протягом двох років поспіль (2020-2021) та масове відчуття небезпеки (ще до пандемії понад 6 із 7 людей декларували відчуття небезпеки) [4].

HDR пропонує рамку з трьох І: «*Three I's framework» - Investment, Insurance, and Innovation* (інвестиції, страхування та інновації), які полягають у наступному.

Її змістовне наповнення дає змогу осмислити новий комплекс невизначеності та визначити базові орієнтири для державної політики у сфері протидії системним ризикам. *Інвестиції* розглядаються як фундамент для довгострокового підвищення стійкості суспільства через забезпечення рівного доступу до освіти, охорони здоров'я, цифрової інфраструктури та механізмів соціальної мобільності. У цьому контексті особливе значення мають інституційні інвестиції, спрямовані на розвиток довіри до державних інститутів, адже дефіцит соціального капіталу посилює вразливість до дезінформаційних атак і підриває національну стійкість у ширшому вимірі.

Друга складова рамки – *страхування,* передбачає формування багаторівневої системи захисту населення та економіки від кризових явищ. Йдеться не лише про фінансові інструменти (наприклад, страхування від безробіття чи механізми соціальних гарантій), але й про політико-правові запобіжники, які дозволяють мінімізувати ризики дестабілізації у випадку гібридних атак, масштабних кіберасигнальних операцій чи енергетичних криз. Таким чином, страхування виконує роль буфера, що пом'якшує наслідки системних шоків і забезпечує збереження функціональної спроможності держави навіть у надзвичайних обставинах.

Третя складова – *інновації,* є рушієм адаптації до нових викликів, зокрема у сфері інформаційної безпеки та стратегічних комунікацій. Інноваційні рішення охоплюють як розвиток технологій штучного інтелекту для виявлення дезінформаційних кампаній, так і нові формати взаємодії держави з громадянами, спрямовані на підвищення прозорості та підзвітності. При цьому інноваційність

трактується не лише як технологічне оновлення, а й як здатність суспільства до соціальних і культурних трансформацій, які підсилюють його стійкість перед глобальними ризиками [4].

Таким чином, рамка «трьох І» формує концептуальний підхід до протидії сучасним загрозам національній стійкості, що поєднує довгострокові інвестиції у розвиток, ефективні механізми страхування від криз та інноваційні практики реагування. Для України, яка перебуває у стані тривалих гібридних викликів і водночас здійснює інтеграцію до європейського безпекового простору, імплементація цього підходу може стати ключовою передумовою зміцнення стійкості державних інститутів та суспільства.

Аргументація WDR 2022 [3] логічно доповнює HDR [4]: окремі аспекти присвячені фінансовій інклюзії, державним гарантійним схемам, а також «зеленим» ринкам капіталу (державні стійкі/зелені облігації) як інструментам стійкого відновлення.

У комплексі ці два звіти формують єдину концепцію: перший окреслює новий структурний стан невизначеності та його багатовимірні наслідки для суспільств, другий пропонує практичні інструменти фінансового регулювання як запобіжники системних криз. Їх інтеграція у політику національної стійкості дозволяє сформувати висновок, що без одночасного зміцнення соціальних, екологічних та фінансових інститутів жодна держава не зможе адекватно реагувати на виклики гібридного, багатовимірного середовища XXI століття. Для політики національної стійкості це означає, що стратегічні комунікації та інституційні реформи мають реалізовуватись паралельно з превентивним управлінням балансами домогосподарств, бізнесу, банків і держави, оскільки саме на їх перетині вирішується, чи перетворяться окремі шоки на довготривалі кризи.

Таким чином, інформаційні загрози, гібридні впливи та стратегічні ризики формують єдиний взаємопов'язаний кластер, де кожен елемент підсилює інший, створюючи синергетичний ефект дестабілізації і ставить під сумнів національну стійкість у цілому. Таке поєднання вимагає не лише комплексного розуміння природи небезпек, але й належних механізмів протидії, які здатні адекватно реагувати на всі елементи цього складного спектру загроз.

Очевидним є те, що сама по собі класифікація загроз, хоча й важлива для теоретичного осмислення проблеми, не забезпечує належного рівня національної стійкості. Умовою її практичного утвердження є наявність інтегрованої системи механізмів реагування, яка поєднує політико-комунікаційні, організаційно-правові та інформаційно-технологічні засоби.

Перш за все, стратегічні комунікації у науковому та практичному вимірі визнаються ключовим чинником протидії гібридним загрозам. Як зазначає Д. Казмірук, стратегічні комунікації є не лише технологією поширення

інформації, а інституційно організованим процесом формування суспільного дискурсу та ціннісних орієнтацій, що здатні мобілізувати суспільство в умовах гібридної війни [5]. Відтак, стратегічна комунікація має розглядатися не як додатковий інструмент, а як системоутворюючий елемент державної політики безпеки.

У дослідженні А. Благодарного та О. Кононця наголошується, що для сектору безпеки і оборони України стратегічні комунікації виконують функцію поєднання військових, інформаційних та політичних зусиль у єдиний захисний контур, що дозволяє зменшувати ефективність ворожих маніпуляцій і підвищувати рівень довіри громадян до державних інституцій [6].

Таким чином, стратегічні комунікації не обмежуються суто інформаційною сферою, а стають фактором консолідації державної політики та громадської підтримки, що є критично важливим в умовах затяжної гібридної агресії.

У практичному вимірі стратегічні комунікації виступають також як механізм координації між державними інституціями, громадянським суспільством та міжнародними партнерами. Це чітко простежується у практичному посібнику «Стратегічні комунікації для безпекових і державних інституцій», де підкреслюється, що комунікаційні стратегії повинні будуватися на принципах довіри, прозорості та проактивності, створюючи умови для формування стійкого інформаційного середовища [7]. Такий підхід не лише підвищує ефективність реагування на зовнішні інформаційні атаки, але й зміцнює внутрішній соціальний капітал, що є фундаментом національної стійкості.

Водночас стратегічні комунікації не можуть функціонувати ефективно без належної системи інформаційної безпеки, що забезпечує захист інформаційно-комунікаційних систем від кіберзагроз, інформаційних атак та технологічних збоїв. Закон України «Про захист інформації в інформаційно-комунікаційних системах» визначає базові правові засади захисту даних та регламентує діяльність у сфері кіберзахисту [8].

У стратегічному вимірі ключовим документом є «Стратегія інформаційної безпеки України», затверджена Указом Президента № 685/2021, яка визначає цілі державної політики у сфері захисту інформаційного простору, протидії дезінформації та розвитку національних спроможностей у галузі кіберзахисту [9]. Ця стратегія є відповіддю на актуальні загрози та дороговказом для формування інтегрованої системи, що охоплює нормативне регулювання, інституційні практики та міжнародне співробітництво.

Організаційно-правові механізми є невід’ємною складовою системи протидії сучасним загрозам. В умовах багатовимірного безпекового середовища це поле охоплює загальнонаціональні нормативно-правові акти і стратегічні документи, спеціалізовані закони й регламенти.

Першою складовою механізму є загальнонаціональні нормативні акти, які визначають принципи та суб'єкти політики безпеки. Закон України «Про національну безпеку України» закріплює основні принципи державної політики у сфері національної безпеки, розмежовує повноваження органів влади та створює правову основу для координації дій у кризових ситуаціях; цей закон виступає рамковим актом для всіх спеціалізованих норм [10].

Стратегія національної безпеки України (схвалена РНБО та введена в дію Указом Президента, 2020) [11] конкретизує підходи до забезпечення стійкості, роблячи акцент на стійкості як складовій стримування і оборони та визначаючи міжвідомчу структуру реагування. Наступним компонентом є спеціалізовані стратегії та акти, які адресують конкретні сфери вразливостей. Зокрема, Стратегія інформаційної безпеки України [9] встановлює цілі й пріоритети у сфері захисту інформаційного простору, протидії дезінформації та розвитку національних спроможностей у кіберсередовищі; її впровадження вимагає координації між оборонними, правоохоронними, комунікаційними та освітніми інституціями. Закон «Про основні засади забезпечення кібербезпеки України» формує правову архітектуру для захисту життєво важливих інтересів держави в цифровому просторі, визначає ключових національних суб'єктів кібербезпеки та механізми їх координації [12]. Разом ці нормативні акти створюють юридичну базу, без якої неможливе ні системне управління кризами, ні реалізація превентивних заходів.

Третій компонент можна визначити як процесуально-інституційний: закони і стратегії реалізуються через міжвідомчу координацію, стандарти діяльності, режимні процедури і кризові плани, ефективність яких залежить від чіткої регламентації повноважень, алгоритмів обміну інформацією, режимів швидкого прийняття рішень і прозорих процедур підзвітності.

Не менш важливим аспектом є відповідність національного законодавства міжнародним стандартам та інтеграція європейських механізмів підвищення стійкості в національну практику. Європейські ініціативи, зокрема Директива про стійкість критичних об'єктів (Critical Entities Resilience Directive), яка визначає базові вимоги щодо ідентифікації критичних суб'єктів, оцінки ризиків, а також створення планів безперервності діяльності та механізмів реагування на кризи [13].

Її положення доповнюються Директивою NIS2 та відповідними актами імплементації, зокрема Регламентом (ЄС) 2024/2690, який встановлює технічні та методологічні вимоги до заходів з управління ризиками кібербезпеки [14].

Рекомендація Ради ЄС 2024 року щодо координації реагування на порушення роботи критичної інфраструктури з транскордонними наслідками пропонує «дорожню карту» взаємодії держав-членів у випадку масштабних криз, підкреслюючи необхідність колективних дій та обміну інформацією між компетентними органами [15].

Адаптація цих європейських підходів на національному рівні створює умови для посилення сумісності міждержавних механізмів реагування, підвищує якість інцидент-менеджменту та сприяє зміцненню колективної безпеки в регіоні. Для України це означає не лише формальну імплементацію норм щодо захисту критичних об'єктів, але й розвиток механізмів публічно-приватного партнерства, які забезпечують постійний обмін інформацією про інциденти та координацію відповідей між державними органами і операторами інфраструктури.

Механізми фінансово-правової підтримки стійкості є наступним компонентом: закони та підзаконні акти повинні створювати правові підстави для бюджетного резерву, спеціальних фондів відновлення, державних гарантій і стимулів для інвестицій у критичну інфраструктуру та кіберзахист. Це безпосередньо корелюється із висновками WDR 2022 про роль фінансів у запобіганні затяжним кризам: без правових механізмів, що дозволяють швидко мобілізувати ресурси й спрямовувати їх на пріоритетні напрями, держава втрачає можливість ефективно амортизувати шоки.

Нарешті, не можна ігнорувати соціально-правову складову. Законодавчі норми повинні збалансувати заходи безпеки з гарантіями прав і свобод, щоб протидія, спрямована на відновлення стійкості, не підривала легітимності держави в очах громадян. Саме правова прозорість, контроль над повноваженнями органів під час надзвичайних ситуацій і механізми доступу до правосуддя формують довгострокову суспільну стійкість.

Отже, організаційно-правові механізми виконують роль архітектури державної стійкості: вони встановлюють правила, координаційні канали, ресурсні підстави та межі застосування надзвичайних повноважень. У контексті гібридних і інформаційних загроз їхня сила залежить від двох взаємопов'язаних властивостей: інституційної цілісності (чітко визначені повноваження й відповідальність) та регуляторної гнучкості (здатність оперативно адаптуватися до нових форм викликів), а також від здатності до імплементації європейських стандартів захисту критичних об'єктів і кіберстійкості.

**Висновки.** Національна стійкість у XXI столітті визначається здатністю держави не лише відбивати традиційні загрози, але й ефективно адаптуватися до гібридних викликів, які поєднують військові, інформаційні, кібернетичні, економічні та соціальні чинники. Ключову небезпеку становлять інформаційні маніпуляції, що підривають довіру, а також стратегічні ризики, пов'язані з фінансовою нестабільністю, інституційною слабкістю та глобальними трансформаціями. Протидія цим викликам потребує цілісної системи, де стратегічні комунікації відіграють консолідуючу роль, забезпечуючи мобілізацію суспільства і координацію зусиль між владою, громадянами та міжнародними партнерами. Організаційно-правові механізми формують правову

основу реагування, водночас забезпечуючи баланс між безпековими заходами та захистом прав і свобод. Інтеграція європейських стандартів щодо захисту критичної інфраструктури та управління ризиками створює умови для підвищення сумісності з колективними безпековими практиками. Фінансово-правові інструменти, включаючи резервні фонди та державні гарантії, дозволяють запобігати затяжним кризам, тоді як інноваційні підходи забезпечують гнучкість і здатність швидко реагувати на нові загрози.

Отже, зміцнення національної стійкості України потребує комплексного поєднання стратегічних комунікацій, правових гарантій, інституційних реформ і міжнародної інтеграції, що у сукупності створюють основу для ефективного протистояння багатовимірним викликам сучасності.

***Література***:

1. Joint communication to the european parliament, the european council, the council, the european economic and social committee and the committee of the regions. Action Plan against Disinformation. 2018. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018JC0036&

2. Countering hybrid threats. NATO 2024. URL : https://www.nato.int/cps/en/natohq/topics_156338.htm

3. World Development Report 2022. FINANCE FOR AN EQUITABLE RECOVERY. URL: https://www.worldbank.org/en/publication/wdr2022

4. Human Development Report 2021-2022. Uncertain Times, Unsettled Lives: Shaping our Future in a Transforming World. URL : https://hdr.undp.org/content/human-development-report-2021-22

5. Д.Казмірук. Роль стратегічної комунікації в забезпеченні національної безпеки України в умовах гібридної війни. *Вісник Прикарпатського університету. Серія: Політологія*. 2025. № 20. URL : https://journals.pnu.if.ua/index.php/politology/article/view/226

6. Благодарний, А., Кононець, О. Стратегічні комунікації у секторі безпеки і оборони України. *Молодий вчений*. 2023. № 1 (113), С. 5-9. https://molodyivchenyi.ua/index.php/journal/article/view/5685

7. Стратегічні комунікації для безпекових і державних інституцій : практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин; за заг. ред. О. Давліканової, Л. Компанцевої]. Київ: ТОВ «ВІСТКА», 2022. 278 с. URL : http://fes.kiev.ua/n/cms/fileadmin/upload2/Book_28-06-2022_web-3.pdf

8. Про захист інформації в інформаційно-комунікаційних системах: Закон України. URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України №685/2021. URL : https://www.president.gov.ua/documents/6852021-41069

10. Про національну безпеку України : Закон України. URL : https://zakon.rada.gov.ua/laws/main/2469-19#Text

11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України. URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text

12. Про основні засади забезпечення кібербезпеки України : Закон України. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

13. Making critical entities more resilient. 2022. URL : https://eur-lex.europa.eu/EN/legal-content/summary/making-critical-entities-more-resilient.html

14. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures. URL : https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

15. COUNCIL RECOMMENDATION on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance. 2024. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371

***References:***

1. European Commission. (2018). Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan against Disinformation. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018JC0036&

2. NATO. (2024). Countering hybrid threats. Retrieved from: https://www.nato.int/cps/en/natohq/topics_156338.htm

3. World Development Report 2022. World Bank. Finance for an Equitable Recovery. Retrieved from: https://www.worldbank.org/en/publication/wdr2022

4. Human Development Report 2021-2022. UNDP. 2022. Uncertain Times, Unsettled Lives: Shaping our Future in a Transforming World. Retrieved from: https://hdr.undp.org/content/human-development-report-2021-22

5. Kazmiruk, D. (2025). Rol stratehichnoi komunikatsii v zabezpechenni natsionalnoi bezpeky Ukrainy v umovakh hibrydnoi viiny [The Role of Strategic Communication in Ensuring Ukraine's National Security under Hybrid Warfare]. Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia, (20). Retrieved from: https://journals.pnu.if.ua/index.php/politology/article/view/226 [in Ukrainian].

6. Blahodarnyi, A., & Kononets, O. (2023). Stratehichni komunikatsii u sektori bezpeky i oborony Ukrainy [Strategic Communications in Ukraine's Security and Defense Sector]. Molodyi vchenyi, 1(113), 5–9. Retrieved from: https://molodyivchenyi.ua/index.php/journal/article/view/5685 [in Ukrainian].

7. Kompantseva, L., Zaruba, O., Cherevatyi, S., Akulshyn, O. (2022). Stratehichni komunikatsii dlia bezpekovykh i derzhavnykh instytutsii: Praktychnyi posibnyk [Strategic Communications for Security and State Institutions: A Practical Guide]. O. Davlikanova & L. Kompantseva (Eds.). Kyiv: Vistka. Retrieved from: http://fes.kiev.ua/n/cms/fileadmin/upload2/Book_28-06-2022_web-3.pdf [in Ukrainian].

8. Verkhovna Rada of Ukraine. (1994). Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Zakon Ukrainy [On the Protection of Information in Information and Communication Systems: Law of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [in Ukrainian].

9. Verkhovna Rada of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky»: Ukaz Prezydenta Ukrainy №685/2021 [On the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 «On the Information Security Strategy»: Presidential Decree №685/2021]. Retrieved from: https://www.president.gov.ua/documents/6852021-41069 [in Ukrainian].

10. Verkhovna Rada of Ukraine. (2018). Zakon Ukrainy «Pro natsionalnu bezpeku Ukrainy» [Law of Ukraine «On National Security of Ukraine»]. Retrieved from: https://zakon.rada.gov.ua/laws/main/2469-19#Text [in Ukrainian].

11. Verkhovna Rada of Ukraine. (2020). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy [On the Decision of the National Security and Defense Council of Ukraine of September 14, 2020 «On the National Security Strategy of Ukraine»: Presidential Decree]. Retrieved from: https://zakon.rada.gov.ua/laws/show/392/2020#Text [in Ukrainian].

12. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy [On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

13. European Commission. (2022). Making critical entities more resilient. Retrieved from: https://eur-lex.europa.eu/EN/legal-content/summary/making-critical-entities-more-resilient.html

14. European Commission. (2024). Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures. Retrieved from: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

15. Council of the European Union. (2024). Council Recommendation on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371