

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»**

Кваліфікаційна наукова
праця на правах рукопису

КРАВЦОВ ОЛЕГ ВАЛЕНТИНОВИЧ

УДК 354:328.185:303

ДИСЕРТАЦІЯ

**ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ
МОДЕЛІ СТІЙКОСТІ У ФОРМАТІ ЦИФРОВОГО СУСПІЛЬСТВА**

25.00.01 – теорія та історія державного управління

Подається на здобуття наукового ступеня
доктора наук з державного управління

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

О.В. Кравцов

Дніпро – 2025

АНОТАЦІЯ

Кравцов О.В. Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства. – Рукопис.

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління. – Національний технічний університет «Дніпровська політехніка», Міністерство освіти і науки України, Дніпро, 2025.

Дисертаційне дослідження присвячено комплексному, теоретично й методологічно вивіреному обґрунтуванню формування національної моделі стійкості (НМС) України в умовах становлення цифрового суспільства, повномасштабної збройної агресії та глибинних трансформацій системи публічного управління. Дисертація одночасно виконує дві функції: з одного боку, репрезентує цілісну авторську концепцію НМС як нового наукового напрямку в теорії державного управління, а з іншого – пропонує детально опрацьований інструментарій її практичної реалізації в архітектурі сучасної цифрової держави.

У центрі дисертації – стійкість як ключова, системоутворююча категорія науки державного управління, яка синтезує безпековий, інституційний, соціальний, правовий та цифровий виміри функціонування держави. Послідовно доведено, що в умовах радикального зростання невизначеності, гібридизації загроз і тотальної цифровізації класичні парадигми державного управління, зорієнтовані на стабільність, ієрархічний контроль та лінійне планування, є концептуально й інструментально недостатніми. У цьому контексті НМС обґрунтовується як інтегральна рамка модернізації публічного управління, яка забезпечує життєстійкість держави, суспільства та територіальних громад в умовах тривалих криз, воєнних потрясінь і прискореної цифрової трансформації.

Актуальність теми обґрунтовано на основі якісно нової конфігурації у роботі загроз, з якими стикається українська держава. Поєднання воєнних,

політичних, економічних, безпекових, соціальних, інформаційних та кібернетичних викликів, масові переміщення населення, руйнування критичної та соціальної інфраструктури, жорсткі вимоги європейської та євроатлантичної інтеграції формують ситуацію, в якій питання не лише ефективності, а й самого існування та суб'єктності української державності безпосередньо залежить від здатності системи публічного управління до стійкого функціонування, адаптації й відновлення. Цифрова трансформація публічного управління, що реалізується через розвиток е-урядування, електронних послуг, інтегрованих інформаційних систем, платформ типу «Дія» та галузевих цифрових екосистем, з одного боку, створює потужні ресурси для прозорості, оперативності, сервісності публічної влади, а з іншого – породжує нові вразливості, пов'язані з кібератаками, дезінформацією, цифровою нерівністю, технологічною залежністю. У цих умовах постає науково й практично значуще завдання – створення такої НМС, яка інтегрувала б цифрові рішення, інституційну реформу та безпекову політику в цілісну, багаторівневу екосистему публічної влади, сумісну зі стандартами ЄС і НАТО, проте адаптовану до екстремальних умов повномасштабної війни.

Метою дисертації є розроблення і теоретико-методологічне обґрунтування національної моделі стійкості України у форматі цифрового суспільства як інтегрованої рамки модернізації публічного управління, здатної забезпечувати життєстійкість держави, суспільства й територіальних громад в умовах тривалих криз, гібридних загроз та прискореної цифровізації. Об'єктом дослідження виступає система публічного управління України в умовах воєнних, безпекових та цифрових трансформацій. Предметом дослідження є теоретико-методологічні засади, концепти, моделі та інструменти формування і реалізації національної моделі стійкості в контексті цифрового суспільства.

Теоретико-методологічну основу дисертації становить широкий спектр сучасних концепцій і теорій: системна теорія (державна як відкрита, складна

адаптивна система), неоінституціоналізм (формальні й неформальні правила та інституційна пам'ять як ресурс стійкості), мережеве та багаторівневе врядування (governance), концепції good governance та open government, теорія публічної цінності, теорії національної безпеки та resilience, підходи до дослідження цифрової держави й цифрового суспільства, теорії складних адаптивних систем та ризик-орієнтоване управління. Методологічний інструментарій включає діалектичний і системний аналіз – для розкриття НМС як цілісної екосистеми; структурно-функціональний та інституційний підходи – для виявлення функцій і ролі ключових суб'єктів стійкості; історичний метод – для простеження еволюції уявлень про стійкість держави; ризик-орієнтований і сценарний підходи – для моделювання можливих сценаріїв розвитку подій у воєнний і повоєнний періоди; мережевий підхід – для аналізу взаємодії держави, громадянського суспільства, бізнесу, міжнародних партнерів і цифрових платформ; компаративний аналіз – для вивчення зарубіжних практик ЄС, НАТО та окремих держав; методи моделювання, контент-аналізу, експертних оцінок, аналізу нормативно-правових актів і стратегічних документів – для конструювання прикладних моделей та інструментів реалізації НМС.

Логіка й структура дисертації підпорядковані послідовному розкриттю поставленої мети та досягненню заявлених наукових результатів. У першому розділі здійснено ґрунтовний теоретико-методологічний аналіз феномену стійкості в науці державного управління та суміжних галузях знань. Систематизовано підходи до тлумачення resilience у безпекознавстві, соціальній теорії, менеджменті, екології, інформаційній безпеці, виокремлює їх сильні й слабкі сторони, окреслює межі релевантності для українського контексту. На цій підставі формується авторська інтерпретація національної стійкості як інтегральної здатності системи публічного управління забезпечувати підтримання ідентичності, функціональну безперервність і здатність до адаптивної трансформації в умовах тривалих потрясінь. Водночас розроблена я й удосконалюється понятійно-категоріальний апарат

дослідження: уточнюється зміст категорій «національна стійкість», «суспільна стійкість», «цифрове суспільство», «цифрова держава», «цифрова резильєнтність», «цифрова інституційна спроможність публічної влади», «екосистема національної стійкості», до наукового обігу вводиться базове поняття «інституціоналізація цифрової політики у форматі НМС». У концептуальному плані це створює підґрунтя для подальшої побудови моделі НМС як самостійного напрямку в науці державного управління.

У другому розділі проаналізовано сучасний стан системи публічного управління України в умовах воєнних, безпекових та цифрових трансформацій. На основі аналізу нормативно-правових актів, стратегічних документів, емпіричних матеріалів та міжнародних рейтингів досліджуються ключові виклики і ризики функціонування інститутів влади в умовах воєнного стану та гібридної агресії. Особливу увагу приділено режимам надзвичайного та воєнного адміністрування, трансформації ролі центральних органів виконавчої влади, обласних військових адміністрацій, органів місцевого самоврядування. У розділі обґрунтовано той факт, що забезпечення стійкості в кризових режимах неможливе без переорієнтації традиційних моделей управління на проблемно-орієнтовані, адаптивні, здатні до швидкого прийняття рішень та інтеграції різнорівневої інформації. Також проводиться аналіз впливу цифрової трансформації на архітектуру публічної влади, виокремлюються основні групи цифрових загроз і вразливостей, пов'язаних із кібератаками, дезінформаційними кампаніями, фрагментацією цифрових систем, цифровою нерівністю.

У третьому розділі наведена теоретико-концептуальна конструкція національної моделі стійкості як національної екосистеми публічного управління. Показано, що НМС охоплює щонайменше п'ять взаємопов'язаних вимірів: онтологічний (існування держави як політичного суб'єкта в умовах екзистенційних загроз), функціональний (забезпечення безперервності виконання ключових публічних функцій і надання базових послуг), інституційний (адаптивність, узгодженість, навчальна спроможність

інститутів публічної влади), цифровий (захищеність, гнучкість та інтероперабельність цифрової інфраструктури, сервісів і даних) та соціально-комунікативний (довіра, участь, згуртованість, інформаційна стійкість суспільства). У межах цього розділу уперше комплексно представлено екосистему національної стійкості в умовах цифрового суспільства як окремий напрям досліджень у вітчизняній науці державного управління та розробляє модель National E-Resilience – національної цифрово орієнтованої моделі інтегрованого управління, спрямованої на забезпечення стійкості України шляхом розвитку національної цифрової інфраструктури, впровадження інструментів штучного інтелекту, хмарних сервісів, блокчейн-технологій, віртуальних платформ підтримки управлінських процесів. Тут же концептуалізується й рамкова модель Integrated Open Governance Framework, що поєднує принципи відкритості, участі, підзвітності та інтегрованості в єдину архітектуру стійкого врядування.

У четвертому розділі основний акцент зроблено на методології реалізації НМС та операціоналізації її цифрового виміру. На основі проблемного підходу розроблена методологічна концепція діяльності органів влади щодо реалізації НМС, в межах якої створено методологію Digital Resilience Assessment (DRA) – оцінювання цифрової стійкості органів публічної влади. Визначено групи індикаторів цифрової стійкості (структурні, процесуальні, результативні), критерії ефективності управління в умовах криз, окреслює можливості використання DRA для моніторингу, аудитів, стратегічного планування й оптимізації цифрових політик. У розділі обґрунтована концепція institutional SaaS platform – єдиної хмароорієнтованої платформи е-адміністрування, що забезпечує уніфікацію управлінських процесів і взаємодію органів влади на основі спільних стандартів даних і сервісів. Як відповідь на потребу нарощування спроможності інститутів у цифровому середовищі розроблено методику Adaptive Institutional Capacity Building (AICB), спрямовану на поетапне зміцнення цифрової інституційної спроможності органів публічної влади з урахуванням їхнього поточного

рівня розвитку, ресурсних можливостей і контексту функціонування.

У п'ятому розділі досліджено регіональний і муніципальний виміри НМС, а також механізми її практичної імплементації на рівні територіальних громад і регіонів. Проаналізовано вплив децентралізації, воєнного стану, переміщення населення, руйнування інфраструктури на стійкість територій, окреслює роль органів місцевого самоврядування як «першої лінії» національної стійкості. У цьому контексті розроблено концепцію смарт-резильєнтних регіональних стратегій (СРРС), які поєднують інструменти стратегічного планування, просторового розвитку, цифрового врядування та локальної безпекової політики в єдину рамку забезпечення стійкості громад і регіонів. Практична значущість запропонованих підходів підтверджена прикладами їх використання в діяльності центральних органів виконавчої влади, обласних військових адміністрацій, органів місцевого самоврядування, громадських організацій, що засвідчено відповідними документами про впровадження.

Таким чином, дисертаційна робота поєднує системне теоретико-методологічне осмислення стійкості як фундаментальної категорії науки державного управління та розроблення концептуально й інструментально завершеної національної моделі стійкості, орієнтованої на реальні потреби воєнного й повоєнного розвитку України в умовах цифрового суспільства.

Практичне значення одержаних результатів полягає в розробленні пропозицій і рекомендацій щодо вдосконалення нормативно-правового регулювання у сфері цифрової трансформації державного управління, формування національної політики цифрової стійкості, підвищення цифрових компетентностей державних службовців, упровадження стандартів прозорості, підзвітності та кібербезпеки. Розроблені в роботі концепції, моделі та методичні підходи можуть бути використані органами державної влади та місцевого самоврядування при підготовці стратегічних документів розвитку, формуванні та реалізації національних і регіональних стратегій

стійкості, адаптації міжнародного досвіду до українських реалій, а також у навчальному процесі закладів вищої освіти за спеціальностями галузі знань «Публічне управління та адміністрування».

Ключові слова: національна стійкість, цифрове суспільство, цифрова стійкість, цифрова держава, цифровізація, державне управління, теорія та історія, публічне управління, кібербезпека, цифрові платформи, електронне врядування.

Kravtsov O.V. Theoretical and Methodological Foundations of Formation and National Model of Resilience in the Digital Society Format. – Qualification scientific work. – Manuscript.

Dissertation for obtaining the scientific degree of Doctor of Sciences in public administration, speciality 25.00.01 – Theory and History of Public Administration, Dnipro University of Technology, Ministry of Education and Science of Ukraine, Dnipro, 2025.

The dissertation research is devoted to a comprehensive, theoretically and methodologically substantiated justification for the development of Ukraine's National Resilience Model (NRM) under the conditions of digital society formation, full-scale armed aggression, and profound transformations of the public administration system. The dissertation simultaneously performs two key functions: on the one hand, it offers a holistic authorial concept of the NRM as an innovative research direction in the theory of public administration; on the other hand, it provides a thoroughly elaborated toolkit for its practical implementation within the architecture of the modern digital state.

At the core of the dissertation lies the concept of resilience, recognized as a key, system-forming category within public administration science. This notion synthesizes security, institutional, social, legal, and digital dimensions of state functioning. The work consistently demonstrates that, under conditions of radical uncertainty, hybrid threats, and pervasive digitalization, classical paradigms of public administration—focused on stability, hierarchical control, and linear

planning—are both conceptually and instrumentally inadequate. In this context, the NRM is substantiated as an integral framework for the modernization of public administration, which ensures the viability of the state, society, and local communities amidst protracted crises, military shocks, and accelerated digital transformation.

The relevance of the research topic is justified by the emergence of a qualitatively new configuration of threats facing the Ukrainian state. These include the simultaneous impact of military, political, economic, security, social, informational, and cyber challenges, mass population displacement, destruction of critical and social infrastructure, as well as the increased demands of European and Euro-Atlantic integration. All these circumstances have created a situation in which not only the effectiveness, but also the very existence and subjectivity of Ukrainian statehood directly depend on the capacity of the public administration system for resilient functioning, adaptation, and recovery. The digital transformation of public administration, realized through the development of e-governance, electronic services, integrated information systems, platforms like “Diia”, and sectoral digital ecosystems, generates—on the one hand—powerful capabilities for transparency, operationality, and client-oriented public authorities, and—on the other hand—new vulnerabilities associated with cyberattacks, disinformation, digital inequality, and technological dependence. In such circumstances, there emerges both a scientifically and practically significant task: the development of an NRM that integrates digital solutions, institutional reform, and security policy into a holistic, multi-level ecosystem of public authority, compatible with EU and NATO standards while adapted to the extreme conditions of full-scale war.

The purpose of the dissertation is to elaborate and provide a theoretical and methodological substantiation of a National Resilience Model of Ukraine in the format of the digital society, as an integrated framework for modernizing public administration. This model aims to ensure the survivability of the state, society, and territorial communities under long-term crises, hybrid threats, and accelerated

digitalization. The object of research is the system of Ukrainian public administration in conditions of war, security, and digital transformation. The subject of the study includes the theoretical and methodological foundations, concepts, models, and tools for building and realizing the national resilience model in the context of digital society.

The theoretical and methodological foundation of the dissertation encompasses a broad spectrum of modern concepts and theories: systems theory (the state as an open, complex adaptive system), neo-institutionalism (formal and informal rules and institutional memory as resources for resilience), network and multi-level governance, good governance and open government concepts, public value theory, security studies, the theory of resilience, approaches for exploring the digital state and digital society, theories of complex adaptive systems, and risk-oriented management. The methodological toolkit comprises: dialectical and systems analysis—for revealing NRM as a holistic ecosystem; structural-functional and institutional approaches—for identifying the functions and roles of key resilience actors; historical method—for tracing the evolution of resilience conceptualizations in state theory; risk-based and scenario approaches—for modeling potential developments in wartime and post-war settings; network approach—for analyzing interactions between the state, civil society, business, international partners, and digital platforms; comparative analysis—for studying best practices from the EU, NATO, and specific countries; as well as modeling methods, content analysis, expert assessments, and analysis of legal acts and strategic documents—for constructing applied models and tools for NRM implementation.

The logic and structure of the dissertation are subordinated to the consistent disclosure of the stated purpose and the achievement of declared scientific results.

Chapter One: This chapter provides an in-depth theoretical and methodological analysis of the resilience phenomenon in public administration science and cognate fields. The dissertation author systematizes approaches to interpreting “resilience” in security studies, social theory, management, ecology,

and information security, outlines their strengths and weaknesses, and delineates their relevance to the Ukrainian context. On this basis, the author's interpretation of national resilience is formulated as the integral capacity of the public administration system to maintain identity, functional continuity, and the ability to adaptively transform under conditions of protracted shocks. Simultaneously, the study refines and develops the conceptual and categorical apparatus: the meanings of "national resilience", "societal resilience", "digital society", "digital state", "digital resilience", "digital institutional capacity of public authority", and "national resilience ecosystem" are clarified. The study introduces the fundamental concept of "institutionalization of digital policy in the NRM format". Conceptually, this lays the groundwork for further construction of the NRM as an independent direction in public administration science.

Chapter Two: This chapter analyzes the current state of Ukraine's public administration system under conditions of war, security, and digital transformations. Drawing on the analysis of legal acts, strategic documents, empirical materials, and international ratings, the dissertation investigates the key challenges and risks faced by government institutions under martial law and hybrid aggression. Special attention is devoted to extraordinary and wartime administrative regimes, the transformation of the roles of central executive authorities, regional military administrations, and local self-government bodies. It is substantiated that ensuring resilience in crisis regimes is impossible without shifting from traditional management models to problem-oriented, adaptive models capable of rapid decision-making and multi-level information integration. The chapter also analyzes the impact of digital transformation on the architecture of public authority, distinguishing key digital threats and vulnerabilities associated with cyberattacks, disinformation campaigns, the fragmentation of digital systems, and digital inequality.

Chapter Three: This chapter presents the theoretical and conceptual construct of the National Resilience Model as a national ecosystem of public administration. It is demonstrated that the NRM encompasses at least five

interrelated dimensions: ontological (the survival of the state as a political actor amidst existential threats), functional (ensuring continuity in performing key public functions and providing basic services), institutional (adaptability, consistency, and learning capacity of public institutions), digital (security, flexibility, and interoperability of digital infrastructure, services, and data), and socio-communicative (trust, participation, cohesion, and information resilience of society). For the first time in Ukrainian public administration research, the dissertation provides a comprehensive presentation of the resilience ecosystem within the digital society and develops the “National E-Resilience” model—a digitally oriented, integrated governance model for Ukraine’s resilience, leveraging the development of national digital infrastructure, artificial intelligence tools, cloud services, blockchain technologies, and virtual platforms supporting governance processes. The “Integrated Open Governance Framework”, combining openness, participation, accountability, and integration principles into a single architecture of resilient governance, is also conceptualized here.

Chapter Four: The main emphasis here is placed on the methodology for NRM implementation and the operationalization of its digital dimension. Based on a problem-oriented approach, the author develops a methodological concept for public authority activities aimed at NRM implementation. Within this framework, the “Digital Resilience Assessment (DRA)” methodology is devised, enabling the assessment of the digital resilience of public authorities. The chapter identifies groups of digital resilience indicators (structural, process, performance), criteria for crisis management effectiveness, and explores opportunities for using DRA in monitoring, audits, strategic planning, and the optimization of digital policies. The chapter substantiates the concept of an “institutional SaaS platform”—a unified, cloud-based e-administration platform that standardizes management processes and public authority interactions based on shared data and service standards. To address the need for institutional capacity building in the digital environment, the methodology of Adaptive Institutional Capacity Building (AICB) is developed, focusing on incremental strengthening of public authorities’ digital institutional

capacities, considering current development levels, resource endowments, and operational contexts.

Chapter Five: This chapter investigates the regional and municipal dimensions of NRM, as well as mechanisms for its practical implementation at the level of territorial communities and regions. The study analyzes the effects of decentralization, martial law, population displacement, and infrastructure destruction on territorial resilience, delineating the role of local self-government bodies as the “first line” of national resilience. In this context, the concept of “smart resilient regional strategies (SRRS)” is developed, combining tools of strategic planning, spatial development, digital governance, and local security policies into an integrated framework for community and regional resilience. The practical significance of the proposed approaches is confirmed by examples of their application in the activities of central executive authorities, regional military administrations, local self-government bodies, and public organizations, as corroborated by official implementation documentation.

Thus, the dissertation combines a systematic theoretical and methodological examination of resilience as a foundational category in public administration science with the development of a conceptually and instrumentally complete national resilience model, tailored to the real needs of Ukraine’s wartime and post-war development within a digital society.

The practical significance of the research results lies in the development of proposals and recommendations for improving the regulatory framework in the sphere of digital transformation of public administration, shaping a national digital resilience policy, enhancing the digital competencies of civil servants, introducing standards of transparency, accountability, and cybersecurity. The concepts, models, and methodological approaches developed in the dissertation can be used by public authorities and local self-government bodies in preparing strategic development documents, forming and implementing national and regional resilience strategies, adapting international experience to the Ukrainian context, as well as in the educational process of higher education institutions in the field of “Public

Administration and Management”.

Keywords: national resilience, digital society, digital resilience, digital state, digitalization, public administration, theory and history, public governance, cybersecurity, digital platforms, e-governance.

.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

Монографії

1. Гуманізація публічної служби в Україні: науково-практичні засади. монографія. Дніпро : ДРІДУ НАДУ, 2015. 253 с. URL:https://palsg.nmu.org.ua/ua/Sci/Monograph/Гуманізація_публічної_служби.pdf.

Особистий внесок: обґрунтовано напрями застосування інформаційних технологій у навчанні публічних службовців у контексті гуманізації освітнього простору (поширення гіпертекстових і гіпермедіальних систем).

2. **Кравцов О.В.**, Кравцова Т. В. Удосконалення інформаційного забезпечення органів публічної влади на місцевому рівні. Східна політика Європейського Союзу : здобутки, виклики та перспективи / Wschodnia polityka Unii Europejskiej: osiagniecia, wyzwania i perspektywy : **монографія** ; за наук. ред. Я. Турчин, Т. Астрамович-Лейк, О. Горбача. Львів-Olsztyn : РОМУС-ПОЛІГРАФ, 2021. 220 с. (С. 185-198). URL: <https://lpnu.ua/sites/default/files/2021/pages/14947/forum-monografiya-maket.pdf>.

Особистий внесок: розроблено на основі практико-орієнтованих методик сучасного інформаційного забезпечення діяльності органів влади в умовах цифровізації.

3. Маматова Т.В., **Кравцов О.В.** Забезпечення якості публічних послуг в умовах цифрової трансформації (Section 10. Ensuring the administrative services quality in the context of digital transformation). Development vectors in public management and administration: **collective monograph**. Riga, Latvia : Publishing House «Baltija Publishing», 2021. 338 p. P. 208–228. URL: <http://baltijapublishing.lv/omp/index.php/bp/catalog/book/137/> DOI: <https://doi.org/10.30525/978-9934-26-082-7-10>.

Особистий внесок: розроблено методологію адаптивної моделі формування критеріїв оцінювання якості публічних послуг, уточнено критерії рамкової цифровізації.

4. Kravtsov O.V. Development of digital competencies of digital competencies in management desigion-making in public administration. *Modernization of Public Authorities in the Digital State Format: Challenges and Prospects under Martial Law and Postwar Reconstruction: scientific monograph*. Riga, Latvia : “Baltija Publishing”, 2025. P. 244-260. URL: <http://baltijapublishing.lv/omp/index.php/bp/catalog/download/611/16417/34706-1?inline=1/>. DOI <https://doi.org/10.30525/978-9934-26-51-6-12>.

статті, опубліковані щонайменше у двох різних періодичних виданнях, включених до категорії «А» Переліку наукових фахових видань України, або у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus

5. Маматова Т., Chykarenko I., Chykarenko O., Kravtsova T., **Kravtsov O.** Information Systems in Project Management of The Public Sphere. IJCSNS International Journal of Computer Science and Network Security. 2021. Vol. 21. № 8. P. 141–148. URL: http://paper.ijcsns.org/07_book/202108/20210819.pdf/ doi: <https://doi.org/10.22937/IJCSNS.2021.21.8.19>. (**Web of Science**).

Особистий внесок: охарактеризовано сучасні підходи до формування інформаційних системи публічного менеджменту в умовах цифрового суспільства, розвинуто поняття управління в цифрову еру.

6. **Kravtsov O.**, Kravtsova T., Lashenko O., Lola V., Rudik N., Holokha L (2023). Strategic Security Imperatives in the Development of Communities in the Post-War Period in Ukraine. Review of Economics and Finance. 2023. Vol. 21, P. 723-730. URL: <https://refpress.org/ref-vol21-a77//>. doi: <https://doi.org/10.55365/1923.x2023.21.77>. (**Scopus**).

Особистий внесок: уточнено сучасні методологічні підходи до цифровізації державного управління в умовах війни та повоєнного відновлення.

7. Verkhovod, I., Haponenko, V., **Kravtsov, O.**, Kravtsova, T., & Bulbeniuk, S. (2024). La influencia de las tecnologías de la información y la

comunicación en el desarrollo de las estructuras sociales y políticas de la sociedad red. *Interacción Y Perspectiva*, 14(2), 386-398. [URL: https://dialnet.unirioja.es/servlet/articulo?codigo=9736909](https://dialnet.unirioja.es/servlet/articulo?codigo=9736909). doi: <https://doi.org/10.5281/zenodo.10909782>. (**Web of Science**).

Особистий внесок: запропоновано нові підходи запровадження цифрового інструментарію визначення стану стійкості систем управління, обґрунтовано особливості формування спеціальних інструментів цифрового урядування.

8. Sydorchuk, O., Bashtannyk, V., Terkhanov, F., **Kravtsov, O.**, Akimova, L., & Akimov, O. (2024). Integrating digitization into public administration: Impact on national security and the economy through spatial planning. *Edelweiss Applied Science and Technology*, 8(5), 747–759. URL: <https://learning-gate.com/index.php/2576-8484/article/view/1740>. doi: <https://doi.org/10.55214/25768484.v8i5.1740> (**Scopus**).

Особистий внесок: запропоновано авторські підходи до впровадження диджиталізації публічного управління у межах безпекового концепту національної моделі стійкості.

9. Mamatova T., Chykarenko I., Chykarenko, O., Kravtsova T., **Kravtsov O.** (2022). Innovative digital technologies in the pr-management specialists training for public administration bodies on the blended learning. *Revista Eduweb*. 16(3), 160–176. URL: <https://revistaeduweb.org/check/16-3/12-160-176.pdf/> doi: <https://doi.org/10.46502/issn.1856-7576/2022.16.03.12>. (**Web of Science**).

Особистий внесок: розроблено авторську методику запровадження цифрових технологій в системі навчання публічних службовців, запропоновано удосконалені алгоритми асинхронного навчання в системі вищої освіти.

10. Bashtannyk, O., Bykov, I., **Kravtsov, O.**, Bashtannyk, V., Baikevych, R., & Pushkar, O. (2025). Evolution of economic security institutions: integrating international standards for strategic risk management in global contexts. *Sapienza: International Journal of Interdisciplinary Studies*, 6(2), e25035, P. 1-11. e-ISSN:

2675-9780.

URL:

<https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/e25035>.

doi:

<https://doi.org/10.51798/sijis.v6i2.1072> (Scopus)

Особистий внесок: розроблено авторську методологію розвитку цифрових технологій для спеціальної підготовки фахівців у сфері публічного управління.

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

11. **Кравцов О.В.** Напрями удосконалення підготовки державних службовців в умовах інформаційного суспільства. *Аналітика і влада* : журнал експерт.-аналіт. матеріалів і наук. пр. ПДМУС НАДУ. 2013. № 8. С.219-229.

12. **Кравцов О.В.** Краудсорсинг в системі державного управління. *Державне управління та місцеве самоврядування*. 2014. № 4. С. 15-23.

13. **Кравцов О.В.,** Кандзюба С.П., Титаренко О.М. Методика формування простору електронної взаємодії у межах об'єднаної територіальної громади. *Аспекти публічного управління*. 2015. № 5-6. С. 76-

84. URL: <https://aspects.org.ua/index.php/journal/article/view/169>. doi: <https://doi.org/10.15421/151551>.

Особистий внесок: розроблено державноуправлінські підходи щодо формування сучасного механізму електронної взаємодії на рівні органів місцевого самоврядування.

14. **Кравцов О.В.** Формування інформаційно-комунікативної компетентності публічних службовців в умовах розвитку електронного урядування: загальні підходи. *Публічне адміністрування: теорія та практика*. 2016. Вип. 1. (електронне видання). URL: http://nbuv.gov.ua/UJRN/Patp_2016_1_10.

15. **Кравцов О.В.,** Губа М.І., Андросович А.В. Роль цифрових технологій у покращенні доступності та якості публічних послуг в Україні.

Державне управління: удосконалення та розвиток. 2024. № 9. (електронне видання) URL: <https://www.nayka.com.ua/index.php/dy/article/view/4612/> DOI: <http://doi.org/10.32702/2307-2156.2024.9.13>.

Особистий внесок: розроблено методологію дослідження особливих технологічних засобів та інструментів надання публічних послуг.

16. **Кравцов О.В.** Баштанник В.В. Інституціональні механізми забезпечення участі громади в муніципальному управлінні. *Публічне управління та адміністрування в Україні*. 2023. № 35. С.201-210. URL: <https://pag-journal.iei.od.ua/archives/2023/35-2023/38.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2023.35.38>.

Особистий внесок: узагальнені спеціальні механізми забезпечення участі громади в муніципальному управлінні у форматі цифрового суспільства на основі концепту національної стійкості.

17. **Кравцов О.В.,** Баштанник В.В., Порівняльний аналіз сучасних моделей участі громади в муніципальному управлінні країн ЄС та України у контексті сучасних трендів адміністрування. *Публічне управління та адміністрування в Україні*. 2023. № 37. С.202-214. URL: <https://pag-journal.iei.od.ua/archives/2023/37-2023/37.pdf> doi: <https://doi.org/10.32782/pma2663-5240-2023.37.37>.

Особистий внесок: детерміновані основні виклики для системи національної стійкості, на основі аналізу зарубіжного досвіду та особливостей його впровадження в умовах проведення реформи децентралізації.

18. **Кравцов О.** Кравцова Т.В., Лащенко О.В. Теоретичні основи впровадження антикризового менеджменту в діяльність органів публічного управління. *Аспекти публічного управління*. 2021. № 9. 64-72. URL: <https://aspects.org.ua/index.php/journal/article/view/878/> doi: <https://doi.org/10.15421/152129>.

Особистий внесок: розроблено методологію впровадження антикризового управління в діяльності органів публічного управління для забезпечення національної стійкості із застосуванням системного підходу.

19. **Кравцов О.В.**, Кравцова Т.В., Лащенко О.В. Державна політика в сфері вищої освіти України в умовах цифровізації. *Вісник національного університету цивільного захисту України: серія «Державне управління»*. 2021. Випуск 1(14). С. 73–85. URL: https://www.researchgate.net/publication/352922841_Derzavna_politika_v_sferi_v_isoi_osviti_Ukraini_v_umovah_cifrovizacii. doi: <https://doi.org/10.52363/2414-5866-2021-1-10>.

Особистий внесок: детерміновано особливості формування та реалізації державної політики в сфері вищої освіти України в умовах цифровізації, визначено освітні компоненти процесу формування цифрового суспільства.

20. Кравцова Т.В., Лащенко О.В., **Кравцов О.В.** Використання маркетингового підходу в діяльності органів публічного управління медичною сферою. *Аспекти публічного управління*. 2021. Т. 9. № 4. С. 72–84. URL: <https://aspects.org.ua/index.php/journal/article/view/890>. doi: <https://doi.org/10.15421/152139>.

Особистий внесок: систематизовано сучасні адміністративні підходи щодо використання маркетингового підходу в діяльності органів публічного управління медичною сферою на основі застосування цифрових технологій.

21. **Кравцов О.В.** Роль соціально-ментальних чинників становлення національної ментальної стійкості в умовах цифрового суспільства. *Публічне управління та адміністрування в Україні*. 2023. Випуск 34. С. 212-218. URL: <https://pag-journal.iei.od.ua/archives/2023/34-2023/39.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2023.34.39>.

22. **Кравцов О.В.** Інституціональний зміст сучасного механізму національної стійкості. *Публічне управління та адміністрування в Україні*. 2023. Випуск 38. С. 293-299. URL: <https://pag->

journal.iei.od.ua/archives/2023/38-2023/52.pdf. doi: <https://doi.org/10.32782/pma2663-5240-2023.38.52>.

23. **Кравцов О.В.** Концептуалізація моделі державотворчих процесів в Україні на основі проблемного підходу: феномен цифрової резильєнтності державних структур. *Держава і регіони*. 2023. № 1. URL: http://pa.stateandregions.zp.ua/archive/1_2023/1_2023.pdf. doi: http://pa.stateandregions.zp.ua/archive/1_2023/1_2023.pdf

24. **Кравцов О.В.** Формування особливих механізмів національного розвитку на основі цифровізації в умовах правового режиму воєнного стану. *Публічне управління та місцеве самоврядування*. 2024. Випуск 3. С. 26-33. URL: <https://journals.politehnica.dp.ua/index.php/public/article/view/666>. doi: <https://doi.org/10.32782/2414-4436/2024-3-4>.

25. **Кравцов О.В.** Роль державного управління в розбудові національної моделі стійкості в цифровому суспільстві. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. №4. С. 7-12. URL: <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/631>. doi: <https://doi.org/10.51547/ppp.dp.ua/2024.4.1>.

26. **Кравцов О.В.** Децентралізація і локалізація в контексті формування цифрової моделі стійкості. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. №5. С. 71-78. URL: <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/659>. doi: <https://doi.org/10.51547/ppp.dp.ua/2024>.

27. Прокопчук І., Воронкова А., **Кравцов О.** Дослідження впровадження інноваційних цифрових технологій в державному управлінні. *Успіхи і досягнення у науці*. Серія «управління та адміністрування». 2024. № 10. С. 714-728. URL: <http://perspectives.pp.ua/index.php/sas/article/view/18067>. doi: [https://doi.org/10.52058/3041-1254-2024-10\(10\)-714-728](https://doi.org/10.52058/3041-1254-2024-10(10)-714-728).

Особистий внесок: проаналізовано динаміку індексу запровадження електронного врядування в діяльності органів влади, досліджено критерії

оцінки ефективності впровадження цифрових технологій в управлінському середовищі.

28. **Кравцов О.В.** Упровадження моделі «раціональної інформаційної стабільності» як основи формування національної ментальної системи (НМС) 3.0. *Публічне управління та адміністрування в Україні*. 2024. № 39. С.278-285. URL:<https://pag-journal.iei.od.ua/archives/2024/39-2024/54.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2024.39.52>.

29. Ковальов В., **Кравцов О.** Діджиталізація публічних послуг для внутрішньо переміщених осіб: огляд, виклики, перспективи. *Публічне управління і адміністрування в Україні*. 2025. №46. С. 156-161. URL: <https://pag-journal.iei.od.ua/archives/2025/46-2025/29.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2025.46.27>.

Особистий внесок: розроблено авторську методологію надання публічних послуг у цифровому форматі, запропоновано авторський підхід до класифікації наявних електронних послуг, а також наведено алгоритми удосконалення механізмів надання послуг внутрішньо переміщеним особам.

30. Філатов В., **Кравцов О.** Публічна діджиталізація та Е-демократія: сучасні інструменти, проблеми і моделі регулювання. *Вчені записки Таврійського національного університету ім. В.Вернадського. Серія «Публічне управління та адміністрування»*. 2024. Т.35 (74). № 6. С.219-225. URL:

https://www.pubadm.vernadskyjournals.in.ua/journals/2024/6_2024/6_2024.pdf. doi: <https://doi.org/10.32782/TNU-2663-6468/2024.6/37>.

Особистий внесок: обґрунтовано феномен публічної діджиталізації в суспільних відносинах, охарактеризовано механізми публічного управління в контексті феномену Е-демократії.

Праці, які додатково відображають наукові результати дисертації (апробація матеріалів дисертації на наукових конференціях) за науковою спеціальністю 25.00.01 – теорія та історія державного управління

31. **Кравцов О.В.** Удосконалення інформаційного наповнення сайтів

ОТГ. *Новітні інформаційно-комунікаційні технології в модернізації публічного управління: зарубіжний і вітчизняний досвід* : матеріали VII наук.-практ. семінару, 25 липня 2019 р., м. Дніпро. Дніпро: ДРІДУ НАДУ. 2019. URL: https://dridu.dp.ua/konf/konf_dridu/Seminar%20ITIC%2007.2019.pdf.

32. **Кравцов О.В.** Актуальні проблеми розвитку штучного інтелекту в Україні. *Сталий розвиток територій: проблеми та шляхи вирішення* : матеріали X міжнар. наук.-практ. конф., м. Дніпро. 25 жовт. 2019 р., Дніпро : ДРІДУ НАДУ. 2019. С. 305–308. URL: http://dridu.dp.ua/konf/konf_dridu/2019_10_25_material_erep.pdf.

33. **Кравцов О.В.** Напрями удосконалення підготовки публічних службовців з питань інформаційної безпеки. *Інноваційний розвиток і підвищення рівня спроможності об'єднаних територіальних громад*: матеріали наук.-практ. конф. за міжнар. участю. м. Дніпро. 30 жовтня – 29 листопада 2019 р. Дніпро: ДРІДУ НАДУ. 2019. С. 354-356. URL: http://www.dridu.dp.ua/konf/konf_dridu/2019_11_29_materialy_mup.pdf.

34. **Кравцов О.В.** Соціальні ефекти інформаційної безпеки. *Проблеми управління соціальним і гуманітарним розвитком*: матеріали XIV наук.-практ. конф. за міжнар. участю. Дніпро : ДРІДУ НАДУ, 2020. С. 166-170. URL: http://dridu.dp.ua/konf/konf_dridu/2020_Material_Social_develop.pdf.

35. **Кравцов О.В., Кравцова Т.В., Маматова Т.В.** Формування цифрових компетентностей публічних службовців. *Науково-практичне забезпечення надання публічних послуг в умовах децентралізації*: матеріали науково-практичної інтернет-конференції за міжнародної участі, м. Київ, 20 квітня 2021 р., Інститут підготовки кадрів Державної служби зайнятості України. Київ: ІПК ДСЗУ, 2021 С. 125–130. URL: https://ipk.edu.ua/wp-content/uploads/2021/09/Konf21_04_2021.pdf.

36. **Кравцов О.В., Кравцова Т.В., Лащенко О.В.** Цифровізація вищої освіти України в умовах пандемії. *Актуальні проблеми європейської інтеграції та євроатлантичного співробітництва України*: матеріали XVIII регіон. наук.-практ. конф., м. Дніпро. 13 трав. 2021 р. Дніпро : ДРІДУ НАДУ,

2021. С. 117-120. URL: http://www.dridu.dp.ua/konf/konf_dridu/2021_05_13_pei_material.pdf.

37. Кравцова Т.В., **Кравцов О.В.**, Лашенко О.В. Сутність та зміст державної політики і управління в галузі освіти. *Формування дієвих механізмів державного управління з забезпечення державної безпеки: круглий стіл за міжнар. участю*, м. Харків, 14 трав. 2021 р. Харків: Нац. ун-т цивільного захисту України, 2021. С. 45–47. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/12968/3/ZBNMKS2021.pdf>.

38. **Кравцов О.В.**, Кравцова Т.В. Розвиток цифрових навичок: досягнення та перспективи. *Східна політика Європейського Союзу: здобутки, виклики та перспективи / Wschodnia Polityka Unii Europejskiej: osiagniecia, wyzwania i perspektywy: Materiały VI Polsko-Ukraińskiego Forum Naukowego* (27-28 maja 2021, Lwów). Львів-Olsztyn: «ROMUS-POLIGRAF», 2021. 256 s. URL: https://palsg.nmu.org.ua/ua/Sci/Publ_postgrad/Drobakhina-2021.pdf.

39. **Кравцов О.В.**, Кравцова Т.В. Цифровізація медицини – запорука ефективного здоров'язбереження. *Трансформація системи публічного управління створенням здоров'язбережувального та безпечного простору України (модернізація, інновації, розвиток): II Міжнародна науково-практична конференція*, м. Переяслав, 11 червня 2021 року. Переяслав : Університет Григорія Сковороди, 2021. 245 с. С. 141-148. URL: <https://uhsp.edu.ua/event/ii-mizhnarodna-naukovo-praktychna-konferenciya>.

40. Кравцова Т.В., **Кравцов О.В.**, Кіреєва О.Б. Інформаційне забезпечення органів місцевого самоврядування в сфері надання адміністративних послуг: проблеми та пріоритетні напрями вдосконалення. *Modern scientific research: achievements, innovations and development prospects. Abstracts of the I International scientific and practical conference*, July 4-6, 2021, Berlin, Germany. MDPC Publishing. Berlin, Germany. 2021. Pp. 217-223. URL:

<https://sci-conf.com.ua/wp-content/uploads/2021/07/MODERN-SCIENTIFIC-RESEARCH-ACHIEVEMENTS-INNOVATIONS...-4-6.07.21.pdf>.

41. Кравцова Т.В., **Кравцов О.В.** Комплекс пріоритетів здоров'язбереження територіальної громади у поствоєнний період. *Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні* : матеріали Всеукр. наук.-практ. конф. м. Київ, ДЗВО «Університет менеджменту освіти» НАПН України, 15-28 квітня 2022 р. Київ : ДЗВО «УМО» НАПН України, 2022. С. 146–150. URL: https://palsg.nmu.org.ua/ua/Sci/konf/Збірник_тез_Том_I.pdf

42. Кравцова Т.В., Лащенко О.В., **Кравцов О.В.** Муніципальний маркетинг як інструмент забезпечення ревіталізації та розвитку територіальних громад. *Міжнародні економічні відносини. Сталий розвиток України в умовах глобалізації та європейської економічної інтеграції: проблеми, перспективи, ефективність*. Фенікс-2022»: матеріали міжнародної науково-практичної конференції, м. Харків, 31 травня 2022 р. Харків. С. 144–146. URL: https://palsg.nmu.org.ua/ua/Sci/konf/Збірник_тез_ФЕНІКС-2022.pdf

43. **Кравцов О.В.** Цифрова трансформація публічного управління в Україні. *Актуальні проблеми європейської та євроатлантичної інтеграції України* : матеріали XIX-ї регіон. наук.-практ. конф. 16 червня 2022 р., Дніпро / за заг. ред. Л.Л. Прокопенка. Д : НТУ ДП, 2022. С. 112–115. URL: https://palsg.nmu.org.ua/ua/Sci/konf/Material_conference_16_06_2022.pdf.

44. **Кравцов О.В.** Цифровізація територіальних громад в Україні. *Digital transformation and technologies for sustainable development all branches of modern education, science and practice*. International Scientific and Practical Conference Proceeding, January 26, 2023. International Academy Applied Sciences in Lomza (Poland) - State Biotechnological University (Ukraine). Publishing house: MANS w Łomży, Lomza, Poland, 2023. Part 2. С. 154-157. URL:

https://www.researchgate.net/publication/373070515_Digital_transformation_and_technologies_for_sustainable_development_all_branches_of_modern_education_s

[cience_and_practice_Electronic_resource_International_Scientific_and_Practical_Conference.](#)

45. **Кравцов О.В.** Дезінформація, маніпуляція та фейки як загрози інформаційної безпеки органів публічного управління в умовах європейської інтеграції. *Національна безпека: загрози та виклики*: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 квітня – 12 травня 2024 року. Львів – Торунь : Liha-Pres, 2024. С. 98-101. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/22907/1/%D0%90dvanced_training_UzhNU.pdf.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	29
ВСТУП	31
РОЗДІЛ 1	
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬНИХ ВІДНОСИН	46
1.1. Концептуальні засади становлення сучасних моделей функціонування системи публічного управління як суспільного феномену	46
1.2. Формування національної моделі державотворчих процесів в Україні на основі проблемного підходу: стійкість як багатовимірний феномен	86
1.3. Сутність та особливості формування системи публічного управління в умовах цифровізації: соціальний вимір цифрового суспільства	123
1.4. Формування механізмів національного розвитку у межах НМС шляхом інтеграції цифрових технологій у систему державного управління	140
Висновки до розділу 1	166
РОЗДІЛ 2	
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ МОДЕЛІ СТІЙКОСТІ В УМОВАХ ЦИФРОВОГО СУСПІЛЬСТВА	168
2.1. Національна модель стійкості: визначення, особливості та основні складники	169
2.2. Принципи формування національної моделі стійкості у форматі цифрового суспільства	187
2.3. Формування методології національного розвитку на основі	

цифровізації в умовах правового режиму воєнного стану: актуалізація НМС	223
2.4. Особливості застосування функціонального підходу у дослідженні механізмів національної стійкості в умовах цифрового суспільства	252
Висновки до розділу 2	280
РОЗДІЛ 3 ЦИФРОВІ УПРАВЛІНСЬКІ ПЛАТФОРМИ ТА РОЗВИТОК ДЕРЖАВНИХ І СУСПІЛЬНИХ ІНІЦІАТИВ В УКРАЇНІ: ВПЛИВ НА СОЦІАЛЬНУ СТАБІЛЬНІСТЬ І БЕЗПЕКУ УПРАВЛІНСЬКИХ СИСТЕМ	284
3.1. Цифрові управлінські платформи у форматі НМС: теоретичний аналіз	284
3.2. Integrated Open Governance як нова концепція публічного управління в цифрову епоху	300
3.3. Цифрові управлінські платформи як фактор зміцнення соціальної стабільності та безпеки функціонування управлінських систем	316
3.4. Запровадження алгоритму оцінки цифрової стійкості (Digital Resilience Assessment, DRA) у межах теоретичної концепції National E-Resilience	333
Висновки до розділу 3	354
РОЗДІЛ 4 ХАРАКТЕРИСТИКА МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ МОДЕЛІ СТІЙКОСТІ В УМОВАХ ЦИФРОВОГО СУСПІЛЬСТВА	357
4.1 Теоретико-методологічні засади системного проєктування механізмів забезпечення національної моделі стійкості в умовах цифрової трансформації	357
4.2. Алгоритм динамічного моніторингу функціонування національної моделі стійкості та його інтеграція у межах Digital Resilience	

Assessment (DRA)	380
4.3. Модель «смарт-резильєнтних регіональних стратегій» як інноваційний інструмент просторової диференціації національної моделі стійкості	397
4.4. Компаративно-адаптаційні механізми розвитку НМС та формат «раціональної цифрової стабільності» в умовах гібридних загроз	419
4.5. Модель «раціональної інформаційної стабільності» як інтегральний механізм забезпечення НМС 3.0	456
Висновки до розділу 4	474
РОЗДІЛ 5	
ЦИФРОВА РЕЗИЛЬЄНТНІСТЬ ДЕРЖАВИ Й СУСПІЛЬСТВА: КОНЦЕПЦІЇ, УПРАВЛІНСЬКІ СТАНДАРТИ ТА ІНСТИТУЦІЙНІ МОДЕЛІ	477
5.1. Концептуалізація НМС в умовах війни та цифрової трансформації	477
5.2. Integrated Open Governance Framework як нова концепція державного управління в цифрову епоху	496
5.3. Класифікація цифрових управлінських стандартів як нормативно-алгоритмічного формату НМС	515
5.4. Інституціональні механізми реалізації НМС	532
Висновки до розділу 5	557
ВИСНОВКИ	561
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	572
ДОДАТКИ	616

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

- AICB – Adaptive Institutional Capacity Building / адаптивна цифрова інституціональна спроможність
- AI – Artificial Intelligence / штучний інтелект
- Big Data – великі дані, аналітика великих даних
- DSS – Decision Support Systems
- DSS – Decision Support Systems / системи підтримки прийняття рішень
- DGT – Digital Government Transformation / цифрова трансформація
- DIC – Digital Inclusion Criteria / критерії цифрової інклюзії
- DRA – Digital Resilience Assessment / методологія оцінки цифрової стійкості
- CPPC – смарт-резильєнтні регіональні стратегії
- IOG – Integrated Open Government / інтегроване відкрите управління (державне)
- Integrated Open Governance Framework – рамкова модель інтегрованого відкритого врядування
- Institutional SaaS platform – хмароорієнтована платформа е-адміністрування
- GIS – геоінформаційна система
- ICT – Information and Communication Technologies / інформаційно-комунікаційні технології
- ML – Machine Learning (машинне навчання)
- National E-Resilience (NER) – національна цифрово-орієнтована модель інтегрованого управління
- ВПО – внутрішньо переміщені особи
- ДКІ – державна критична інфраструктура
- ДПМ – державна політика модернізації
- Е-врядування – електронне урядування
- Е-сервіси – електронні сервіси
- Е-демократія – електронна демократія
- ЕФІ – ефективність функціонування інституцій

ЄС – Європейський Союз

ІДТ – інноваційні діджитал-технології

КІ – критична інфраструктура

КІС – кластер інституційної стійкості

КСІ – Крос-секторальна інтеграція

МВА – місцева військова адміністрація

НАТО – Організація Північноатлантичного договору

НМС – національна модель стійкості

НМС 3.0 – національна ментальна система (модель 3.0)

НРМ – національна resilience-модель (аналог НМС у деяких англomовних публікаціях)

НДП – національна цифрова платформа

ОТГ – об'єднана територіальна громада

ОВА – обласна військова адміністрація

ППП – публічно-приватне партнерство

ПУ – публічне управління

ЦР – цифрова резильєнтність

ЦС – цифрове суспільство

ЦД – цифрова держава

ЦП – цифрова політика

ЦСД – цифрова стійкість держави

ЦІС – цифрова інституціональна спроможність

ЦТ – Цифрові траєкторії (digital institutional trajectories)

ВСТУП

Актуальність дисертаційного дослідження зумовлена глибинними трансформаційними процесами в Україні, які змінюють умови функціонування системи державного управління в епоху цифровізації. Упровадження цифрових технологій у публічне управління є глобальним трендом, спрямованим на підвищення ефективності, прозорості та якості надання публічних послуг. Водночас цей складний і багатовимірний процес відбувається в умовах екзистенційної загрози для української державності, спричиненої повномасштабною збройною агресією РФ проти України. Уведення правового режиму воєнного стану загострило потребу не лише в оперативній адаптації державної управлінської системи до воєнних викликів, а й у її глибокому реформуванні й зміцненні на засадах гнучкості, інноваційності та прозорості. У таких умовах особливої актуальності набуває формування перспективних механізмів державного управління, здатних одночасно забезпечувати вирішення невідкладних завдань воєнного часу та відповідати довгостроковим глобальним викликам і вимогам цифрового розвитку.

Дослідження національної моделі стійкості (НМС) в умовах цифрового суспільства є важливим завданням, оскільки формування раціональної НМС дозволяє визначити, як цифрові технології можуть сприяти підвищенню ефективності публічного управління. Важливим аспектом є розробка теоретико-методологічних засад формування НМС, що враховують специфіку українського контексту та міжнародний досвід у сфері цифровізації, формування нових механізмів публічного управління, які відповідають вимогам сучасного цифрового суспільства. Адже інституціональна спроможність держави та адаптивність її структур до нових викликів є ключовими елементами, які визначають здатність країни забезпечувати національну безпеку, ефективно реагувати на кризи та зберігати стабільність. Так само дослідження кращих світових практик та їх

адаптація до українських реалій має визначальне значення для вдосконалення механізмів стійкості. Саме цифровізація суспільства створює нові можливості для розвитку, але водночас і нові ризики та загрози, які потребують системного підходу до управління.

Актуальність обраної теми дослідження посилюється наявними проблемами формування НМС. У вітчизняній науковій думці цьому питанню приділяють значну увагу, зокрема у працях таких дослідників, як М.Ажажа, О.Акімов, Л.Акімова, О.Ахмедова, А.Андрієнко, О.Антонова, В.Баштанник, Г.Блінова, О.Бобровська, Є.Бородін, Р.Ботвінов, В. Бульба, Т. Василевська, Л.Гаєвська, Н.Гончарук, С.Домбровська, І.Драган, Н.Драгомирецька, І.Дробот, Н.Калашник, С.Квітка, І.Квеліашвілі, В.Колтун, В.Копанчук, А.Колодій, М.Лахижа, Н.Липовська, І.Лопушинський, А.Макурін, Т.Маматова, І.Матвеєнко, С.Мороз, В.Мороз, О.Пархоменко-Куцевіл, П.Петровський, А.Помаза-Пономаренко, О.Поступна, А.Рачинський, Є.Романенко, О.Руденко, О.Сидорчук, В.Сичова, Н.Сорокіна, Т.Тарасенко, В.Тертичка, І.Хожило, І.Чикаренко, Ю.Шаров, І.Шпекторенко, О.Федорчак, Т.Яровий та інші. Важливими аспектами дисертаційного дослідження виступили напрями модернізації системи публічного управління на основі формування національної моделі стійкості, які були розглянуті в працях зарубіжних учених Д.Беккет, С.Халфорд, М.Томпсон, С.МакМеюс, Д. МакОлі, Д.Роса, Л. ДеМарко, Е.Сміт, Х.Джонс, Р.Джонсон, К.Худ, Д.Лін, К.Хаутон, Р.Девіс, В.Елкінтон, М.Барлоу, Е.Рітчі, П.МакГоуен, Л.Еванс та інші. Зарубіжними науковцями запропоновано методологію трансформації державного управління в умовах цифрової стійкості через комплексний аналіз інституційних механізмів адаптації соціальних систем до технологічних змін. Зокрема, це моделі оцінювання цифрової стійкості (резильєнтності) локальних спільнот, які включають системи моніторингу кіберзагроз, методики підвищення цифрової грамотності населення та інструменти стратегічного планування розвитку в умовах невизначеності. Загальним науковим обширом у форматі НМС виступає концепція

«адаптивного врядування», яка передбачає формування гнучких інституційних структур, здатних швидко реагувати на виклики цифрового середовища, забезпечувати інформаційну безпеку та створювати умови для інклюзивного розвитку громад через використання передових цифрових технологій. У контексті інтеграції цифрових технологій у моделі державного управління важливими для дисертаційного дослідження виступили праці дослідників наукової школи професора С.Квітки – О.Мазура, Н.Новиченко, Н.Піскохи, Н.Гусаревич, О.Бардаха, Г.Демошенка.

Разом з тим, за наявності значної кількості наукових праць, присвячених становленню цифрового суспільства та розвитку цифрових інструментів публічного управління, низка ключових аспектів залишається недостатньо опрацьованою. Насамперед це стосується комплексного аналізу взаємообумовленості процесів реформування системи державного управління та формування НМС в умовах цифрової трансформації. Потребує подальшого наукового осмислення, яким чином цифрові технології, електронне урядування, системи відкритих даних, інструменти електронної демократії та цифрові сервіси впливають на здатність держави протистояти внутрішнім і зовнішнім загрозам, підтримувати безперервність функціонування критичних інфраструктур, забезпечувати довіру громадян до влади та підвищувати адаптивність інститутів публічної влади. Важливо також визначити, як саме цифровізація сприяє формуванню інституційних, організаційних та кадрових передумов реалізації НМС, зокрема в умовах воєнного стану та тривалих кризових явищ.

Окремої уваги потребує адаптація законодавства України до міжнародних стандартів і кращих практик у сфері цифрового розвитку, інформаційної безпеки, захисту персональних даних, кіберстійкості та електронного урядування. Гармонізація нормативно-правової бази з європейськими та глобальними підходами є ключовою умовою не лише ефективності управлінських процесів, а й інтеграції України до єдиного цифрового простору, зміцнення її інституційної та функціональної стійкості,

підвищення рівня довіри міжнародних партнерів і залучення інноваційних ресурсів для відбудови та модернізації держави. У цьому контексті постає потреба у цілісному науковому підході, який поєднує аналіз цифрових трансформацій у державному управлінні з розробленням теоретико-методологічних засад національної моделі стійкості, здатної забезпечувати збалансований розвиток, безпеку та конкурентоспроможність України в довгостроковій перспективі. Недостатній розвиток наукової теорії та методології розбудови національної моделі стійкості в умовах цифровізації, а також гостра необхідність визначення ефективних шляхів її формування та реалізації в Україні, обумовлюють актуальність авторського дисертаційного дослідження.

Джерельну базу дослідження становлять законодавчі акти України, нормативно-правові документи зарубіжних країн та міжнародні правові акти, що безпосередньо пов'язані з формуванням національної моделі стійкості в умовах цифрового суспільства. Комплексний підхід забезпечено залученням наукових напрацювань у галузях державного управління, теорії держави і права, конституційного права, політології, соціальної філософії та інших суміжних наук, з особливим акцентом на дослідженнях законодавства ЄС та країн-членів ЄС щодо цифрового розвитку та забезпечення конституювання феномену національної стійкості (national resilience).

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконана відповідно до планів науково-дослідної роботи кафедри державного управління і місцевого самоврядування Навчально-наукового інституту державного управління Національного технічного університету «Дніпровська політехніка» у межах теми науково-дослідної роботи «Забезпечення стійкості, ревіталізації та розвитку територій і громад в Україні» (ДР 0122U002375). Дисертантом у межах зазначеної теми науково-дослідної роботи досліджено теоретико-методологічні аспекти формування НМС в умовах цифрового суспільства, концептуальні основи стійкості та механізми адаптації суспільних інститутів до цифрових

трансформацій, розроблено методологію оцінювання стійкості територій і громад у контексті цифровізації публічного управління. Сформовано моделі цифрової стійкості громад і стратегії підвищення стійкості територіальних систем з використанням цифрових інструментів. Також автором досліджено соціально-комунікативні аспекти, такі як цифрова інклюзія, участь громадян у прийнятті рішень та формування цифрової культури управління, також потребують глибокого аналізу. Основні ідеї дисертаційної роботи, наукові результати та дисертаційні положення сформовані у межах участі у межах науково-дослідних робіт за темами: «Розвиток концепції «електронного села» в контексті побудови інформаційного суспільства» (державний реєстраційний номер 0110U002235, 2010), у межах якої автором розроблені пропозиції щодо формування сучасної цифрової моделі розвитку управлінських механізмів на рівні локальних спільнот; «Гуманізація публічної служби в Україні в контексті формування сучасної парадигми державотворення «Держава для людей»: науково-практичні засади» (державний реєстраційний номер 0113U001136, 2013), у межах якої автором запропоновано визначати індикатори суспільної стабільності та стійкості в умовах нових умов державотворення; «Системний підхід як методологія реформування державної служби» (номер державної реєстрації 0115U002888, 2015), у межах якої автором представлено сучасну методологічну концепцію сучасного державотворення з урахуванням моделей національної стійкості; «Цифрова трансформація публічного управління» (державний реєстраційний номер 0122U002236), 2022-2024 роки – у межах якої автором запропоновано концепцію формування національної моделі стійкості в умовах воєнного стану та повоєнного відновлення.

Мета і завдання дослідження. *Мета* дослідження полягає в теоретико-методологічному обґрунтуванні наукових підходів щодо формування НМС в умовах цифрового суспільства та розробленні на цій основі концептуальних засад для реалізації ефективних стратегій розвитку держави в умовах зовнішніх викликів. Досягнення мети передбачає

вирішення таких основних дослідницьких завдань:

- розкрити сутність НМС у контексті сучасних інституціональних підходів, особливостей розвитку державного управління в умовах правового режиму воєнного стану та викликів цифрового суспільства;
- визначити структурні проблеми та перспективи становлення та розвитку основ законодавства у сфері формування НМС, діяльності державних інститутів у форматі цифрового суспільства та їх адаптивності до інституціональних змін;
- проаналізувати вплив цифровізації на розвиток державних та суспільних ініціатив в Україні, дослідити їх роль у зміцненні соціальної стабільності й безпеки функціонування управлінських систем, формалізувати феномен цифрових управлінських платформ;
- розробити теоретичну концепцію *National E-Resilience* – моделі інтегрованого управління, яка спрямована на забезпечення стійкості України в умовах цифровізації, особливо під час воєнного стану, і включає систематичний підхід до оцінки, аналізу та посилення спроможності держави реагувати на зовнішні та внутрішні виклики;
- дослідити напрями інтеграції передових інформаційних технологій у систему державного управління в контексті формування НМС;
- визначити державноуправлінські інструменти формування суспільної довіри до органів влади та активізації громадянського суспільства в умовах цифрового суспільства;
- дослідити роль крос-інституціонального співробітництва (на рівні крос-інституціональних платформ) в реалізації НМС як процесу взаємодії між державними структурами, бізнесом та неурядовими організаціями у запобіганні кризовим явищам;
- розробити та обґрунтувати комплексну стратегію моніторингу та оцінювання ефективності реалізації НМС, що включає використання сучасних механізмів публічного контролю.

Об'єктом дослідження є суспільні відносини, які виникають у процесі

формування національної моделі стійкості.

Предметом дослідження є теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства

Методи дослідження. Методологічною основою дослідження виступають сучасні теоретичні розробки вітчизняних і зарубіжних учених з питань державного управління в умовах цифрового суспільства, забезпечення стійкості та розвитку держави, цифрової трансформації, інформаційної безпеки, а також загальнонаукові принципи пізнання суспільних явищ. Ключовими підходами виступають системний, міждисциплінарний, інституціональний, конкретно-історичний та функціональний підходи. Системний підхід використовується для дослідження особливостей формування НМС в умовах цифрового суспільства як цілісної системи взаємопов'язаних елементів (розділи 1, розділ 4). Застосування методології системного аналізу дозволило проаналізувати організаційно-правові засади діяльності суб'єктів забезпечення стійкості в системі державного управління, визначити їх функціональні ознаки, характеристики, тенденції та етапи формування НМС (розділ 2).

У процесі дослідження використані загальнонаукові принципи об'єктивності, історизму, аналізу, синтезу, узагальнення та індукції, а також інструментальний, інституційний, соціологічний, аксіологічний, діяльнісний методи, методи статистичної обробки емпіричного матеріалу, особистого спостереження. Історичний метод застосовано для виявлення передумов і факторів формування НМС (розділи 1-3). Логічний метод уможливив теоретичну реконструкцію сутності національної моделі стійкості та її впливу на проведення системних реформ (розділ 4). На основі аналізу конкретизовано типи та сучасні форми реалізації завдань органів влади у сфері забезпечення НМС. Узагальнення використано для аналізу загальних властивостей та закономірностей ролі держави у формуванні НМС. Моделювання дозволило розробити модель оптимізації національної моделі

стійкості в умовах системних реформ. Нормативно-правовий та формально-юридичний методи сприяли аналізу юридичного змісту відповідних документів (розділ 2, розділ 5). Комплексний метод забезпечив проведення аналізу факторів впливу національної моделі стійкості на розвиток держави та громадянського суспільства. Систематизація підходів до розробки засад імплементації зарубіжного досвіду формування та реалізації моделей стійкості дозволила проаналізувати особливості процесів реформування державного управління в контексті відповідності міжнародним стандартам (розділи 2 та 5). Функціональний аналіз використано для обґрунтування напрямів удосконалення державного управління та розроблення структурно-функціональної моделі імплементації зарубіжного досвіду. Важливим методом дослідження виступає аналіз фактологічної та емпіричної інформації органів державного управління, результатів соціологічних досліджень для визначення актуальних напрямів підвищення ефективності державного управління в процесі формування та реалізації національної моделі стійкості. На основі використання наведених методів проаналізовано специфіку та форму впливу ефективності на функціонування системи державного управління.

Наукова новизна одержаних полягає у комплексному обґрунтуванні теоретико-методологічних засад формування НМС у форматі цифрового суспільства на основі вирішення наукової проблеми формування та реалізації концепту Integrated Open Government (IOG) як практичного інструменту для реалізації державних реформ, а також розробки складників парадигми цифрової держави як самостійного напрямку в науці державного управління.

На основі одержаних наукових результатів сформульовано нові положення, які становлять наукову новизну і полягають у тому, що:

у перше :

– комплексно представлено екосистему національної стійкості в умовах цифрового суспільства як окремий напрям у вітчизняній науці державного управління, у межах якого розроблено та науково обґрунтовано

National E-Resilience – національну модель інтегрованого управління, спрямована на забезпечення стійкості України в умовах цифровізації, яка акцентує увагу на розвитку національної стійкості шляхом ефективного використання інформаційних технологій, що дозволяє державі інтегрувати ресурси, політики та процеси в єдину систему, здатну швидко реагувати на кризи та адаптуватися до нових викликів; головними компонентами моделі визначено централізовану цифрову платформу державного управління;

– розроблено методологічну концепцію діяльності органів влади щодо реалізації НМС в Україні на основі проблемного підходу, сутність якої полягає запровадженні формули державно-управлінської діяльності на основі локалізації цифрових рішень для управління, пропонує адаптивні механізми функціонування цифрових систем з урахуванням регіональних відмінностей. Така концепція включає баланс між централізованим контролем і автономністю регіональних органів у цифровому середовищі, й на відміну від усталених у вітчизняній державноуправлінській науці стандартних алгоритмів, передбачає, що базові інституціональні й теоретичні засади неперервності функціонування державного управління в умовах кризових ситуацій враховують сучасні виклики кіберзагроз, руйнування інфраструктури та соціальні ризики; на цій основі розроблено методологію оцінки цифрової стійкості (англ. Digital Resilience Assessment, DRA), що передбачає оцінку здатності складних адміністративних систем адаптуватися до викликів, пов'язаних із цифровою трансформацією;

– запропоновано методологію імплементації зарубіжного досвіду формування НМС, в основу якої покладено компаративно-адаптаційну парадигму, яка, на відміну від раніше відомих вітчизняних методик, ґрунтується на встановленні дихотомічної сутності інституціонального та ментального підходів, іманентних їм критеріїв класифікації форм і методів резильєнтного функціоналізму, що дозволило запропонувати до практичного впровадження теоретичну модель компаративного аналізу модельних платформ національної стійкості, що включає в себе співвідношення між

різними інституційними структурами та культурними цінностями країни. Ця модель дозволяє виявити ключові елементи, які впливають на процеси адаптації та розвитку стійкості в умовах сучасних викликів, зокрема воєнного стану та цифровізації;

– узагальнено комплекс засобів формування та реалізації НМС на центральному, регіональному, галузевому й локальному рівнях через поєднання технологій соціо-динамічного дизайну, принципів пропорційності і супервентності, і передбачає механізми інтеграції цифрових технологій у державне управління для розбудови цифрової резильєнтності, які включають підходи до модернізації державних інститутів. Такі механізми передбачають поступове впровадження міжнародних стандартів кібербезпеки, створення адаптаційних стратегій для використання технологій штучного інтелекту, автоматизації процесів та роботизації управлінських функцій. У такому контексті запропоновано методику побудови механізму цифрової інституційної спроможності (англ. Adaptive Institutional Capacity Building);

удосконалено:

- понятійно-категоріальний апарат науки державного управління, зокрема уточнено зміст ключових категорій: «національна стійкість», «суспільна стійкість», «цифрове суспільство», «цифрова держава», «цифрова політика». У межах дослідження розроблено авторську концепцію формування засад державного управління у сфері цифровізації, яка включає інноваційні критерії реалізації національної моделі стійкості (НМС) на різних рівнях публічного управління та спрямована на посилення спроможності державних інститутів до адаптації й розвитку в умовах цифрових трансформацій. Визначено базову категорію дослідження – «інституціоналізація цифрової політики у форматі НМС», що відображає процес формування та розвитку інституційних засад державного управління у сфері цифрової політики. Цей процес зорієнтований на забезпечення цифрової резильєнтності держави в умовах системних змін і викликів, пов'язаних із цифровізацією, та охоплює: визначення правових рамок

державної політики, створення й удосконалення організаційних структур публічної влади, здатних оперативно адаптуватися до нових умов, а також забезпечення активної участі інститутів громадянського суспільства у формуванні та реалізації цифрової політики, що підвищує соціальну згуртованість, легітимність рішень і довіру до органів державної влади.

– теоретичні засади дослідження основних викликів реалізації в умовах особливих режимів адміністрування та державно-управлінських реформ, що дозволило: виокремити специфічні форми діяльності органів влади; обґрунтувати феномен сучасного публічного управління у форматі «цифрового врядування», встановити пряму залежність стану ефективності НМС від методів і форм державноуправлінської діяльності; На цій основі сформовано рамкову модель інтегрованого відкритого державного управління (англ. «Integrated Open Governance Framework»), яка передбачає системну інтеграцію цифрових технологій саме в систему державного управління з метою забезпечення її відкритості, прозорості, підзвітності та розширення участі громадян і локальних спільнот у процесах вироблення та ухвалення управлінських рішень. У межах такої моделі здійснюється аналіз механізмів взаємодії між органами державної влади та суспільством, оцінка ефективності цифрових інструментів залучення громадян до управління, а також розробляються рекомендації щодо вдосконалення нормативно-правового та організаційного забезпечення сучасного державного управління на засадах відкритості, інтегрованості та стійкості;

– методологічні підходи до формування механізмів інтеграції цифрових технологій у систему державного управління, спрямовані на забезпечення цифрової стійкості держави. Запропоновані підходи передбачають розроблення системи індикаторів оцінки стійкості державного управління в умовах цифрової трансформації, яка охоплює, зокрема, показники: ефективності кіберзахисту; адаптивності інституцій публічної влади; рівня цифрової інклюзії; резильєнтності критичних інфраструктур до сучасних загроз і викликів. Наведена система індикаторів дає змогу системно

оцінювати результативність механізмів забезпечення стійкості державного управління, що є критично важливим для його адаптації до нових умов цифрового розвитку та кризових ситуацій. Розроблені механізми інтеграції цифрових технологій ґрунтуються на принципах інституційної адаптації, захисту даних, прозорості та відкритого доступу до інформації, що формує основу для модернізації державноуправлінських процесів, підвищення їх ефективності, підзвітності та довіри громадян до органів державної влади.

дістали подальшого розвитку:

- методологія структурно-функціонального аналізу сучасного соціального тренду «цифрова стійкість» у системі державного управління та дослідження його інституціональних форм, обґрунтування змісту технологій. На цій основі запропоновано використовувати три підходи: 1) адаптивний структурно-функціональний підхід (англ. Adaptive Structural-Functional Approach), який акцентує увагу на гнучкості та адаптивності системи державного управління в умовах швидких соціальних змін, зокрема в контексті цифровізації; 2) інтегративний функціональний підхід (англ. Integrative Functional Approach), спрямований на об'єднання різних аспектів державного управління (соціальні, економічні та технологічні фактори, для досягнення стійкості системи. Цей підхід передбачає, що ефективність управлінських рішень залежить від їхньої здатності інтегрувати різні елементи суспільних відносин;

- управлінські технології в умовах упровадження зарубіжного досвіду формування НМС, що дало змогу сформулювати концептуальні засади практичної реалізації НМС у системі державного управління з метою приведення її у відповідність до європейських стандартів, зокрема шляхом: 1) інтеграції багаторівневого управління, яка передбачає узгодженість рішень на національному, регіональному та місцевому рівнях із залученням усіх зацікавлених сторін – органів державної влади, приватного сектору та інститутів громадянського суспільства; застосування цього підходу сприяє ефективнішій координації у вирішенні кризових ситуацій та забезпеченні

стійкості; 2) запровадження механізмів е-врядування, що включають використання цифрових платформ для надання адміністративних послуг, моніторингу загроз та інтеграції інформаційних ресурсів, що, у свою чергу, прискорює комунікацію між державними інститутами, забезпечує прозорість управлінських процесів і підвищує довіру громадян до держави; 3) розроблення стратегій управління ризиками, орієнтованих на попередження кризових ситуацій і мінімізацію їх наслідків; при цьому методологія прогнозування, оцінювання та управління ризиками запозичена з європейських практик, серед яких ключове місце посідає створення систем раннього попередження та адаптації до змінних умов

– наукові підходи щодо реформування державного управління на основі реалізації моделі НМС та Стратегії реформування державного управління на до 2025 р., й на цій основі доведено, що суттєвих змін потребують концептуальні нормативно-правові акти з питань регіональних стратегій запровадження НМС, у межах яких регіони виступають ключовими суб'єктами впровадження НМС, й на цій основі запропоновано розробити смарт-резильєнтні регіональні стратегії (СРРС). Смарт-резильєнтні регіональні стратегії є інноваційним підходом до забезпечення стійкості регіонів, що враховує їх унікальні соціально-економічні, географічні, екологічні та культурні особливості. Ці стратегії спрямовані на зміцнення регіональної здатності реагувати на кризи, адаптуватися до нових умов і підвищувати свою життєздатність на основі інтеграції інтелектуальних (смарт) рішень та принципів резильєнтності, які враховуватимуть особливості кожного регіону, а також забезпечуватимуть інтеграцію регіональних планів із загальнонаціональними цілями стійкості.

Практичне значення одержаних результатів Основні положення дослідження щодо формування напрямів реалізації НМС впроваджені:

– Державним агентством водних ресурсів України при використанні результатів дисертаційного дослідження в частині розробки нормативних документів (довідка про впровадження № 6480/01/11-24 від 12.01.2025 р.);

- Херсонською обласною військовою адміністрацією при використанні результатів дисертаційного дослідження у діяльності органів влади Херсонської області (довідка про впровадження № 01-01-58-12095/0/24/ від 12.01.2025 р.);
- Громадською організацією ГНО «Фундація публічно-правових ініціатив» у межах науково-методичного забезпечення проєкту «Розвиток громад Дніпропетровської області» в контексті організації правової та методичної допомоги територіальним громадам (довідка про впровадження від 28.08.2024 № 20-21/28-1);
- Перещепинською міською радою Самарського району у розробки та впровадження цифрової інтегрованої інформаційно-аналітичної системи «Єдина платформа житлово-комунальних послуг», від 08.01.2025 № 2/23-25;
- Адвокатським об'єднанням «Пантеон» у межах громадських ініціатив протягом 2022-2024 рр. у контексті організації правової та методичної допомоги територіальним громадам (довідка про впровадження від 28.10.2024 № 112/28-11).

Апробація результатів дисертації. Основні положення дисертації висвітлено в доповідях на науково-практичних конференціях і семінарах, у тому числі: «Формування дієвих механізмів державного управління з забезпечення державної безпеки» (м. Харків, 14 трав. 2021 р.), «Східна політика Європейського Союзу: здобутки, виклики та перспективи» / *Wschodnia Polityka Unii Europejskiej: osiagniecia, wyzwania i perspektywy*: VI Polsko-Ukraińskiego Forum Naukowego (27-28 maja 2021, Lwów), «Трансформація системи публічного управління створенням здоров'я збережувального та безпечного простору України» (модернізація, інновації, розвиток), (м. Переяслав, 11 червня 2021 року), «Modern scientific research: achievements, innovations and development prospects», (July 4-6, 2021, Berlin), «Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні» м. Київ, 15-28 квітня 2022 р., «Міжнародні економічні відносини. Сталий розвиток України в умовах глобалізації та європейської

економічної інтеграції: проблеми, перспективи, ефективність» (м. Харків, 31 травня 2022 р.), «Актуальні проблеми європейської та євроатлантичної інтеграції України» (16 червня 2022 р., Дніпро), «Публічне управління та адміністрування в сучасних умовах» (м. Дніпро, 28 квітня 2022 р.), «International Scientific and Practical Conference Proceeding), (January 26, 2023) та інші.

Особистий внесок здобувача. Дисертація є завершеною самостійною науковою працею. Основні положення, розробки в межах дослідження, наукові результати, винесені на захист, ґрунтуються на особистих дослідженнях автора. Ідеї та розробки, що належать співавторам окремих робіт, у дисертації не використовувалися. Внесок автора в публікації, виконані в співавторстві, конкретизовано у списку праць, опублікованих за темою дисертації.

Публікації. Основні положення та результати дисертації відображено у публікаціях автора: 4 колективних монографіях (2 з яких видані у зарубіжному видавництві), 6 статей у зарубіжних наукових періодичних виданнях (індексованих у НМБ Scopus і Web of Science); 20 статей у фахових наукових виданнях України з публічного управління та адміністрування, 15 тезах доповідей у збірниках матеріалів наукових комунікативних заходів.

Структура й обсяг дисертації. Дисертаційна робота складається зі вступу, п'яти розділів, висновків, списку використаних джерел, додатків. загальний обсяг дисертації становить 678 сторінок, у тому числі 558 сторінок основного тексту. Дисертація містить 17 рисунків, 43 таблиці. Список використаних джерел складається з 392 найменувань. У роботі 4 додатки на 64 сторінках.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬНИХ ВІДНОСИН

1.1. Концептуальні засади становлення сучасних моделей функціонування системи публічного управління як суспільного феномену

Сучасний етап розвитку світової цивілізації характеризується фундаментальними змінами у взаємодії між державою та суспільством. Зростання використання цифрових технологій у публічному управлінні трансформувало процес надання послуг, зміщуючи фокус з уніфікованих бюрократичних процедур на гнучкі, адаптивні моделі [1;2;3]. Глобальна цифровізація диктує нові вимоги: громадяни, звиклі до високих стандартів сервісу у приватному секторі (банкінг, ритейл, розваги), очікують аналогічного рівня комфорту, швидкості та уваги від державних органів. У цьому контексті акцент на необхідності персоналізованого підходу до задоволення різнопланових потреб громадян стає не просто трендом, а імперативом виживання та легітимації сучасних систем державного управління. Саме персоналізація публічних послуг стає вирішальним фактором покращення клієнтоорієнтованості органів державної влади, зміцнення довіри громадян і підвищення ефективності надання послуг. Перехід від моделі «держава для всіх» до моделі «держава для кожного» (на кшталт «Government for Citizens to Government for You») вимагає переосмислення самої філософії публічного адміністрування [4-5].

Актуальність тематики дисертаційного дослідження у широкому розумінні зумовлена швидким глобальним переходом до електронного урядування (e-governance) та зростаючими очікуваннями громадян щодо оперативного реагування на їхні потреби в адміністративних послугах, адаптованих до індивідуальних запитів. В умовах невизначеності, кризових

явищ та, зокрема для України, умов воєнного стану, здатність держави надавати адресну, точкову допомогу та послуги стає питанням національної безпеки та соціальної стабільності. На думку Є.Бородіна, С.Квітки, Г.Демошенка, цифрові технології, зокрема штучний інтелект (ШІ), аналіз великих даних (Big Data) і блокчейн, відкривають перед органами державної влади нові можливості для аналізу даних про громадян, прогнозування їхніх потреб і надання індивідуальних рішень [6;7]. Водночас, впровадження таких технологій порушує складні питання інклюзивності, етичного використання даних та балансу між ефективністю й справедливістю. Ці виклики є особливо актуальними для України, де цифрова трансформація відбувається швидкими, але нерівномірними темпами, що створює як значні можливості, так і системні обмеження.

Очевидно, що систему публічного управління доцільно розглядати не лише як набір органів та процедур [8], а як складний суспільний феномен, що формується на перетині владних повноважень, суспільних очікувань, культурних норм, технологічних можливостей і історичного досвіду. Така система втілює спосіб, у який суспільство самоорганізовується, визначає прийнятні форми колективної дії, розподілу ресурсів і відповідальності [9]. У цьому сенсі публічне управління водночас є й інструментом реалізації політичної влади, і механізмом координації багатьох соціальних акторів, і простором, де вибудовується довіра, легітимність та відчуття спільної належності до політичної спільноти.

Адже у традиційних концепціях державного управління, побудованих на веберівській бюрократичній моделі, наголос робився переважно на формально-юридичній організації апарату: ієрархії, компетенціях, нормативних регламентах, стандартизованих процедурах [10]. Такий підхід забезпечував передбачуваність, контроль і формальну рівність, але водночас відсував на другий план людину як унікального суб'єкта з її конкретними потребами, обставинами та очікуваннями щодо якості взаємодії з публічною владою. У міру розвитку демократії, громадянського суспільства та ринкових

відносин виявилося (на думку І. Арістової), що цієї бюрократичної раціональності недостатньо для легітимації держави в очах громадян, які дедалі більше орієнтуються на цінності гідності, поваги, участі, а також на стандарти сервісу, задані приватним сектором [11-12].

Цей методологічний зсув у ціннісних орієнтаціях збігся з появою нових теоретичних парадигм у науці державного управління – від нового публічного менеджменту до концепцій *good governance*, публічного врядування та нового публічного сервісу, раціонально представленою британською науковою школою – С.Hood [13-15], G.Mulgan [16-18], D.Rosenbloom [19-20]. Їх спільною рисою є визнання того, що система публічного управління має оцінюватися не лише за формальними показниками виконання функцій, а насамперед за тим, якою мірою вона створює та підтримує публічну цінність, тобто відповідає реальним потребам громадян, зміцнює довіру, забезпечує справедливий доступ до благ і можливостей. Очікування індивідуального, ефективного й швидкого підходу у взаємодії з державними установами прямо впливають із цієї логіки: громадянин більше не задовольняється роллю пасивного «одержувача послуг», він бачить себе клієнтом, партнером, співтворцем політики [21].

Проте традиційні стандартизовані моделі т.з. «сервісного управління», ймовірно успадковані від попередніх етапів розвитку державності, часто не відповідають таким запитам. Вони зорієнтовані на умовного «середньостатистичного» отримувача, для якого встановлюється єдина процедура незалежно від життєвого контексту [22]. Такий підхід певною мірою забезпечує формальну рівність, але на практиці призводить до ситуацій, коли саме найбільш уразливі групи стикаються з найвищими бар'єрами доступу. Тим часом приватний сектор (банки, електронна торгівля, телекомунікації) завдяки використанню цифрових технологій, аналізу даних та сервіс-дизайну давно перейшов до моделей персоналізованого обслуговування, де інтерфейси, пропозиції та канали взаємодії налаштовуються під конкретного користувача. Цей контраст створює для

публічного управління постійно відчутний «сервісний розрив», який підриває сприйняття держави як сучасного та ефективного інституту. Сучасна наукова теорія державного управління фіксує, що цей розрив має не лише технологічний, а й глибокий інституційно-ціннісний характер. З одного боку, органи влади за інерцією зорієнтовані на мінімізацію власних ризиків, жорстке дотримання формальних процедур, уникнення помилок будь-якою ціною. З іншого боку, суспільство очікує гнучкості, адаптивності, емпатії та готовності враховувати специфіку життєвих ситуацій. Відтак на перетині цих протилежних логік виникає трансформаційна напруга, яка й стає рушійною силою для переходу від уніфікованого адміністрування до людиноцентричного державного управління [23].

Саме тому цифрові технології, що стрімко проникають у сферу публічного управління, істотно змінюють можливості реалізації цієї трансформації. Інструменти електронного урядування, інтегровані державні реєстри, аналітика великих даних, штучний інтелект, мобільні платформи дозволяють принципово інакше організувати як внутрішні процеси, так і взаємодію з громадянами. У теоретичній площині це означає перехід від моделі «апарату», що механічно виконує набір функцій, до моделі «цифрової екосистеми врядування», де дані, сервіси й комунікація інтегруються в єдиний контур. У цій екосистемі стає реалістичною персоналізація послуг, коли держава не просто однаково обробляє всі звернення, а будує індивідуальні траєкторії взаємодії з кожною людиною, враховуючи її статус, історію звернень, життєві події [24].

Поступове впровадження такої цифрової екосистеми закономірно виводить дослідження у площину національної стійкості. На перший погляд, персоналізація та клієнтоорієнтованість можуть сприйматися як «сервісна надбудова», що мало стосується базових питань безпеки та виживання держави. Однак у сучасній теорії державного управління все більш утверджується підхід, за яким стійкість системи розглядається не лише через призму матеріальної інфраструктури чи силових інститутів, а й через

здатність інституцій влади забезпечувати безперервність публічних функцій, адаптуватися до шоків і підтримувати довіру громадян у довгостроковій перспективі. У цій логіці те, як саме організовано надання адміністративних послуг, як швидко й чутливо держава реагує на індивідуальні та колективні потреби, стає безпосередньою складовою національної стійкості.

Поступово стає очевидно, що система публічного управління як суспільний феномен є водночас і ядром, і індикатором національної стійкості. Якщо інституції діють із запізненням, залишають значні групи населення «невидимими», не здатні налаштувати механізми підтримки під реальні життєві ситуації людей, це породжує накопичення фрустрацій, розчарування, відчуття «неналежності», що особливо небезпечно в умовах гібридних загроз і інформаційних атак. Навпаки, коли громадянин бачить, що навіть у кризовій ситуації держава здатна швидко ідентифікувати його потреби, надати доступну й зрозумілу допомогу, мінімізувати бюрократичні бар'єри, це зміцнює відчуття захищеності, формує досвід позитивної взаємодії з інститутами, підвищує готовність до солідарної поведінки.

У межах теорії державного управління це варто описати через поняття резильєнтного врядування – такого типу сучасного врядування, що поєднує здатність до превенції, адаптації й відновлення. Резильєнтність системи публічного (державного) управління передбачає, що така система не лише формально виконує закріплені за нею функції, а й здатна гнучко змінювати правила, процедури, організаційні форми, зберігаючи при цьому базові цінності та принципи. Саме цифровізація й персоналізація стають тими інструментами, які дозволяють здійснювати такі зміни швидко та адресно: інтеграція реєстрів забезпечує комплексне бачення ситуації окремих домогосподарств, алгоритми аналізу даних дають змогу виявляти тенденції та вразливості, а цифрові платформи полегшують донесення рішень до кінцевих користувачів [25]. При цьому важливо підкреслити, що застосування концепції національної стійкості до сфери публічного управління не повинно зводитися до суто технократичного виміру. Йдеться

не лише про те, щоб захистити реєстри від кібератак чи забезпечити резервні канали зв'язку. Справжня стійкість формується на рівні взаємних очікувань та зобов'язань між громадянами й державою. Якщо система публічного управління сприймається як чужа, байдужа або несправедлива, готовність суспільства підтримувати її в умовах кризи знижується. Якщо ж вона постає як простір, де поважають людську гідність, чують індивідуальні голоси, намагаються враховувати контексти, тоді навіть у найскладніших обставинах зберігається базова довіра та мотивація до кооперації.

Саме тому поступове «навантаження» проблематики національної стійкості на концепцію публічного управління як суспільного феномену розкриває її справжню глибину. Питання персоналізації послуг, клієнтоорієнтованості, цифрової інклюзії, захисту даних, алгоритмічної справедливості перестають бути другорядними деталями сервіс-дизайну і постають як чинники, що безпосередньо впливають на здатність держави витримувати й долати довготривалі потрясіння – військові, економічні, демографічні, інформаційні. У теоретичному плані це означає зближення двох дослідницьких полів: класичної науки державного управління та міждисциплінарних студій з безпеки й resilience, де предметом аналізу стає уже не лише «ефективність» чи «результативність» політики, а й її внесок у збереження та розвиток соціальної тканини суспільства.

Концепція стійкості (резильєнтності) у системі базових категорій і понять державного управління визначається як здатність суб'єктів публічної влади та суспільних систем адаптуватися, протистояти, відновлюватися та розвиватися після стану «управлінського шоку», кризи чи зовнішньої агресії, зберігаючи при цьому свою ключову функціональність, структуру та легітимність. Стійкість є не статичною властивістю, а динамічним процесом і ключовим індикатором ефективності управління в умовах гібридних загроз та екстремальних навантажень. Стійкість також не є синонімом традиційної безпеки чи стабільності, а є комплексним поняттям, яке інтегрує наведені категорії, й детермінує здатність системи адаптуватися, поглинати кризовий

стан, швидко відновлюватися та навчатися після його дії. Фактично, у межах предметного поля державного управління мова йде про інтеграцію понять стабільності (як здатності системи тривалий час функціонувати у заданих параметрах за відсутності зовнішніх впливів, тобто збереження стану) та безпеки (захищеності від відомих загроз через превентивні та оборонні заходи),

Таким чином, концепція становлення системи публічного управління як суспільного феномену, доповнена виміром національної стійкості, дозволяє по-новому осмислити як поточні реформи, так і стратегічні орієнтири держави [26]. Вона показує, що трансформація від бюрократичної машини до людиноцентричної, цифрово підсиленої системи врядування є не лише шляхом до підвищення сервісної якості, а й необхідною умовою виживання та розвитку політичної спільноти в умовах тривалої невизначеності. Публічне управління в цьому контексті постає як ключовий модератор взаємодії між індивідуальними життєвими траєкторіями та колективною здатністю суспільства зберігати цілісність, адаптуватися до нових викликів і водночас утверджувати цінності демократії, прав людини та верховенства права.

Аналіз еволюції теоретичних парадигм публічного управління демонструє, що кожна з них по-своєму інтерпретує природу, механізми та виміри стійкості управлінських систем. У сучасному світі, де держави стикаються з безпрецедентними безпековими, кліматичними, демографічними та технологічними викликами, стійкість (resilience) перестає бути лише технічною характеристикою організацій і набуває статусу фундаментальної якості всієї системи публічного управління. Пропонований аналіз виокремлює п'ять базових концепцій суспільного управління та досліджує, як кожна з них концептуалізує феномен стійкості, якими інструментами її забезпечує та які ціннісні орієнтири вважає ключовими для її досягнення. Перш за все, мова йде про бюрократію (стійкість через процедурну раціональність).

Власне, класична теорія бюрократії, розроблена М.Вебером на початку ХХ століття, заклала основи сучасного розуміння публічного управління як окремої сфери професійної діяльності. Модель М.Вебера постулює, що стійкість управлінської системи досягається насамперед через деперсоналізацію влади та раціоналізацію процедур – передбачуваність, ієрархічність, стандартизацію, документальну фіксацію дій та рішень. У цій парадигмі ключовим механізмом забезпечення стійкості виступає формалізація процедур, що мають залишатися незмінними незалежно від зміни політичних лідерів чи зовнішніх обставин [27-28]. Так само німецька школа адміністративного права розвинула ідеї М.Вебера, закріпила принцип законності як фундаментальної опори стійкості. Вона стверджує, що саме чітке дотримання правових норм усіма учасниками адміністративних відносин створює передбачуваність, яка є основою стабільності державних інститутів. Ця концепція була домінуючою протягом більшої частини ХХ століття й досі залишає значний відбиток на організації державної служби в більшості країн.

У цій інтерпретації стійкість системи публічного управління гарантується її здатністю функціонувати за встановленими правилами незалежно від політичних флуктуацій. Отже, у контексті національної стійкості модель М.Вебера пропонує свою специфічну конструкцію: інституціональна пам'ять, процедурна стабільність і чітко регламентована ієрархія забезпечують безперервність функціонування держави навіть в умовах зміни адміністративних режимів чи глибоких політичних криз. Це продемонстрували приклади повоєнної Німеччини та Японії, де саме збереження базових елементів бюрократичного апарату (попри його трансформацію) забезпечило управлінську спадкоємність.

Водночас концепція стійкості (у моделі М.Вебера) має суттєві обмеження, особливо в контексті сучасних динамічних загроз. Надмірна регламентація призводить до ригідності, що знижує адаптивність системи до швидких змін. Як зазначає Г. Пітерс, «класична бюрократія чудово

функціонує в передбачуваному середовищі, але виявляє критичну вразливість перед обличчям невизначеності та плинності» [29]. Особливо це стосується ситуацій гібридних загроз, коли стійкість потребує не тільки дотримання процедур, а й здатності до швидкої реконфігурації та інновацій.

Власне, сама еволюція класичних теоретичних парадигм державного (у широкому розумінні, публічного управління) демонструє, що кожна з них по-своєму інтерпретує природу, механізми та виміри стійкості управлінських систем. У сучасному світі, де держави стикаються з безпрецедентними безпековими, кліматичними, демографічними та технологічними викликами, стійкість (resilience) перестає бути лише технічною характеристикою організацій і набуває статусу фундаментальної якості всієї системи публічного управління. Пропонований аналіз виокремлює п'ять базових концепцій суспільного управління та досліджує, як кожна з них концептуалізує феномен стійкості, якими інструментами її забезпечує та які ціннісні орієнтири вважає ключовими для її досягнення.

Першою концептуальною моделлю є концепція бюрократії М.Вебера, яку ми визначаємо як стійкість через процедурну раціональність. Концепція бюрократії М.Вебера є класичною моделлю раціонального управління, що ґрунтується на процедурній раціональності. Проведення аналізу цієї моделі з позиції резильєнтності (стійкості), яку ми визначаємо як стійкість через процедурну раціональність, дозволяє оцінити сильні та слабкі сторони веберівської ідеальної бюрократії в умовах сучасних криз та гібридних загроз. М.Вебер розглядав бюрократію як ідеальний тип адміністративного апарату, що є найбільш ефективним і технічно досконалим: 1) ієрархія як чітка структура підпорядкування, що забезпечує єдність командування та швидке доведення рішень (*функціональна стійкість*); 2) правила та норми (Rules and Regulations), коли управління здійснюється на основі писаних, універсальних та обов'язкових правил (*стійкість регулювання*); 3) безособовість, де рішення приймаються об'єктивно, незалежно від особистих відносин (*стійкість управлінського алгоритму*); 4) спеціалізація, коли кожен

чиновник має чітко визначені повноваження та експертизу (*стійкість процедури*); 5) кар'єра на основі кваліфікації, а чиновники призначаються за компетентністю (меритократія), а не за політичною лояльністю (*стійкість втручання*) [27-28].

Таблиця 1.1

Концептуалізація підходів щодо феномену стійкості у межах концепції
бюрократії М.Вебера: стійкість через процедурну раціональність

Вимір / аспект	Характеристика (бюрократія М.Вебера)	Потенціал для стійкості	Обмеження / ризики для стійкості
Природа публічного управління	Ієрархічна, формалізована система; управління як реалізація законів через чіткі процедури	Забезпечує передбачуваність, послідовність дій, керованість у стабільних умовах	Ригідність, слабка здатність до швидкої адаптації в умовах невизначеності й криз
Джерело стійкості	Законність, формалізація, стандартні процедури, професійна бюрократія	Інституційна пам'ять, збереження функцій незалежно від зміни політичних еліт	Формалізм, домінування процедури над результатом, загроза «паралічу через правила»
Роль громадянина	Переважно підпорядкований об'єкт управління; «адресат» норм і процедур	Уніфікований підхід гарантує формальну рівність доступу до послуг	Індивідуальні потреби ігноруються, низька клієнтоорієнтованість, відчуття дистанції й відчуження
Інструменти та механізми	Регламенти, інструкції, жорстка ієрархія, контроль дотримання норм	Розподіл повноважень і відповідальності знижує хаос і зловживання	Надмірний контроль гальмує інновації, ініціатива «знизу» придушується
Формат національної стійкості	Процедурна стійкість: безперервність роботи завдяки стабільним правилам і структурі	Можливість функціонування базових адміністративних процесів навіть за політичних змін чи турбулентності	Недостатня гнучкість для реагування на нові, нетипові загрози (гібридні війни, кіберзагрози, швидкі соціальні зміни)
Представницькі школи / автори	М. Вебер; німецька адміністративно-правова школа; класична адмін. школа (В. Вільсон)	Закладають фундамент правової та процедурної стійкості, що й досі є основою багатьох сучасних адміністративних систем	Орієнтація на «нормальний стан» суспільства, слабе опрацювання кризових і надзвичайних режимів

Джерело: [27-28].

Саме універсальність правил і безособовість рішень є процедурною

раціональністю. Отже, якщо процедура дотримана, результат є легітимним, незалежно від політичних змін. Класична теорія бюрократії, розроблена М.Вебером на початку XX століття, заклала основи сучасного розуміння публічного управління як окремої сфери професійної діяльності. Модель М.Вебера постулює, що стійкість управлінської системи досягається насамперед через деперсоналізацію влади та раціоналізацію процедур – фактично, ми вказуємо на передбачуваність, ієрархічність, стандартизацію, документальну фіксацію дій та рішень як властивості стійкості.

У цій парадигмі ключовим механізмом забезпечення стійкості, на нашу думку, виступає формалізація процедур, що мають залишатися незмінними незалежно від зміни політичних лідерів чи зовнішніх обставин. Адже у стабільних умовах така модель дозволяє ефективно керувати масштабними структурами, мінімізуючи вплив суб'єктивних особливостей та персональних інтересів. Це призводить до повторюваності адміністративних рішень: аналогічні ситуації вирішуються однаково з урахуванням єдиного для всіх підходу. Джерелом стійкості бюрократії є саме законність, жорстка формалізація процедур і професіоналізм апарату, що забезпечує інституційну пам'ять: система зберігає та відтворює управлінські практики навіть при зміні політичних еліт чи політичного режиму (Weber, 1968) [28]. Таким чином, національна держава може підтримувати базові функції, законність і керованість у довгостроковій перспективі, незалежно від турбулентності політичного процесу.

Проте надмірна формалізація несе й певні ризики. Вона може перерости у «формалізм», коли дотримання процедури стає самоціллю, незалежно від її реальної корисності для суспільства. У такій ситуації бюрократична машина може ставати занадто інертною, а громадяни можуть зіштовхуватись із ситуаціями абсурдних вимог і процедур, що знижує гнучкість апарату та його орієнтацію на досягнення конкретного результату. У моделі М.Вебера громадянин виступає радше як адресат норм і процедур, аніж повноцінний суб'єкт партнерських відносин із державою. Його роль

зводиться до виконання встановлених правил, що забезпечує формальну рівність, але водночас ігнорує унікальність особистих або життєвих обставин. Це породжує дистанцію й відчуження між громадянином і державою, позбавляючи останню гнучкості й здатності враховувати індивідуальні потреби. З погляду веберівської теорії, така модель виправдана бажанням створити прозору, неупереджену й уніфіковану систему розподілу державних благ, але водночас, це чинник потенційної делегітимації в сучасних умовах, де запитується людиноцентричність та персоніфікований сервіс [28].

Основними інструментами та механізмами у парадигмі публічного управління М.Вебера є чіткі регламенти, формалізовані інструкції, вертикальна ієрархія, суворий контроль і система звітності. Їх сила полягає у здатності укріплювати стабільність, забезпечувати розподіл повноважень, мінімізувати хаос і підвищувати передбачуваність процесів у межах великої організації держави. Водночас, саме ці механізми обмежують ініціативу, сприяють консерватизму та гальмують інноваційний розвиток: будь-яка пропозиція чи нова практика, яка виходить за межі усталених правил, сприймається як загроза порядку.

Вважаємо, що форматом національної стійкості в екстраполяції у межах моделі М.Вебера постає процедурна стійкість як здатність державної машини зберігати основні функції навіть за зміни урядів і політичних курсів, забезпечувати безперервність публічних послуг (реєстрації, ліцензування, облік, соціальний захист) й інерційність структур. Це дає значні переваги в умовах політичної турбулентності: бюрократичний апарат виступає гарантом стабільності й зменшує хаос у суспільстві. Однак у ситуаціях нових, гібридних чи непередбачуваних загроз (кібератаки, війна, технологічні злами) класична бюрократія часто виявляється занадто інерційною, оскільки її міцність базується на відтворенні сталої процедури, а не на гнучкому переформатуванні дій. Водночас і німецька, і американська традиції фокусуються переважно на стандартних, «нормальних» умовах

функціонування держави, тоді як управління в умовах кризи чи турбулентності лишається теоретично мало розробленим.

У цій інтерпретації стійкість системи публічного управління гарантується її здатністю функціонувати за встановленими правилами незалежно від політичних флуктуацій. *Стійкість (через концепт «адміністративної ефективності») – це здатність бюрократичної системи стабільно та передбачувано виконувати свої функції завдяки раціональній організації апарату, чіткому розподілу повноважень і мінімізації внутрішніх витрат ресурсів.* У цій логіці стійкість означає, що бюрократична система, спираючись на раціональну організацію й професійний менеджмент, може тривалий час підтримувати керованість, безперервність надання послуг і відтворення управлінських рішень навіть за зміни політичних еліт чи коливань політичного курсу. Вона тримає «нормальний» режим функціонування [30], коли процеси не розпадаються, зв'язки між ланками не рвуться, а базові результати адміністративної діяльності гарантовано досягаються.

Водночас, така модель стійкості має вбудовану межу – адміністративна ефективність у межах класичної бюрократії орієнтована на оптимізацію наявних процедур і структур, а не на їх радикальне переосмислення. Тобто система добре вміє робити «те саме, але краще», проте значно гірше пристосована до ситуацій, коли самі цілі, формати чи правила функціонування потрібно швидко змінити. Тому стійкість на основі адміністративної ефективності є потужною в умовах відносної стабільності та еволюційних змін, але виявляється недостатньою перед обличчям нетипових, гібридних, швидких загроз, де необхідні не лише відтворення і раціоналізація, а й гнучка трансформація самої логіки управління. Отже, національна модель стійкості (через концепт адміністративної ефективності) – це така організація діяльності державних інститутів, процедур і ресурсів, за якої країна здатна стабільно та раціонально виконувати базові публічні функції, підтримувати керованість і безперервність послуг, мінімізувати

внутрішні втрати й втрати функціонування навіть за політичних чи соціально-економічних коливань.

У контексті формування національної моделі стійкості, фундаментальні ідеї М. Вебера щодо раціональної бюрократії (Weber, 1968) [] набувають особливого значення для розуміння стійкості сучасної національної держави. Адже за М.Вебером бюрократія ґрунтується на формальній правовій раціональності, чіткій ієрархії повноважень, імперсональності і суворому дотриманні процедур, усі ключові елементи якої створюють передумови для організаційної та процедурної стійкості. Саме у працях [27-28] М.Вебер розкриває ідеал типу легального панування і апарату, що забезпечує безперервність, повторюваність та передбачуваність державної влади навіть в умовах зміни правителів чи політичної кон'юнктури. Національна держава, за Вебером, структурно і функціонально спирається на професійну бюрократію як «суцільний апарат служби», що покликаний безумовно реалізувати легально встановлені закони (Weber, 1968) [28]. У цьому сенсі адміністративна ефективність виступає категорією, яка дозволяє цілісній державній структурі підтримувати відтворення регламентованих владних функцій у межах чітких національних кордонів, а відтак – гарантувати інституційну стійкість як внутрішню, так і зовнішню (Weber, 1968) [28].

Саме тому слід розвивати ідеї М.Вебера у напрямі інтегративної функціональності, де ефективність вже не просто ототожнюється з жорсткою формалізованістю процедур, а набуває ознак адаптивного балансу між суворою законністю й організаційною гнучкістю у відповідь на виклики доби. Це дозволяє визначати національну модель стійкості як систему інституцій, структур та механізмів, здатних не лише стабільно відтворювати легітимну владу (за М.Вебером), але й забезпечувати адаптивність, інноваційну відкритість та продуктивність публічного апарату навіть у нестабільних соціально-політичних умовах. Зокрема, М.Вебер наголошував, що саме імперсоналізм і професіоналізм державної служби сприяють формуванню довготривалого «державного порядку» (Weber, 1968), який

новітні дослідники інтерпретують як стійкість націй у глобальному контексті. Однак обмеження класичної веберівської моделі полягають у тому, що така система орієнтується на відтворення «нормального» стану, демонструючи обмежену здатність швидко перебудовуватись у відповідь на нетипові кризи (Weber, 1968) [28]. Сучасне теоретичне продовження вчення М.Вебера полягає у конструюванні моделі національної стійкості, яка зберігає принципи раціональної бюрократії як основи державності, але водночас доповнює їх механізмами організаційної, цифрової та соціальної адаптації, що забезпечує «життєздатність» національної держави в умовах гібридних, інформаційних і технологічних викликів.

Очевидно, що слід екстраполювати публічне управління за М.Вебером як раціонально організовану, ієрархічну та формалізовану систему реалізації політичної влади, у якій кожен рівень державного апарату діє на основі чітко встановлених норм, правил і інструкцій, забезпечуючи повторюваність, прогнозованість і професіоналізм у реалізації законів і рішень національної держави. Це логічно для класичних моделей суспільного управління (Л.Антонова) [31]. Проте сучасний зміст публічного управління характеризується іншими критеріями раціонального врядування, і авторське розуміння розширює обсяг суб'єктності, зміщуючи акцент із жорстких структур на динамічну взаємодію різних компонентів суспільства. Відповідно до цієї позиції, публічне управління розглядається як діяльність (складова суспільного управління), що забезпечує ефективне функціонування не лише органів державної влади, але й регіонального врядування, органів місцевого самоврядування, громадських (неурядових) організацій, фізичних осіб та інших суб'єктів громадянського суспільства з метою реалізації публічної (державної) влади.

У такій парадигмі національна стійкість тлумачиться не як результат жорстко законсервованої адміністративної дисципліни, а як інтегративна, мережево інтегративна властивість суспільства і держави, здатна до адаптації, самооновлення і партнерського розв'язання кризових викликів.

Основою такого бачення стає публічно-приватна та міжсекторальна взаємодія, розвитку горизонтальних зв'язків, залучення соціального капіталу та потенціалу громадянського суспільства для збалансованого функціонування національної системи в умовах складних викликів та змін.

Відтак національна стійкість у сучасному розумінні – це не лише збереження і відтворення адміністративних процедур, а насамперед здатність різних гравців публічного та громадянського секторів до коаліційних дій, гнучкого реагування, інституційної креативності й інновацій у політиці управління. Вона спирається на локальні ініціативи, децентралізацію, самоорганізацію громад та залучення громадян до розробки і реалізації рішень. Таким чином, мережева модель публічного управління створює підґрунтя для гнучкої національної стійкості, яка не лише витримує удари, а й активно трансформується для досягнення спільного блага (таблиця 1.2).

Таблиця 1.2

Порівняльний аналіз концепцій М.Вебера і сучасної інтегративної моделі
національної стійкості

Критерій / Модель	бюрократія М.Вебера	Сучасна інтегративна (мережева) модель
Суб'єкти публічного управління	Державний апарат, чиновники	Держава, місцеві органи, громадські організації, громадяни, бізнес
Структура управління	Ієрархічна, вертикальна	Горизонтальна, мережево-кооперативна
Підходи до прийняття рішень	Чіткі регламенти, інструкції, централізований контроль	Децентралізація, партнерство, участь зацікавлених сторін
Джерело стійкості	Законність, формалізовані процедури, професіоналізм, інерція	Адаптивність, взаємодія, гнучкість, кооперація
Роль громадянина	Адресат норм, підпорядкований об'єкт	Учасник процесу, суб'єкт ініціативи, партнер
Відношення до змін	Фокус на стабільності, слабка чутливість до змін	Орієнтація на інновації, відкритість до змін, гнучке реагування
Ризики/Обмеження	Формалізм, бюрократичний параліч, відчуження громадян	Можлива розмитість відповідальності, складність координації
Формат національної стійкості	Процедурна, «інерційна» стійкість	Кооперативна, динамічна, адаптивна стійкість

Джерело: узагальнено автором

Отже, сучасне осмислення національної стійкості, передбачає переосмислення класичних адміністративних моделей і акцентування на інтегративних типах управління. Там, де бюрократія М.Вебера є взірцем ієрархічної, формалізованої та закритої системи, що забезпечує стабільність виключно завдяки повторюваності процедур і контролю, інтегративна (мережева) модель виступає як відкрита, динамічна система, що спирається на багатосуб'єктну кооперацію та гнучке реагування..



Рис. 1.1. Формалізація сучасної національної моделі стійкості в системі публічного управління (концепт М.Вебера)

Джерело: розроблено автором.

В умовах гібридних загроз, що вимагають адаптивності та міжсекторальної гнучкості, модель М.Вебера демонструє значні системні

недоліки (таблиця 1.3).

Таблиця 1.3

Проблеми застосування концепції М.Вебера до формування
раціональної НМС

Джерело вразливості	Прояв дисфункції в кризі	Наслідок для резильєнтності
Нездатність процедур до гнучкості	Фетишизація правил як надмірна фіксація на правилах (т. зв. «бюрократичний патологізм») робить систему нездатною до швидкої адаптації та прийняття нестандартних рішень	Низька адаптивна стійкість, коли система не може швидко реагувати на непередбачувані загрози гібридної війни
Відсутність міжсекторальної взаємодії	Спеціалізація (вузька експертиза), при цьому «ідеальна бюрократія» не працює; нездатність до горизонтальної співпраці унеможливорює ефективне управління комплексними гібридними загрозами (інформація + економіка + політика)	Вразливість до комплексних загроз, обмежена здатність до системного аналізу
Елітарна ізоляція	Безособовість, ієрархія, відчуження чиновників від потреб суспільства та політичних процесів	Низька соціальна стійкість, зниження довіри суспільства до влади, що створює сприятливий ґрунт для колабораційної пропаганди та соціального розколу
Відсутність механізмів навчання	Формалізм, коли система призначена для повторення, а не для інновацій	Низька трансформаційна стійкість, нездатність використати кризу для якісної зміни та розвитку (навчання на помилках)

Модель М.Вебера пропонує чіткий поділ компетенцій, централізованість управлінських функцій і жорстку прив'язку до формалізованих норм. Це формує підґрунтя для процедурної (інерційної) стійкості: держава здатна зберігати керованість і впорядкованість навіть в умовах політичних коливань, проте стає малорухливою у відповідь на екстраординарні кризи чи вимоги до швидкої інновації. Громадянин у цій парадигмі найчастіше залишається підлеглим, адресатом рішень, відчуженим від процесу творення публічної політики.

Натомість, важливого значення набуває саме підхід (за С.Квіткою), що трактує публічне управління як діяльність (а не як статичну структуру), що інтегрує функціонування державних інститутів, органів місцевого самоврядування, неурядового сектору, бізнесу, громад і окремих громадян на паритетних та партнерських засадах [31]. Така модель забезпечує динамічну, кооперативну стійкість, яка ґрунтується на відкритості до змін, гнучкості процедур, залученні різноманітних ресурсів та участі громадянського суспільства у реалізації публічної політики. Національна стійкість в умовах сучасних загроз – це вже не механічне відтворення усталених алгоритмів, а здатність до консолідації, інновацій, локальної ініціативи, крос-секторальної взаємодії. У цій системі громадянин стає партнером, співтворцем, а не лише об'єктом управління. Таким чином, кооперативна, інтегративна модель не лише розширює палітру інструментів держави, а й підвищує її життєздатність через постійну адаптацію, що повною мірою відповідає сучасним концепціям *resilience* та *adaptive governance*. Саме таке порівняння дозволяє побачити якісну трансформацію природи публічного управління і національної стійкості від ригідної закономірності до мережевої, відкритої до змін і партнерства системи, де стійкість обумовлюється не лише стабільністю, але й здатністю до взаємодії, самооновлення та розвитку.

Важливим складником формування національної моделі стійкості виступає інтегративний аналіз нового публічного менеджменту, в межах ідеологем *«стійкість через ефективність та конкуренцію»*. Концепція нового публічного менеджменту (NPM), що набула поширення з 1980-х років під впливом робіт Д.Осборна [32], Г.Еллінека [33] та практик урядів М.Тетчер (Велика Британія) і Р.Рейгана (США) [34], запропонувала принципово інший погляд на стійкість управлінської системи на рівні національної держави. У цій парадигмі стійкість досягається не через бюрократичну стабільність, а через економічну ефективність, конкурентність та результативність. Адже NPM розглядає публічний сектор крізь призму ринкових механізмів. Ключовими елементами стійкості стають:

децентралізація прийняття рішень, впровадження квазіринкових механізмів у публічному секторі, орієнтація на вимірювані результати діяльності, контрактні відносини, професійний менеджмент. Як зазначав К.Гуд у своїй фундаментальній праці «A Public Management for All Seasons?», стійкість системи визначається не її здатністю зберігати процедури, а здатністю досягати визначених цілей з мінімальними витратами [13].

У межах концепції NPM публічне управління інтерпретується не як класична бюрократична система, а як різновид «квазі-ринку», у якому органи державної влади, комунальні структури, приватні та неприбуткові організації функціонують за логікою бізнесу. Центральний акцент переноситься з процедурної впорядкованості на ефективність, результативність, продуктивність та скорочення витрат. Для національної стійкості це створює важливий позитивний потенціал: система управління стає більш економною, оптимізованою, орієнтованою на досягнення конкретних результатів, що є критично значущим за умов дефіциту ресурсів, кризових станів економіки чи воєнного часу. Водночас, надмірне підпорядкування публічного управління логіці бізнес-ефективності несе ризик редукції публічних цілей до вузьких фінансових показників. У такому випадку виникає загроза маргіналізації або ігнорування довгострокових соціальних ефектів, питань суспільної згуртованості, довіри, національної ідентичності та безпеки, які не завжди піддаються безпосередньому виміру у форматі короткострокових KPI. Отже, NPM підвищує гнучкість та економічну раціональність, але вимагає додаткового теоретичного балансування з категоріями публічної цінності та суспільного блага.

У класичних бюрократичних моделях джерелом стійкості виступають законність, формалізованість процедур і структурна інерційність інститутів. У парадигмі NPM, на нашу думку, джерело стійкості концептуалізується інакше: на перший план виходять ефективний менеджмент, конкуренція між провайдерами послуг, контрактні механізми, децентралізація функцій та організаційна гнучкість. Такий підхід корелює з потребою адаптації

публічного сектору до динамічного, мінливого середовища, коли з'являється спроможність швидко модифікувати формати послуг, змінювати організаційні конфігурації. Це посилює адаптивну складову національної стійкості, забезпечуючи інституціям спроможність реагувати на виклики шляхом переформатування, а не лише шляхом пасивного опору.

Разом з тим, посилення конкуренції та контрактних механізмів супроводжується ризиком фрагментації системи публічного управління. Умовною «ціною» підвищеної гнучкості стає ускладнення координації, особливо у кризових ситуаціях, коли виникає потреба в центрі прийняття рішень, узгодженості дій та інтегральній державній політиці (таблиця 1.4).

Таблиця 1.4

Формування національної моделі стійкості на основі принципів нового
публічного менеджмент (NPM)

Вимір / аспект	Характеристика в межах NPM	Потенціал для стійкості	Обмеження / ризики для стійкості
Природа публічного управління	Публічний сектор як «квазі-ринок»; управління за логікою бізнесу, фокус на ефективності та результатах	Підвищення продуктивності, скорочення витрат, стимул до оптимізації ресурсів	Ризик редукції публічних цілей до фінансових показників, ігнорування довгострокових соціальних наслідків
Джерело стійкості	Ефективний менеджмент, конкуренція, контрактні механізми, децентралізація	Гнучкі структури краще адаптуються до змін середовища, можливість швидкого переформатування послуг	Фрагментація системи, складність координації у кризах, потенційна втрата цілісності державної політики
Роль громадянина	«Клієнт» або «споживач» послуг, який обирає між альтернативними провайдером	Конкуренція за «клієнта» стимулює покращення якості послуг, орієнтацію на задоволеність громадян	Звуження громадянина до ролі споживача, недооцінка громадянства, участі та спільних цінностей
Інструменти та механізми	KPI, управління за результатами, аутсорсинг, приватизація, квазіринки, контрактний менеджмент	Забезпечують адаптивність, зменшують надмірну бюрократію, стимулюють інновації	Ризик «вимирання» неприбуткових, але соціально важливих функцій; уразливість під час криз, коли ринок не спрацьовує

Продовження таблиці 1.4

Вимір / аспект	Характеристика в межах NPM	Потенціал для стійкості	Обмеження / ризики для стійкості
Формат національної стійкості	Менеджеріальна стійкість: витривалість завдяки гнучким організаційним формам і результативності	Добре працює в умовах економічних коливань, глобальної конкуренції, необхідності швидко перебудовувати структури	Погано пристосований до «масштабних шоків», де потрібна централізована координація, солідарність і довіра

Джерело: узагальнено автором

Очевидно, що за відсутності належних механізмів стратегічного узгодження окремі організації можуть оптимізувати власні показники, не забезпечуючи цілісності національної політики та системної стійкості. Австралійська школа публічного управління (П. Кітінг, Дж. Волш) поглибила це розуміння, розробивши концепцію «управлінських контрактів» – механізму, який забезпечує стійкість через чітку відповідальність менеджерів за результати [35;36]. Європейська традиція NPM (К. Поллітт, Г. Букерт) додала до цієї моделі елементи «керованої конкуренції» [37], де стійкість досягається через диверсифікацію надавачів послуг – держава може делегувати функції приватному чи громадському секторам, зберігаючи роль стратега та координатора. У контексті національної стійкості NPM пропонує специфічне бачення: гнучкість організаційних структур, орієнтація на результат, а не процес, стратегічне планування та бюджетування за результатами створюють систему, здатну адаптуватися до змінних умов.

Проте у форматі сучасних комплексних викликів NPM виявляє суттєві обмеження щодо забезпечення стійкості. Надмірна фрагментація повноважень ускладнює координацію в кризових ситуаціях, а фокус на економічній ефективності може призводити до недооцінки соціальних ризиків та підриву довгострокової стійкості заради короткострокових результатів. У рамках NPM громадянин здебільшого позиціонується як «клієнт» або «споживач» публічних послуг, який здійснює раціональний

вибір між альтернативними провайдерами. Відповідно, відносини в системі «держава – індивід» осмислюються через призму сервісу, задоволеності послугами, можливості обирати й порівнювати.

Такий підхід має очевидний позитивний ефект: конкуренція за «клієнта» стимулює підвищення якості послуг, розвиток сервісної орієнтації, зростання чутливості публічних інститутів до індивідуальних потреб населення. Через це зміцнюється операційна складова національної стійкості: громадяни менше конфліктують із системою, якщо відчують її клієнтоорієнтованість, а рівень довіри до інституцій може зростати завдяки покращенню повсякденної взаємодії.

Водночас зведення ролі громадянина до статусу «клієнта» містить принципове обмеження (П.Скоурфілд, 2007). Громадянин у політичній спільноті є не лише споживачем послуг, а й носієм прав, обов'язків, цінностей, членом політичної нації. Орієнтація виключно на споживчу роль недооцінює вимір громадянської участі, спільної відповідальності й солідарності. У контексті національної стійкості це критично, адже готовність суспільства до колективної мобілізації, самопожертви й взаємодопомоги в умовах війни, катастроф або системних криз не може бути зведена до логіки вибору «кращого провайдера послуг». Таким чином, концептуалізація ролі громадянина в NPM потребує доповнення виміром громадянства як політичної, ціннісної та солідарної категорії, що безпосередньо впливає на стійкість національної спільноти.

У межах NPM формується специфічний тип національної стійкості, який можна позначити як менеджеріальну стійкість [39]. Її сутність полягає у здатності системи витримувати економічні та організаційні виклики за рахунок гнучкості структур, оптимізації витрат, реструктуризації організаційних форм, швидкого перепрофілювання або реорганізації надавачів послуг. Цей формат стійкості виявляється особливо ефективним за умов глобальної економічної конкуренції, бюджетних обмежень, структурних реформ і технологічних змін. Проте за масштабних викликів –

війна, гібридні загрози, масові міграції, системні руйнування інфраструктури, лише менеджеріальної логіки недостатньо. У таких ситуаціях критичного значення набувають: сильні центри координації й стратегічного управління; високий рівень суспільної довіри до інститутів; готовність населення до солідарних дій і самообмеження в інтересах спільного блага; наявність резервних потужностей і надлишкових (із вузькоекономічної точки зору – «неефективних») ресурсів. Отже, менеджеріальна стійкість, що формується внаслідок домінування NPM, є важливим, але частковим виміром національної резильєнтності та має бути доповнена іншими компонентами – безпековою, ціннісно-громадянською та мережево-кооперативною



Рис. 1.2. Формалізація сучасної національної моделі стійкості в системі публічного управління на основі NPM.

Джерело: розроблено автором.

Розвиток парадигми NPM засвідчив, що залучення ринкових і менеджерських механізмів до публічного сектору здатне істотно підвищувати його продуктивність, гнучкість та інноваційність. Водночас накопичення досвіду її практичної імплементації продемонструвало обмеженість вузько менеджерського бачення для забезпечення національної стійкості в умовах політичних, безпекових та цивілізаційних викликів. У цьому контексті стає актуальною подальша концептуалізація публічного управління як багатовимірної системи, де інструменти NPM інтегруються з підходами, орієнтованими на публічну цінність, мережеве (*collaborative*) врядування, резильєнтність та участь громадянського суспільства. Така інтеграція дозволяє поєднати менеджеріальну ефективність із довгостроковою здатністю національної спільноти до самоорганізації, солідарності та відновлення, що й має становити ядро сучасної концепції національної стійкості

Очевидним продовження наукового дескрипту раціональної платформи НМС виступає концепція належного врядування (Good Governance) – «стійкість через партнерство та включеність». На початку 2000-х років значну популярність здобула концепція належного врядування, яка переосмислює природу публічного управління як мережевого, партисипативного процесу. Концепція пропонує розуміння стійкості через призму інклюзивності, прозорості та горизонтальної взаємодії різних суспільних акторів. Основними елементами стійкості в концепції належного врядування виступають: верховенство права, транспарентність процесів ухвалення рішень, підзвітність влади, інклюзивність, орієнтація на консенсус, стратегічне бачення. Як зазначає Я.Кооіман у праці «Governing as Governance» [40], стійкість системи управління досягається не через ієрархію чи ринок, а через формування мереж співпраці між державою, громадянським суспільством та бізнесом.

Європейська школа врядування (Р. Роудз) [41] розвинула концепцію «мережевого врядування» (*network governance*), де стійкість забезпечується

через формування сталих горизонтальних зв'язків між різними учасниками процесу вироблення політики (Д.Стокер) [42]. У цій моделі держава втрачає монополію на прийняття рішень і стає модератором колективного процесу. Скандинавська традиція (Е.Соренсен, Дж. Торфінг) додала до цього розуміння концепцію «колаборативного врядування» – механізму, де стійкість базується на довірі, соціальному капіталі та спільних цінностях учасників [43-45].

У контексті національної стійкості концепція належного врядування пропонує особливе бачення: розподілена відповідальність, широка участь громадян, горизонтальна координація між секторами створюють систему, здатну витримувати різноманітні шоки саме завдяки своїй мережевій природі. Загалом, країни з розвиненими традиціями консенсусного ухвалення рішень та сильним громадянським суспільством виявляють вищу стійкість перед лицем криз – від фінансових до міграційних. Ця концепція, однак, також має свої обмеження в забезпеченні стійкості, особливо в умовах гострих безпекових загроз. Процеси досягнення консенсусу можуть бути надто тривалими в ситуаціях, що вимагають швидкої реакції, а розмивання відповідальності може призводити до проблем координації. Як зазначає Ф.Фукуяма, «надмірна інклюзивність може перетворюватися на паралізуючий фактор, коли система не здатна діяти рішуче через необхідність узгодження інтересів багатьох гравців» [46].

Належне / мережеве врядування концептуалізує публічне управління як систему взаємодії багатьох акторів – держави, бізнесу, неурядових організацій, місцевих громад, експертних спільнот та громадян. Ухвалення рішень у такій моделі розглядається не як виключна прерогатива ієрархічно організованого державного апарату, а як результат координації, переговорів і співдії різних сторін.

Таблиця 1.5

Належне врядування (Good Governance / Network Governance)

Вимір / аспект	Характеристика в межах належного / мережевого врядування	Потенціал для стійкості	Обмеження / ризики для стійкості
Природа публічного управління	Врядування як мережа акторів (держава, бізнес, НУО, громади); ухвалення рішень через взаємодію і координацію	Дозволяє залучити різні ресурси та знання, підвищити гнучкість і легітимність рішень	Може породжувати надмірну складність, розмитість відповідальності, «керованість без відповідальних»
Джерело стійкості	Партнерство, участь, прозорість, підзвітність, верховенство права	Соціальний капітал і довіра посилюють готовність суспільства самоорганізовуватись і підтримувати інституції під час криз	У суспільствах з низькою довірою мережі працюють гірше, є ризик захоплення процесів впливовими групами
Роль громадянина	Співучасник врядування, стейкхолдер, учасник консультацій і спільного ухвалення рішень	Зростає відчуття співвідповідальності й залученості, що робить суспільство більш стійким до зовнішніх впливів	Участь може бути формальною, обмеженою активною меншістю, що репрезентує не все суспільство
Інструменти та механізми	Громадські консультації, багаторівневе врядування, електронна демократія, політичні мережі	Створюють канали горизонтальної комунікації, дозволяють швидко мобілізувати «неурядові» ресурси в кризових умовах	Повільність ухвалення рішень у великих мережах, ризик блокування реформ через конфлікт інтересів
Формат національної стійкості	Мережево-інклюзивна стійкість: витривалість завдяки розподіленій відповідальності та включенню різних суб'єктів	Забезпечує гнучке реагування на поліструктурні кризи (економічні, соціальні, екологічні), де держава сама не може впоратися	У випадку військових/надзвичайних загроз може знадобитися більша централізація, ніж мережеві моделі здатні забезпечити
Представницькі школи / автори	Р.Роудз; європейська / скандинавська школа (Е.Сьоренсен, Дж. Торфінг)	Інституціоналізують принципи good governance як стандарт для оцінки якості державних інститутів та їхньої стійкості	Механізми доброго врядування часто залишаються декларативними без політичної волі й зрілих інститутів

Джерело: узагальнено автором на основі [41-45]

Водночас розгортання мережевого врядування породжує ризики надмірної складності конфігурацій взаємодії, розмитості відповідальності та ситуацій, коли фактично «керують усі й ніхто», що небезпечно з погляду чіткої відповіді на виклики безпеки й розвитку. Джерело стійкості в цій моделі переноситься з формальних процедур або суто менеджерських критеріїв ефективності на такі засади, як партнерство, участь, прозорість, підзвітність, верховенство права. Саме через ці параметри вибудовується соціальний капітал та довіра між громадянами й інститутами, а також між різними секторами. Довіра, у свою чергу, стає ключовою передумовою здатності суспільства до самоорганізації, взаємодопомоги й підтримки інституцій у кризових ситуаціях. Таким чином, національна стійкість у мережевому вимірі розуміється не лише як «міцність» державних структур, а як сукупна резильєнтність усієї мережі акторів. Утім, у контексті суспільств із низьким рівнем довіри, поляризацією чи клановістю, мережі ризикують перетворитися на інструмент захоплення процесів ухвалення рішень впливовими групами й відтворення нерівності доступу до ресурсів та впливу.

У такому підході принципово змінюється роль громадянина. Він уже не лише «клієнт» публічних послуг і не пасивний об'єкт адміністративного впливу, а повноправний співучасник врядування, стейкхолдер, залучений до консультацій, спільного формування політик, контролю за їх виконанням. Це сприяє формуванню відчуття співвідповідальності за суспільні результати, посилює готовність протидіяти загрозам, підтримувати колективні зусилля, а отже, зміцнює соціальну основу національної стійкості. Водночас участь далеко не завжди є інклюзивною: нерідко в процеси залучається відносно вузька, найбільш активна й ресурсна меншість, яка не репрезентує усього спектра суспільних груп. У такому випадку формальна наявність процедур участі може маскувати фактичну нерівність впливу та відтворювати відчуження частини населення.



Рис. 1.3. Формалізація сучасної національної моделі стійкості в системі публічного управління на основі НРМ.

Джерело: розроблено автором.

Формат національної стійкості, який формується в межах належного / мережевого врядування, можна охарактеризувати як мережево-інклюзивну стійкість. Її сутність полягає у розподіленій відповідальності та залученні різних акторів до вироблення й реалізації рішень. Це створює потенціал для гнучкого реагування на комплексні економічні, соціальні, екологічні й технологічні кризи, які виходять за межі компетенції однієї лише держави. У мирний і відносно стабільний період такий формат сприяє стійкому розвитку, підвищенню якості політик, зміцненню довіри. Водночас у ситуаціях

масштабних надзвичайних або військових загроз виникає потреба у швидкій централізації повноважень, чітких ланцюгах командування і персоналізованій відповідальності, що не завжди сумісно з логікою повністю мережевого врядування. Отже, мережеві підходи до належного врядування дають могутній ресурс для підвищення адаптивності та легітимності публічної влади, проте потребують поєднання з інструментами концентрації влади й ресурсів у критичних ситуаціях, аби забезпечити повноцінну національну резильєнтність.

Наступним виміром виступає «Новий публічний сервіс (*New Public Service*)», що реалізується у межах концепції «стійкість через служіння спільним цінностям». На початку XXI століття як відповідь на недоліки NPM і на потребу переосмислення ролі публічного управління в демократичному суспільстві виникла концепція нового публічного сервісу, розроблена Дж.Денхардтом, Б.Боземаном та іншими [48-51]. Ця парадигма розглядає стійкість управлінської системи через призму її здатності служити демократичним цінностям, суспільним інтересам та громадянській участі. Ключові компоненти стійкості в концепції нового публічного сервісу – служіння громадянам (а не клієнтам), пріоритет суспільних інтересів, цінність громадянства та громадянської участі, стратегічне мислення і демократичне врядування. Як стверджують Д.Денхардт у своїй праці «*The New Public Service: Serving, Not Steering*», стійкість системи публічного управління базується не на економічній ефективності чи процедурній раціональності, а на її здатності відображати та підтримувати демократичні цінності та публічні інтереси [47].

Американська школа публічної цінності (Б. Боземан) розвинула концепцію «публічної цінності» (*public value*) як центрального орієнтира для оцінювання стійкості системи управління [49-50]. У цій інтерпретації стійкість забезпечується здатністю інституцій створювати блага, які цінуються громадянами не лише як споживачами, а й як членами політичної спільноти. Європейська традиція (Х. де Врі [52-53], В. ван де Валле [54])

доповнила це розуміння концепцією «демократичної адміністративної етики», де стійкість базується на етичних принципах, що поділяються публічними службовцями та суспільством (таблиця 1.6).

Таблиця 1.6

Новий публічний сервіс (New Public Service, Public Value)

Вимір / аспект	Характеристика в межах нового публічного сервісу	Потенціал для стійкості	Обмеження / ризики для стійкості
Природа публічного управління	Управління як служіння громадянам та суспільству; акцент на публічній цінності, етиці, громадянстві	Посилює моральну легітимність держави, підвищує готовність громадян підтримувати інституції в кризах	Вимагає високої політичної культури та зрілого громадянського суспільства
Джерело стійкості	Спільні цінності, громадянська участь, відданість службовців публічній місії	Ціннісна консолідація суспільства робить його менш уразливим до пропаганди, поляризації, дезінформаційних атак	За відсутності базового ціннісного консенсусу модель може бути декларативною
Роль громадянина	Не лише клієнт, а повноправний громадянин, співтворець публічної цінності і політики	Підсилює відчуття відповідальності за спільне благо, сприяє самоорганізації та взаємодопомозі під час загроз	Частина населення може залишатися пасивною; активна меншість не завжди репрезентує спектр суспільних інтересів
Інструменти та механізми	Співтворення політик, громадянські форуми, етичні кодекси держслужби, орієнтація на публічну цінність	Формують культуру служіння, де службовець бачить свою роль у зміцненні спільноти, а не лише у виконанні формальних завдань	Важко формалізувати й виміряти публічну цінність, складно інтегрувати з «жорсткими» інструментами управління
Формат національної стійкості	Ціннісно-громадянська стійкість: витривалість через спільні цінності, довіру й участь	Допомагає зберігати єдність суспільства в умовах тривалих криз (війна, економічні проблеми), підтримує солідарність	За глибокої поляризації суспільства чи недовіри до еліт відтворення цієї моделі стає складним
Представницькі школи / автори	Дж. і Дж. Денхардт; М. Мур, Б. Боземан (публічна цінність); європейські дослідники (Х. де Врі, В. ван де Валле)	Розкривають, як демократичні цінності й орієнтація на громадянство можуть стати ядром довгострокової стійкості публічних інституцій	Критикуються прихильниками «жорсткіших» моделей за надмірний акцент на нормах та ідеалах без достатньої уваги до ресурсних обмежень

Джерело: [47-54]

У контексті національної стійкості концепція нового публічного сервісу пропонує особливе розуміння: система публічного управління витримує кризи не завдяки жорсткій ієрархії чи ефективним ринковим механізмам, а завдяки цінностям, що об'єднують громадян і публічних службовців, мотивуючи їх до кооперації та солідарної поведінки. Проте і ця концепція має обмеження в забезпеченні стійкості, особливо в умовах глибоких суспільних розколів. Ставка на спільні цінності та демократичний консенсус може виявитися недостатньою у країнах із низьким рівнем соціальної довіри або глибокою поляризацією. Як зауважує П. Розанваллон, «демократичне служіння потребує певного базового консенсусу щодо цінностей, який у багатьох суспільствах є радше ідеалом, ніж реальністю» [55]. Саме тому Новий публічний сервіс та пов'язана з ним концепція публічної цінності інтерпретують публічне управління насамперед як служіння громадянам і суспільству. Управлінська діяльність у такій оптиці має бути спрямована не лише на ефективність чи формальну законність, а на створення й підтримку публічної цінності – того, що посилює добробут, справедливість, безпеку, довіру й згуртованість політичної спільноти.

Це одразу зміщує акцент з «керування процесами» або «надання послуг клієнтам» до етичного виміру: управління мислиться як морально вкорінене служіння, пов'язане з ідеями громадянства, відповідальності й солідарності. Такий підхід підсилює моральну легітимність держави: громадяни сприймають інституції не як зовнішню силу, а як «свої», такими, що втілюють спільні цінності. В умовах криз це збільшує готовність населення підтримувати інститути влади, терпіти тимчасові обмеження, мобілізуватися на захист спільного блага. Водночас реалізація такої моделі потребує високої політичної культури, зрілого громадянського суспільства та відповідальної еліти.



Рис. 1.4. Формалізація сучасної національної моделі стійкості в системі публічного управління на основі Нового публічного сервісу

Джерело: розроблено автором.

Джерело стійкості в межах нового публічного сервісу й публічної цінності переноситься на спільні цінності, громадянську участь і відданість публічних службовців місії служіння суспільству. Суспільство, в якому існує базовий ціннісний консенсус щодо ключових орієнтирів (демократія, права людини, справедливість, верховенство права, національна незалежність), виявляється значно менш уразливим до пропаганди, поляризації, інформаційних операцій. У таких умовах навіть за зовнішнього тиску та тривалих потрясінь зберігається внутрішнє ядро ідентичності та взаємної довіри, яке й забезпечує довгострокову національну стійкість. Проте там, де

спільні цінності не сформовані чи радикально розколоті, будь-яке посилення на публічну цінність і громадянську місію держави може набувати суто декларативного характеру, не підкріпленого реальною поведінкою ані громадян, ані посадових осіб.

У цій моделі суттєво трансформується роль громадянина. Він уже не зводиться до статусу «клієнта» публічних послуг і не розглядається як пасивний об'єкт адміністрування. Громадянин – це повноправний учасник політичної спільноти, співтворець публічної цінності та публічної політики. Від нього очікується не тільки споживання послуг, а й участь у їх формуванні, контролі, оцінюванні; не лише вимога до держави «надати краще», а й готовність брати на себе частку відповідальності за спільні результати. Такий підхід посилює суб'єктність населення, формує відчуття співвідповідальності за спільне благо, сприяє самоорганізації, взаємодопомозі, волонтерству, локальним ініціативам – саме тим практикам, які є критично важливими для витримання тривалих воєн, економічних або гуманітарних криз. Однак не слід ідеалізувати цей процес: частина населення може залишатися пасивною, байдужою або дезорієнтованою; активна ж меншість, що інтенсивно взаємодіє з інституціями, не завжди репрезентує весь спектр суспільних інтересів, що породжує ризики нових дисбалансів.

Набір інструментів нового публічного сервісу й орієнтації на публічну цінність включає співтворення політик (co-production, co-creation), громадянські форуми, партисипативні практики, етичні кодекси державної служби, механізми оцінювання діяльності органів влади з точки зору публічної цінності, а не лише фінансових показників. У центрі – формування культури служіння, в якій публічний службовець сприймає себе не як «агента контракту» чи «гвинтика в ієрархії», а як відповідального носія публічної місії, що працює на зміцнення спільноти й національної спроможності. Такі інструменти сприяють внутрішній мотивації, професійній етиці, готовності діяти в інтересах суспільства навіть за умов невизначеності та браку формальних регламентів, що суттєво посилює стійкість інституцій у критичні

моменти. Разом із тим, публічну цінність складно строго формалізувати й виміряти; її важко без втрат інтегрувати в «жорсткі» системи бюджетування та управління, орієнтовані на кількісні показники. Це створює напругу між нормативно-ціннісним виміром управління і технократичною логікою ресурсних обмежень.

У підсумку формується специфічний формат національної стійкості, який можна описати як ціннісно-громадянську стійкість.

Ціннісно-громадянська стійкість – інтегральна характеристика стану й спроможності суспільства, що відображає збереження, відтворення та розвиток системи базових демократичних і конституційних цінностей, громадянської ідентичності та культури участі, які забезпечують легітимну підтримку інститутів публічної влади й готовність громадян до відповідальної участі у захисті, відбудові та модернізації держави в умовах тривалих криз, гібридних загроз і прискореної цифровізації.

У структурі національної моделі стійкості ціннісно-громадянська стійкість виступає її аксіологічно-громадянським виміром, що доповнює інституційну, безпекову, економічну та цифрову стійкість і забезпечує внутрішній ціннісний консенсус як передумову ефективного функціонування публічної влади. Її ядром є спільні цінності, довіра, почуття приналежності до політичної нації та готовність до участі. Така стійкість виявляється особливо важливою в умовах затяжних криз – воєн, тривалих економічних спадів, періодів глибоких соціальних трансформацій, коли матеріальні ресурси вичерпуються, а навантаження на інституції та суспільство триває роками. Саме ціннісно-громадянський вимір дозволяє зберігати єдність, солідарність і перспективу спільного майбутнього, попри втрати й виснаження..

Цифрове врядування (Digital Governance) як формат сучасного публічного управління – «стійкість через адаптивність і даталогічність». Найновішою з концепцій публічного управління є цифрове врядування, яке сформувалося протягом останнього десятиліття під впливом стрімкої

цифрової трансформації всіх сфер життя. Розроблена спільними зусиллями вчених (Дж. Фаунтейн, В. Майєр-Шенбергер, В. Дрекслер) та технологічних візіонерів (Т. О'Райлі, Б. Новек) [56-60], ця концепція пропонує розуміння стійкості через призму адаптивності, даталогічності та алгоритмічного прийняття рішень. Ключовими елементами стійкості в концепції цифрового врядування виступають: використання даних як стратегічного ресурсу, модульна архітектура управлінських систем, державні цифрові платформи, інтероперабельність даних і сервісів, превентивне реагування на потреби громадян. Як зазначає Б. Новек у праці «Smart Citizens, Smarter State», стійкість системи досягається через її здатність накопичувати, аналізувати та оперативно використовувати дані для ухвалення рішень, передбачення проблем та їх профілактики [60].

Естонська школа електронного урядування (Т.Котка) розвинула концепцію «цифрової стійкості» (digital resilience), де здатність системи відновлюватися після криз безпосередньо пов'язана з цифровою зрілістю її управлінських процесів [61]. Ключовим механізмом тут виступають цифрові бекапи держави – від розподіленого зберігання реєстрів до «цифрових посольств» (data embassies), які забезпечують безперервність навіть у випадку фізичної окупації території. Сінгапурська традиція (К. Чуа) додала до цього розуміння концепцію «розумної нації» (Smart Nation) [62;63], де стійкість досягається через інтеграцію фізичної та цифрової інфраструктури, створення інформаційного простору, що об'єднує державу, громадян і бізнес.

У контексті національної стійкості концепція цифрового врядування пропонує революційне бачення: система публічного управління, побудована як мережа взаємопов'язаних цифрових платформ, здатна не лише реагувати на кризи, але й передбачати їх, адаптуватися в реальному часі, автоматично перерозподіляти ресурси відповідно до потреб. Досвід Естонії, Південної Кореї та Сінгапуру демонструє, що країни з високим рівнем цифровізації публічного сектору виявляють кращу здатність протистояти різноманітним загрозам – від кібератак до пандемій.

Таблиця 1.7

Публічне управління у форматі цифрового врядування (Digital
Governance / e-Governance)

Вимір / аспект	Характеристика в межах цифрового врядування	Потенціал для стійкості	Обмеження / ризики для стійкості
Природа публічного управління	Управління як цифрова екосистема; держава як платформа, що інтегрує дані, сервіси й учасників	Забезпечує швидкість, масштабованість, інтегрованість рішень, можливість цілісного бачення ситуації в реальному часі	Ризик надмірної технократизації, коли «цифра» підміняє політичний і ціннісний вимір управління
Джерело стійкості	Дані, алгоритми, інтероперабельність систем, цифрова інфраструктура, резервування (backup)	Прогнозування загроз, автоматична адаптація сервісів, забезпечення безперервності функцій при фізичних руйнуваннях	Залежність від ІТ-інфраструктури, вразливість до кібератак, складність захисту приватності та персональних даних
Роль громадянина	Користувач цифрових сервісів, джерело даних, співучасник цифрової взаємодії	Полегшує доступ до послуг, підвищує прозорість, розширює можливості участі (e-democracy), зменшує транзакційні витрати	Частина населення виключена через цифровий розрив (відсутність доступу, навичок, довіри до ЦІ)
Інструменти та механізми	Державні цифрові платформи, реєстри, API, аналітика Big Data, ІІІ, цифрові ідентичності	Створюють каркас «цифрової стійкості»: автономність, відмовостійкість, можливість швидкого масштабування програм підтримки	Помилки в даних або алгоритмічні упередження масштабуються системно; нові форми нерівності чи несправедливості
Формат національної стійкості	Цифрово-адаптивна стійкість: резильєнтність завдяки даталогічності й можливості адаптації в реальному часі	Дозволяє забезпечити безперервність державних функцій навіть в умовах війни, катастроф, епідемій; підтримує проактивні моделі послуг	Без належного правового, етичного регулювання цифрова держава може перетворитися на інструмент надмірного контролю
Представницькі школи / автори	Дж. Фаунтейн, В. Майєр-Шенбергер, Б. Новек; естонська школа (Л. Віік, Т. Котка); сингапурська Smart Nation	Демонструють, як цифровізація може стати ядром моделі нац. стійкості (цифрові посольства, інтегровані реєстри, смарт-інфраструктура)	Критика (Є. Морозов та ін.): небезпека редукції складних суспільних проблем до технічних завдань, ризик «цифрового авторитаризму»

Джерело: [61-63].

Очевидно, що цифрове врядування інтерпретує публічне управління як цілісну цифрову екосистему, у якій держава функціонує як платформа, що інтегрує дані, сервіси й різноманітних учасників – органи влади, бізнес, громадян, громади, міжнародних партнерів. Такий підхід дає змогу переходити від розрізнених, фрагментованих процесів до інтегрованих рішень, які приймаються на основі актуальних даних у режимі, наближеному до реального часу. Це суттєво підвищує швидкість реагування, масштабованість управлінських рішень і здатність бачити «загальну картину» під час криз – від міграційних хвиль до масованих атак. Водночас існує ризик надмірної технократизації, коли цифрові платформи та алгоритми починають витісняти політичний і ціннісний вимір управління: замість дискусії про смисли та пріоритети домінує логіка технічної оптимізації, що потенційно послаблює демократичну рефлексію й суспільний контроль.

Джерело стійкості в цій моделі зміщується до даних, алгоритмів, інтероперабельності інформаційних систем, цифрової інфраструктури й механізмів резервування (backup). Стійкість забезпечується не лише міцністю фізичних об'єктів, а й здатністю систем даних переживати фізичні руйнування, автоматично відновлюватися, переключатися на резервні майданчики (наприклад, «цифрові посольства») та підтримувати безперервність критичних сервісів. Аналітика великих масивів даних, моделювання сценаріїв, використання штучного інтелекту створюють можливість прогнозувати загрози, виявляти вразливості, адаптувати сервіси до змінних умов до того, як криза набуде повної сили. Однак посилення залежності від ІТ-інфраструктури означає підвищену вразливість до кібератак, технічних збоїв, збоїв енергопостачання, а також постійні виклики у сфері захисту приватності та персональних даних. Без розвинених механізмів кібербезпеки та надійного регуляторного середовища цифрова стійкість може перетворитися на цифрову вразливість (рис.1.5).



Рис. 1.5. Формалізація сучасної національної моделі стійкості в системі публічного управління на основі концепту цифрового врядування

Джерело: розроблено автором.

У цифровому врядуванні змінюється і роль громадянина. Він виступає як користувач цифрових сервісів, джерело даних (у тому числі через повсякденну цифрову активність) і співучасник цифрової взаємодії з державою. Це радикально знижує транзакційні витрати: доступ до послуг спрощується, часові й фінансові витрати скорочуються, зростає прозорість процедур, відкриваються додаткові канали участі – від електронних петицій до онлайн-консультацій і голосувань. Такі механізми можуть зміцнювати довіру і посилювати залученість, якщо люди відчувають реальну

ефективність та справедливість цифрових інструментів. Водночас частина населення неминуче залишається «за бортом» через цифровий розрив: обмежений доступ до Інтернету, відсутність технічних засобів, недостатні цифрові навички, низький рівень довіри до онлайн-інструментів або страх перед їх використанням. Це створює ризик нових ліній нерівності та сегрегації – між «цифрово включеними» та «цифрово виключеними» громадянами.

Інструментально цифрове врядування спирається на державні цифрові платформи, реєстри, API для інтеграції різних систем, аналітику Big Data та засоби штучного інтелекту, системи електронної ідентифікації та цифрові підписи. Усе це формує каркас «цифрової стійкості» – здатність системи працювати автономно, з високою відмовостійкістю, а також швидко масштабувати програми підтримки населення й бізнесу, запускати нові сервіси у відповідь на кризу (наприклад, виплати допомоги, евакуаційні сервіси, системи оповіщення). Водночас, якщо вихідні дані містять помилки або алгоритми відтворюють приховані упередження, ці вади можуть масштабуватися до рівня всієї системи, породжуючи нові форми несправедливості: нерівний доступ до послуг, дискримінаційні практики ухвалення рішень, вибіркове «виключення» певних груп. У таких випадках технологічна ефективність не лише не підсилює стійкість, а й підриває її, оскільки підточує довіру до держави та відчуття справедливості.

У підсумку формується специфічний формат національної стійкості, який можна окреслити як цифрово-адаптивну стійкість. Її сутність полягає у здатності системи завдяки даним, алгоритмам і мережевим інфраструктурам адаптуватися в режимі реального часу, забезпечувати безперервність ключових функцій навіть в умовах війни, природних катастроф, епідемій чи масштабних техногенних інцидентів. Цифрові інструменти дозволяють переходити до проактивних моделей надання послуг, коли держава сама ідентифікує потреби громадян і бізнесу та ініціює відповідні сервіси. Однак без належного правового, етичного та інституційного врегулювання цифрова

держава ризикує перетворитися на інструмент надмірного контролю й нагляду, де масове збирання даних, алгоритмічна обробка та інтегровані реєстри стають ресурсом не лише для стійкості, а й для потенційного цифрового авторитаризму. Тому цифрове врядування може стати потужним ядром моделі національної стійкості лише за умови, що воно вбудоване в ширшу рамку демократичних цінностей, прав людини, публічної підзвітності та ціннісно-громадянської консолідації.

Втім, і ця концепція має обмеження в забезпеченні стійкості, особливо в умовах цифрової нерівності та технологічних вразливостей. Надмірна залежність від цифрових систем може створювати нові ризики для стійкості – від вразливості до кібератак до виключення з процесу громадян, що не мають доступу до технологій чи навичок їх використання.

1.2. Формування національної моделі державотворчих процесів в Україні на основі проблемного підходу: стійкість як багатовимірний феномен

Проведений аналіз дозволяє сформулювати інтегративне розуміння стійкості системи публічного управління як багатовимірного феномену. Стійкість постає не як статична характеристика, а як динамічна здатність системи підтримувати функціональність, адаптуватися до змін і відновлюватися після криз, зберігаючи при цьому свою ідентичність та здатність служити суспільним інтересам. Стійкість публічного управління як суспільного феномену включає в себе кілька взаємопов'язаних вимірів:

- 1) інституційна стійкість – як здатність формальних структур і правил зберігати функціональність навіть при зміні керівництва чи зовнішніх умов;
- 2) економічна стійкість – як здатність ефективно використовувати ресурси та адаптуватися до економічних шоків;
- 3) соціальна стійкість – як здатність підтримувати довіру, легітимність і соціальний капітал;
- 4) ціннісна стійкість – як здатність зберігати відданість

фундаментальним принципам і цінностям навіть у кризових ситуаціях;

5) технологічна стійкість – як здатність використовувати цифрові технології для забезпечення безперервності функціонування та адаптації до змін.

У цьому контексті найбільш перспективним виглядає синтетичний підхід, який би інтегрував сильні сторони різних концепцій публічного управління. Такий підхід передбачає побудову системи, яка поєднує: процедурну чіткість моделі М.Вебера [28]; економічну раціональність і орієнтацію на результати нового публічного менеджменту; мережеву організацію та партисипативність концепції належного врядування; ціннісну орієнтацію та служіння суспільству нового публічного сервісу; даталогічність і адаптивність цифрового врядування. Як підкреслює Н.Луман, стійкість – це не просто здатність системи повертатися до вихідного стану після кризи, а скоріше її здатність еволюціонувати, зберігаючи свою ідентичність і підвищуючи здатність до адаптації [64]. У цьому сенсі найбільш стійкі системи публічного управління – це ті, що здатні постійно навчатися, переосмислювати свої практики та інтегрувати різноманітні підходи до організації взаємодії держави та суспільства. Таке розуміння має особливе значення в контексті сучасних комплексних викликів, з якими стикаються національні держави: від зміни клімату та пандемій до гібридних воєн і технологічних революцій. Воно дозволяє не протиставляти різні теоретичні підходи до публічного управління, а розглядати їх як взаємодоповнюючі перспективи, що висвітлюють різні грані єдиного феномену – здатності соціальної системи до самоорганізації та адаптивного розвитку в умовах постійних змін.

Проблемний підхід, покладений в основу дослідження, передбачає, що українську модель державотворення доцільно описувати не як абстрактну «ідеальну» конструкцію, а як сукупність конкретних проблемних полів, у межах яких проявляється стійкість або вразливість системи. Такі дослідницькі поля – це, зокрема, забезпечення конституційного ладу та

територіальної цілісності, відновлення й відбудова, соціальний захист і інтеграція ветеранів, протидія корупції, забезпечення рівного доступу до послуг, подолання цифрового розриву, збереження демократичних свобод в умовах воєнного стану, інтеграція в європейський правовий та цифровий простір [65]. Кожне з них має свої специфічні загрози та ресурси, що вимагає диференційованих управлінських рішень, але водночас усі вони взаємопов'язані через спільну інституційну, ціннісну та цифрову рамку.

У сучасних умовах державотворчі процеси в Україні розгортаються у просторі багатовимірних загроз і трансформацій, де класичні уявлення про стабільність держави як про «міцність» інститутів дедалі частіше виявляються недостатніми. Посилення зовнішньополітичного тиску, тривала війна, гібридні загрози, внутрішня поляризація, хронічна незавершеність реформ та квазі-реформи, що змінюють форми, але не завжди торкаються змісту інститутів, висувають на перший план питання національної стійкості як інтегральної характеристики державності. У цьому контексті конституційні зміни постають не лише як юридико-технічний інструмент адаптації Основного Закону до нових суспільних реалій, а як лакмусовий папірець глибших процесів – спроможності української політичної спільноти виробляти, утримувати й відтворювати національну модель стійкості в форматі тривалого державотворення.

Аналіз українського досвіду конституційних змін свідчить, що вони переважно здійснювалися як реакція на кризи, а не як елемент довгострокової державотворчої стратегії [66]. Часті ревізії балансу повноважень між Президентом, Урядом і Парламентом, трансформації виборчої системи, непослідовне перерозподілення компетенцій між центральною владою та місцевим самоврядуванням свідчать про незавершеність інституційної архітектури та відсутність сталих «несучих конструкцій» політичної системи. Цей стан великою мірою обумовлений тим, на що слушно вказують вітчизняні дослідники: незформованістю структур влади, дефіцитом професійних кадрів, спроможних до самостійного

прийняття управлінських рішень і забезпечення їх реалізації, відсутністю історичного досвіду швидкого переходу від авторитарного до демократичного управління без глибоких деформацій інститутів (Г.Зеленько) [67-68]. У таких умовах національна стійкість не може бути зведена до статичної стабільності конституційного тексту чи жорсткості владної вертикалі. Йдеться про здатність держави й суспільства одночасно зберігати базові константи ідентичності, правопорядку та політичного ладу і при цьому адаптуватися до динамічних внутрішніх та зовнішніх змін, відновлюватися після потрясінь, навчатися на власному досвіді, трансформувати інститути так, щоб вони краще відповідали реальним викликам.

Саме такий підхід до стійкості як до резильєнтності пропонується сучасними теоріями публічного управління й національної безпеки, які розглядають державу не як замкнену ієрархічну машину, а як складну, відкриту систему, що функціонує через взаємодію різноманітних акторів, цінностей та інфраструктур (Р.Роуз) [28]. Якщо звести множину чинників, що визначають якість і результативність державотворчих процесів в Україні, до кількох базових вимірів, стає можливим виокремити ті «осьові» параметри, які пояснюють більшу частину варіативності стану системи.

Перший із них – *конституційно-правовий вимір*. Йдеться не лише про текст Конституції як такий, а про спосіб, у який конституційні норми закріплюють розподіл владних повноважень, визначають межі дискреції органів влади, захищають права і свободи громадян, установлюють механізми участі та підзвітності [68;69]. Уразливість цього виміру в Україні пов'язана як із частими змінами Основного Закону, так і з розривом між декларованими принципами й реальною практикою їх імплементації. Стійкість тут означає не догматичну незмінність конституційного тексту, а передбачуваність і легітимність процедур його корекції, відповідність змін фундаментальним правовим і демократичним засадам, участь громадян у процесі конституційного творення, вбудованість норм у ширші міжнародно-правові рамки.

Другий вимір – *інституційно-управлінський*, що охоплює організацію системи органів державної влади, їхню спроможність до координації, професійну якість публічної служби, стабільність і послідовність політик, здатність реагувати на кризи без руйнування базових функцій. Тут показовими є міркування теоретиків мережевого врядування, які трактують сучасну державу як вузол у мережі взаємодії з бізнесом, громадами, неурядовими організаціями, міжнародними інституціями (Р.Роуз, Д.Вудс) [28;70]. З їхньої перспективи, стійкість інституцій досягається не лише через формальні повноваження, а й через здатність органів влади вбудовуватися у ширші мережі, координувати множину акторів, забезпечувати прозорість, відкритість і взаємну відповідальність. Українська реальність демонструє, що кадрова слабкість, політична фрагментація, квазі-реформи, які змінюють вивіски без істотної трансформації практик, знижують саме цю інституційну резильєнтність, роблять систему залежною від особистісного фактору й кон'юнктурних політичних рішень.

Третій вимір – *політико-ціннісний*, пов'язаний із рівнем політичного консенсусу щодо базових засад державності, європейського курсу, прав і свобод людини, бачення майбутнього політичної спільноти. Концепція Нового публічного сервісу та публічної цінності, , підкреслює, що без ціннісної консолідації суспільства й орієнтації публічної влади на служіння громадянам, а не на обслуговування вузьких групових інтересів, жодна інституційна архітектура не буде довготривало стійкою (Дж.Денхардт, Б.Боземан) [47-50]. Для України це особливо виразно проявляється у взаємозалежності між дефіцитом політичного консенсусу й посиленням ролі глави держави: суспільство, яке не має достатньо усталеного бачення спільного майбутнього, схильне переносити свої очікування на фігуру лідера, одночасно посилюючи й уразливість системи. Національна модель стійкості в такому разі має спиратися на поглиблення громадянської участі, розвиток політичної культури, укорінення демократичних норм у повсякденних практиках, що зменшує потребу в компенсаторній персоніфікації влади.

Четвертий вимір – цифрово-інфраструктурний, який за останні роки перетворився на один із ключових для підтримання безперервності державних функцій в умовах війни та надзвичайних ситуацій. Цифрове врядування більше не є другорядним технічним інструментом, а стає структурною опорою державності (Б.Новек) [60]. Держава як цифрова платформа, що інтегрує реєстри, сервіси, аналітичні системи, дозволяє забезпечити доступність послуг, підтримувати керованість і комунікацію з громадянами навіть за умов фізичних руйнувань інфраструктури, міграції населення, зміни лінії фронту.

Для української моделі стійкості цифрова екосистема держави – це не лише зручність і ефективність, а й питання виживання: можливість зберігати дані, ідентичності, реєстрові записи, соціальні гарантії у безпечних середовищах, у тому числі через механізми «цифрових посольств» та міжнародні хмарні рішення. Водночас, справедливою є критика технократичного «солюціонізму», про небезпеки якого попереджає Є.Морозов, коли редукція політичних і соціальних проблем до набору технічних завдань, ризик цифрового авторитаризму, загрози приватності та правам людини в умовах розбудови потужних інформаційних систем. Слід виокремити розвінчання міфу про те, що інтернет автоматично демократизує суспільство. Він показує, як авторитарні режими (Росія, Китай) використовують мережу для стеження та придушення інакомислення, посилюючи стійкість режиму, а не суспільства. Так само дослідник критикує ідею, що складні соціальні проблеми (як стійкість суспільства) можна вирішити за допомогою «розумних алгоритмів» та гаджетів. Є.Морозов стверджує, що це веде до деполітизації та втрати демократичного контролю [71;72]. Тому цифровий вимір національної стійкості має бути жорстко вбудований у правову та ціннісну рамку, забезпечений демократичними механізмами контролю й підзвітності.

П'ятий, невід'ємний вимір – міжнародно-мережевий, який стосується вбудованості України в європейські та глобальні регіональні структури,

режими колективної безпеки, економічні та правові простори. Зовнішньополітична діяльність, конституційно закріплений курс на інтеграцію до ЄС і Євроатлантичного простору мають розглядатися не лише як зовнішній вектор, а як елемент внутрішньої моделі стійкості. Участь у міжнародних інституціях, імплементація європейських стандартів верховенства права, прав людини, державного управління створюють для України не тільки нові зобов'язання, а й потужні механізми самозахисту від внутрішньої деградації, корупції, авторитарного відкату. У такій перспективі як вважає В.Баштанник, конституційні норми, які визначають зовнішньополітичний курс, виступають «якорями стійкості», обмежуючи простір для ситуативних ревізій, пов'язаних із кон'юктурою чи зміною еліт, і водночас інтегруючи національну модель у ширшу архітектуру європейської безпеки й розвитку [73-75]. Це корелює з позицією професора О.Руденко, автором і розробником методологічного концепту безпекової взаємодії [76-80].

Внесок професора О.Руденко полягає у концептуальному обґрунтуванні того, що євроінтеграція та участь у міжнародних інституціях є не лише зовнішньополітичним курсом, а й елементом внутрішньої моделі публічної стійкості держави. Праці дослідниці спрямовані на концептуалізацію теорії публічної стабільності, аналіз трансформації системи публічного управління під впливом Угоди про асоціацію з ЄС та проекту «Східне партнерство». Це дозволяє інтерпретувати інтеграційні процеси як інституційні механізми самозахисту – через імплементацію європейських стандартів верховенства права, прав людини, належного врядування та екологічної безпеки.

Окремим напрямом її наукового доробку є дослідження європейської публічної адміністрації, державної політики у сфері національної та суспільної безпеки, а також публічного управління в країнах-членах ЄС, де європейські норми розглядаються як рамки для підвищення стійкості українських інститутів до корупції, неефективності та авторитарної

рефлексії. О.Руденко практично втілює міжнародно-мережевий вимір – вибудовуючи фахові зв'язки між українськими й європейськими академічними та експертними середовищами, сприяючи запровадженню стандартів ЄС у сфері публічного управління й адміністративних реформ. Орієнтація О.Руденко на європейські критерії якості додатково посилює ефект «вбудованості» України в європейський науковий і професійний простір, підтримуючи розвиток внутрішніх інституційних механізмів стійкості через інтеграцію в глобальні мережі знань і практик

Синтез вимірів вітчизняних та зарубіжних науковців дозволяє говорити про національну модель стійкості як про центральний структурний елемент державотворчих процесів. На нашу думку, саме ця модель, а не сукупність розрізнених реформ, визначає, чи здатна Україна в умовах тривалих потрясінь утримувати легітимний конституційний лад, забезпечувати функціонування інститутів, захищати права своїх громадян, проводити послідовний європейський курс, зберігати соціальну згуртованість та перспективу розвитку. Формування такої моделі вимагає не просто перенесення чужих інституційних шаблонів, а глибокого наукового аналізу власних проблемних полів – взаємодії конституційних змін і політичних криз, механізмів реагування на інституційні альтерації, впливу квазі-реформ на довіру до влади, ресурсного забезпечення публічних політик, соціальних і історичних джерел української державності (О.Резнікова) [81-82].

Важливо наголосити, що професор О.Резнікова робить ключовий внесок у формування українського варіанту концепту національної стійкості. Авторка інтегрує загальну теорію систем, *resilience thinking* і безпекові студії, пропонує міждисциплінарне визначення національної стійкості як здатності держави й суспільства зберігати основні функції та розвиватися під впливом криз. Вона окреслює відмінність стійкості від безпеки й стабільності, моделює систему забезпечення стійкості, описує її суб'єктів, об'єктів, принципи, критерії та показники, взаємодію із системою нацбезпеки. Значущим є розроблений інструментарій: багаторівнева модель оцінювання

ризиків, механізми адаптивного управління, організаційні рішення. На основі аналізу практик НАТО, ЄС, ООН та окремих держав О.Резнікова пропонує концептуальні й нормативні засади створення національної системи стійкості в Україні, фактично закладаючи теоретичний і прикладний каркас відповідної державної політик [81].

У такому контексті сучасна методологія теорії науки державного управління набуває ролі не лише описової, а й конструктивної ролі, завдання якої полягає у виявленні головних структурних вимірів національної стійкості, оцінці їх взаємодії, розробленні теоретико-методологічних засад цілеспрямованого державного впливу на суспільні процеси в межах конституційних повноважень і демократичних процедур (рис.1.6).



Рис.1.6. Інтегрована модель національної стійкості (National E-Resilience) як інституціональна платформа державотворчих процесів

Саме через таке осмислення можливо перейти від хаотичного реагування на кризи до свідомого конструювання національної моделі державотворчих процесів, у центрі якої – не лише прагнення до стабільності як відсутності змін, а стійкість як здатність змінюватися, зберігаючи внутрішній дизайн системи. У межах нашого підходу інтегрована модель національної стійкості (National E-Resilience) розуміється як інституціональна платформа державотворчих процесів. Стійкість розглядається як багатовимірний феномен, який неможливо звести ані до економічних показників, ані до однієї лише військової спроможності чи «правильної» інституціональної конструкції, й при цьому вона має нормативно-ціннісний, інституційний, правовий, інфраструктурно-технологічний, інформаційно-аналітичний, сервісний, громадянський, безпековий та міжнародно-мережевий виміри. Ці виміри по-різному артикулюються в різних теоріях врядування (як показав аналіз), але саме їх взаємодія визначає, наскільки здатна держава й суспільство не лише витримувати удари, а й навчатися, адаптуватися і трансформуватися в умовах зовнішніх викликів.

Умовою успішної державотворчої стратегії для України стає інтеграція цифрового виміру в цю багатовимірну структуру стійкості (Є.Бородін, О.Поступна) [83]. Цифрова держава не може розглядатися лише як технологічне доповнення до «традиційної» моделі, адже така держава радикально змінює способи фіксації прав і обов'язків, формує нові канали взаємодії владних інститутів із громадянами (Л.Антонова), створює нові механізми впливу та контролю, а також відкриває доступ до зовнішніх ресурсів і партнерств [84]. Для України, де цифрові сервіси стали одним із ключових інструментів підтримки управлінської спроможності в умовах повномасштабної війни, критично важливо осмислити цифрове врядування саме як елемент національної моделі державотворення, а не лише як окремий напрямок модернізації.

У цьому контексті наведена нами характеристика екосистеми

цифрового врядування в Україні виконує роль аналітичної рамки, що дозволяє конкретизувати, як саме різні рівні цифрової держави – від цінностей і права до інфраструктури, даних, сервісів, громадянської участі, безпеки та міжнародних мереж – взаємодіють між собою й задають конфігурацію стійкості (таблиця 1.8).

Таблиця 1.8

Екосистема цифрового врядування на основі авторського концепту

Рівень / компонент	Роль у формуванні національної моделі державотворчих процесів (проблемний підхід)	Внесок у стійкість як багатовимірний феномен
Нормативно-ціннісний вимір цифрової держави	Визначає, які саме суспільні проблеми держава вважає пріоритетними для цифрових рішень (безпека, справедливість, інклюзія, відновлення після війни), і якими цінностями керується при цифровізації державотворчих процесів	Формує ціннісне ядро стійкості: цифрові інструменти підпорядковуються демократичним нормам, правах людини, принципам довіри та солідарності, а не лише логіці технічної ефективності
Інституційне забезпечення цифрового державотворення	Визначає архітектуру органів влади, відповідальних за цифрову трансформацію (центральні органи, координаційні структури, регіональний рівень), та їхню здатність колективно вирішувати комплексні проблеми державотворення	Забезпечує організаційну стійкість: спроможність інститутів адаптуватися, зберігати керованість і наступність політики в умовах кризи, ротацій кадрів, воєнних загроз
Правовий та регуляторний контур цифрового врядування	Створює нормативні рамки для використання даних, е-сервісів, кіберзахисту, е-ідентифікації, що перетворюють цифрові рішення з «пілотних проєктів» на сталу частину державотворчої моделі	Підсилює правову стійкість: гарантує захист прав громадян, передбачуваність правил, баланс між безпекою, приватністю та відкритістю даних
Цифрова інфраструктура та критичні платформи	Забезпечує базу для безперервного функціонування інститутів держави (реєстри, сервіси, зв'язок) навіть за умов фізичних руйнувань, переміщення органів влади, релокації бізнесу та населення	Підтримує інфраструктурну та технологічну стійкість: зменшує залежність від території, дає можливість відновлювати функції держави, спираючись на резервні майданчики та хмарні рішення
Дані та інтероперабельність як ресурс державотворення	Уможливають проблемно-орієнтований аналіз: виявлення реальних розривів у послугах, нерівності, вразливих територій і груп населення, моніторинг ефективності реформ у різних сегментах державотворчих процесів	Формують інформаційну стійкість: держава здатна бачити повну картину, швидко виявляти нові ризики, коригувати політики, зменшуючи простір для маніпуляцій та дезінформації

Продовження таблиці 1.8

Рівень / компонент	Роль у формуванні національної моделі державотворчих процесів (проблемний підхід)	Внесок у стійкість як багатовимірний феномен
Алгоритмічний та аналітичний рівень (Big Data, III)	Забезпечує інструменти прогнозування, моделювання сценаріїв відбудови, демографічних зрушень, економічної динаміки, що дає змогу будувати державотворчі стратегії як відповідь на конкретні, емпірично верифіковані проблеми	Підсилює проактивну стійкість: держава не лише реагує на кризи, а й передбачає їх, тестує політики «на моделі», знижуючи ризики помилкових рішень у критичних сферах
Цифрові публічні сервіси як інструмент державотворення	Переводять ключові державотворчі процеси (реєстрація, соціальний захист, підтримка ветеранів, відбудова, вибори, участь громад) у цифровий формат, роблячи їх доступними, масовими й прозорими	Зміцнюють функціональну стійкість: забезпечують безперервність надання послуг, скорочують корупційні ризики, підвищують довіру до інститутів через прозорість і простоту взаємодії
Громадяни та громади як суб'єкти цифрового державотворення	Залучають громадян, місцеві громади, волонтерські й експертні спільноти до виявлення проблем, спільного проектування цифрових рішень, контролю за їх реалізацією; перетворюють їх із «користувачів» на співтворців державної політики	Посилюють соціальну та громадянську стійкість: розвивають здатність суспільства до самоорганізації, взаємодопомоги, спільного вирішення проблем у кооперації з державою
Безпека, кібероборона та безперервність управління	Інтегрують кіберзахист, резервування, кризове управління в загальну модель державотворення, де збереження керованості та довіри до інститутів стає першочерговою проблемою в умовах гібридних та воєнних загроз	Формують безпекову стійкість: держава здатна витримувати кібератаки, інформаційний тиск, зберігаючи спроможність приймати та виконувати рішення, критичні для виживання політичної спільноти
Міжнародний та мережевий цифровий контекст	Вбудовує українську модель державотворення в європейський та глобальний цифровий простір (ЄС, НАТО, партнерські держави), використовуючи зовнішні платформи, стандарти та підтримку як ресурс розв'язання внутрішніх проблем	Підсилює зовнішню й мережеву стійкість: дає доступ до спільних інфраструктур, стандартів безпеки, технологій та практик, зменшує ізолюваність і вразливість держави перед глобальними викликами

Джерело: розроблено автором

Формування національної моделі державотворчих процесів в Україні в умовах війни, гібридних загроз і затяжних криз неможливе в межах одновимірного, «механічного» уявлення про державу. Досвід останніх

десятиліть у зарубіжних країнах, зокрема, у нових «цифрових державах» показує, що стійкість публічної влади залежить не лише від формальної міцності інституцій чи ефективності окремих управлінських процедур, а від складної взаємодії цінностей, інститутів, мережових взаємин, цифрової інфраструктури та громадянської участі. Упродовж останніх десятиліть у зарубіжних країнах, особливо у тих, які позиціонують себе як нові «цифрові держави» (Естонія, Сінгапур, окремі північноєвропейські країни), відбулася кардинальна переоцінка підходів до побудови стійкості публічної влади. Традиційні уявлення про державну спроможність, які робили акцент виключно на юридичній сталій інституційній структурі або ефективності окремих управлінських процедур, дедалі більше поступають місце системному, багатовимірному баченню стійкості, що враховує усю складність взаємодії структурних та культурних чинників [44;45].

По-перше, зарубіжний досвід показує, що формальна архітектура навіть добре структурованих національних законів та підзаконних актів може бути неприйнятною у кризових ситуаціях, якщо національні інститути залишаються ізольованими й недостатньо інтегрованими з іншими соціальними системами в державі. Формально, мова йде не лише про інтегровану систему публічного управління, а про національну надсистему суспільних відносин, центральним елементом якої ми визначаємо НСМ. Це актуалізує категорію інституціональної резильєнтності – здатності адаптивно реагувати на виклики й використовувати кризу для розвитку (Д.Фонтейн, 2001; К.Вегріч, 2021) [56;85;86]. Але наше трактування інституціональної резильєнтності є принципово іншим. Країни, які успішно пережили системні кризи (наприклад, Естонія під час кібератак 2007 року), робили це завдяки розбудові взаємопов'язаних мереж класичних інститутів держави, публічно-приватного партнерства, специфічних майданчиків кризового управління, широкому доступу до даних та готовності делегувати повноваження в екстрених умовах. Фактично, мова йде про позитивний інституціональний зміст стійкості.

По-друге, вирішальною у такому успіху є ціннісна складова стійкості. Перехід до цифрової держави або до інноваційних моделей публічного урядування (наприклад, завдяки швидкому поширенню цифрових ідентичностей, електронного уряду, відкритих даних, платформ співучасті громадян) є реальним лише там, де ці інструменти спираються на довіру до держави, сприйняття публічної влади як служіння суспільству, громадянську культуру й інклюзивність. Це певною мірою перетинається з підходами Д.Денхарта [47-48], адже саме довіра й цінність публічного рішення лежать в основі ефективності інституційних новацій і визначають рівень участі громадян у процесах управління.

По-третє, значно зростає роль мережевих взаємин – і в горизонталі (між різними гілками, відомствами, організаціями), і у вертикалі (між рівнями урядування), і у міждержавному аспекті (міжнаціональні цифрові платформи, транскордонні сервіси, міжнародні системи кіберзахисту). Ці мережі не просто підвищують мобільність ресурсів у кризових ситуаціях, але стають інфраструктурою для обміну найкращими практиками управління, нормативного перенесення й спільної підготовки фахівців.

По-четверте, цифрова інфраструктура вже не обмежується множиною сервісів «одного вікна» чи автоматизованих процедур. У країнах-лідерах цифрової трансформації вона стає інструментом фундаментальної інтеграції даних (Б.Новек), що дає змогу швидко оновлювати політики у відповідь не лише на рутинні зміни, а й на зовнішні шоки [60]. В умовах пандемій, енергетичних криз, масованих кібератак ті уряди, які побудували захищені, масштабовані та взаємопов'язані цифрові інфраструктури, змогли гарантовано підтримувати базові функції влади й реалізацію прав громадян.

Нарешті, громадянська участь виступає не лише умовою легітимності цифрових перетворень, а й визначальним елементом стійкості всієї екосистеми держави. Найуспішніші платформи залучають громадян до співтворення політик, оперативного тестування сервісів, роботи в системах моніторингу й зворотного зв'язку (Б.Новек) [60]. Це створює self-sustaining

system – самопідтримуване середовище, в якому держава є орієнтованою на спільні цінності платформою для співучасті, а не єдиною монопольною структурою влади (Б.Волкер, К.Холлінг) [87:88].

Загалом, порівняльний аналіз доводить, що саме багатовимірність – поєднання ціннісної, інституційної, мережевої, цифрової, громадянської компонент наукового аналізу стає базисом сучасної моделі стійкості публічної влади. Український контекст підтверджує цей висновок: масштабна цифровізація, адвокатура відкритих реєстрів у боротьбі з корупцією, висока мобілізаційна здатність суспільства та його залучення до публічного врядування стають додатковими «опорами» національної стійкості поруч із класичними інститутами конституційної держави. Досвід новітніх цифрових держав підтверджує – стійкість влади не може ґрунтуватися на якомусь одному факторі (інститути, процедури, технології). Лише інтегративна модель, що включає й ціннісно-громадянський, і «цифрово-платформений», і мережевий підхід до побудови публічної влади, спроможна забезпечити реальний захист від багатоманітних сучасних викликів. Для України це означає необхідність не механічного копіювання інституційних форм, а розбудови власної багатовимірної національної моделі стійкості публічної влади.

Інституціональна резильєнтність посідає центральне місце в сучасних дослідженнях стійкості публічної влади, особливо в контексті цифрової трансформації держав та ускладнення середовища публічного управління. С.Пирожков, О.Резнікова, В.Горбулін задають стратегічно-безпековий і державно-політичний вимір – національні доповіді, аналіз безпекового середовища, гібридні загрози, «війна майбутнього» [89-90;91;93;94;96;100;102]. Г.Ситник, М.Орел вводять стійкість у рамку публічного управління та національної безпеки, аксіологічний (ціннісний) вимір стійкості держави [92;94;101]. О.Суходоля конкретизує стійкість через критичну інфраструктуру та життєво важливі функції [95]. О.Кондратенко, Я. Лазебник розгортають геополітичний і концептуальний аналіз національної

стійкості в українському контексті [97]. М.Масик, О.Клименко акцентують інституціональну й міждисциплінарну стійкість, зближуючи дискурс із теоріями інститутів та governance [99].

Втім, для збереження керованості в умовах криз недостатньо лише формальної міцності інституцій або оптимізації окремих процедур. Потрібна якісно інша здатність публічних інститутів – витримувати екзогенні імпульси, адаптуватися, вбудовувати зміни у власну структуру, не втрачаючи при цьому легітимності та довіри громадян. Саме цю властивість зазвичай позначають поняттям інституціональної резильєнтності. У класичному розумінні резильєнтність постає як спроможність інститутів підтримувати базові функції, реагуючи на зовнішні й внутрішні виклики за допомогою організаційної адаптації, координації між акторами та вибіркового оновлення політик у межах наявного інституційного поля. Дж.Фаунтейн аналізує цифрову трансформацію державного управління, наголошує, що запровадження інформаційних технологій часто не руйнує усталені інституційні структури, а, навпаки, «вмонтовується» в них, підсилюючи або навіть відтворюючи статус-кво. Це дозволяє говорити про резильєнтність як про стійкість інституційних шаблонів до радикальних змін: вони адаптуються до нових технологічних інструментів, не втрачаючи своєї базової логіки [85]. Водночас така стійкість набуває двозначного характеру: з одного боку, вона захищає систему від руйнації під впливом надто швидких змін; з іншого – може гальмувати необхідні структурні перетворення, якщо адаптація відбувається без переосмислення ціннісних і владних основ функціонування інститутів.

К. Вегріх, досліджуючи наслідки реформ у публічному секторі та трансформації під впливом доктрини «нового публічного менеджменту», концентрується на тому, як різні конфігурації інституцій і ступінь їх автономії впливають на спроможність системи до стабільного функціонування та фінансового оздоровлення. У його працях інституційна резильєнтність постає як результат поєднання формальних правил,

організаційних практик і механізмів координації, які дають змогу витримувати бюджетні, політичні та управлінські кризи, не втрачаючи здатності виконувати основні публічні функції. Тут ключовою є ідея про те, що резильєнтність закладається у дизайн інституцій: у розподіл повноважень, механізми контролю й підзвітності, форми взаємодії між державними та недержавними акторами [86].

Отже, класичне розуміння інституціональної резильєнтності можна описати як здатність публічних інститутів забезпечувати безперервність виконання базових функцій в умовах криз за рахунок адаптації процедур, тимчасової переналаштування механізмів координації, часткового оновлення політик та інституційного «навчання». Кризу тут розглядають водночас як загрозу і як можливість для точкових реформ – криза виявляє «слабкі місця» інституційної архітектури, примушує до корекції норм і практик, але фінальна мета зазвичай полягає у відновленні функціональної рівноваги системи, часто в дещо оновленому, проте впізнаваному вигляді [103]. Такий підхід має низку сильних сторін. По-перше, він дозволяє уникнути наївної віри у «повну перезагрузку» інститутів, підкреслюючи інерційність інституційних структур і важливість поступової еволюції. По-друге, він фокусує увагу на реальних організаційних механізмах, через які здійснюється адаптація: міжвідомча координація, гнучкі регуляторні режими, використання цифрових інструментів для підтримки прийняття рішень тощо. По-третє, він пропонує операціоналізовані критерії оцінки резильєнтності, зокрема, ступінь збереження функцій, швидкість відновлення після кризи, масштаб необхідних ресурсів для підтримання системи в робочому стані.

Разом з тим, у класичному розумінні інституційна резильєнтність часто має приховано консервативний характер. Вона тяжіє до моделі, в якій головним завданням інститутів є «повернення до нормальності» – хоч і з урахуванням окремих уроків, але в межах тієї ж парадигми владних відносин, легітимаційних практик і організаційних структур. Кризу осмислюють насамперед як «збій», відхилення від норми, яке потрібно виправити. У

результаті навіть досить глибокі технологічні чи процедурні зміни нерідко відбуваються без радикального перегляду цінностей, посилення участі громадян чи перерозподілу влади між центром і периферією. Іншими словами, інституція вчиться краще захищати себе від майбутніх потрясінь, але не завжди вчиться змінювати свою природу.

Крім того, класичний підхід часто недооцінює конфліктогенний, політичний вимір резильєнтності. Інституції розглядають як нейтральні механізми управління, хоча насправді вони втілюють певний баланс сил та інтересів. Те, що для одного сегмента суспільства є проявом стійкості, для іншого може означати закріплення несправедливого розподілу ресурсів чи збереження неінклюзивних практик. Резильєнтність у такому випадку перетворюється на здатність системи «пережити» критику й тиск, не змінюючи свого характеру, що може призводити до накопичення латентних конфліктів. Виходячи з таких обмежень, доцільно запропонувати авторську, принципово іншу інтерпретацію інституціональної резильєнтності. У межах цієї інтерпретації резильєнтність доцільно розуміти не як здатність інституцій повернутися до рівноваги після кризи або навіть інкрементально оновитися, а як їхню структуровану схильність до самооновлення через розширення множини можливих станів розвитку. Інакше кажучи, справді резильєнтний інститут має можливість перетворювати кризові події на ресурс для якісної зміни власної конфігурації, відкриття нових ролей, форм взаємодії та каналів легітимації. У цій логіці інституціональна резильєнтність може бути визначена так: це здатність інститутів публічної влади не лише підтримувати базові функції та адаптувати процедури у відповідь на кризи, а й цілеспрямовано розширювати простір власних життєздатних сценаріїв, використовуючи конфлікт, невизначеність і зовнішній тиск як каталізатори створення нових норм, структур і практик, що краще відповідають зміненому середовищу та суспільним очікуванням.

Даний підхід переносить акцент із «відновлення» на «проєктивну еволюцію» – свідоме конструювання майбутніх конфігурацій інститутів, у

яких уроки кризи не просто інтегруються у стару логіку, а переосмислюють її. Принципова відмінність полягає в тому, що класична модель резильєнтності мислить систему переважно в координатах «стабільність – шок – відновлення», тоді як авторська модель оперує координатами «стабільність – шок – множинність – нова конфігурація». Ключовим стає проміжний стан множинності, коли інституція не намагається одразу ж відновити попередній порядок, а допускає (і навіть інституційно підтримує) конкуренцію альтернативних сценаріїв, експериментування з новими формами організації, залучення нових акторів і каналів участі. У такій перспективі криза не є аномалією, що порушує «нормальний» хід подій, а невід’ємним елементом розвитку, який сигналізує про вичерпання попередньої конфігурації системи державного управління. Щоб чіткіше показати відмінності між класичним і авторським підходами, доречно представити порівняльну таблицю (таблиця 1.9). У ній узагальнено ключові параметри розуміння інституціональної резильєнтності: мету, ставлення до кризи, типові механізми змін, критерії успішності та роль громадян.

Таблиця 1.9

Концептуалізація інституціональної резильєнтності

Параметр	Класичне розуміння інституціональної резильєнтності	Авторська інтерпретація інституціональної резильєнтності
Базова мета	Збереження безперервності функціонування інститутів, швидке відновлення після криз, мінімізація втрат, підтримання інституційної стабільності	Розширення простору можливих станів розвитку інститутів, трансформація їхньої структури та ролі через творчий використання криз для якісного оновлення
Ставлення до кризи	Криза – це загроза і водночас можливість для адаптивних, переважно поступових (у напрямі покращення) змін у межах наявної логіки системи	Криза – це сигнальний механізм вичерпання попередньої конфігурації, каталізатор множинності сценаріїв і інструмент систематизації нових регламентів
Тип змін	Переважно поступові, вибіркові реформи: корекція політик, уточнення процедур, посилення координації, запровадження технологічних інновацій без руйнування основ	Можливі як поступові, так і хвилеподібні зміни, включно з переосмисленням цінностей, перерозподілом повноважень, появою нових інституційних форматів і каналів участі

Продовження таблиці 1.9

Параметр	Класичне розуміння інституціональної резильєнтності	Авторська інтерпретація інституціональної резильєнтності
Орієнтація в часі	Переважно ретроспективна та короткострокова: аналіз «уроків кризи», корекція поточних практик, фокус на швидкому поверненні до керованої рівноваги	Переважно проєктна й середньо/довгострокова, коли конструювання бажаних майбутніх конфігурацій інститутів, вбудовування невизначеності та конфлікту інтегровано в саму логіку розвитку
Ставлення до статус-кво	Статус-кво вважається в цілому прийнятним; завдання інститутів – краще захищати й адаптувати його до змін, зберігаючи основні баланси	Статус-кво розглядається як один із можливих, а не єдино легітимний стан; інституція свідомо допускає його перегляд, якщо він втрачає відповідність цінностям і суспільним очікуванням
Критерії успішності	Мінімізація перерв у виконанні функцій, обмеження масштабу руйнувань, здатність зберегти базову структуру та легітимність	Здатність системи породжувати нові, більш адекватні форми організації та взаємодії, підвищення якості легітимації, розширення участі та посилення спроможності до саморефлексії
Роль громадян	Переважно як об'єкта захисту й адресата послуг; участь – важлива, але часто другорядна щодо організаційної та технологічної адаптації	Громадяни як співтворці нових інституційних конфігурацій; участь і політичний конфлікт розглядаються як ресурс розвитку, а не лише як ризик для стабільності
Політичний вимір	Здебільшого імпліцитний – інститути розглядаються як нейтральні механізми управління, увага зосереджена на технічній і процедурній стороні	Класичний політичний – резильєнтність включає здатність переформатовувати партійні коаліції, змінювати механізми розподілу влади та перетворювати конфлікти на інституційні інновації

Джерело: [85;86]; дослідження автора

Як видно з порівняльної таблиці, ключова відмінність авторської інтерпретації від класичної полягає в переході від «захисного» до «творчо-еволюційного» бачення резильєнтності. Інститут більше не мислиться як фортеця, завдання якої – вистояти під ударами та зберегти форму, а як живий організм або навіть як відкрита платформа, здатна змінювати власну архітектуру, типи зв'язків, ролі учасників. У цьому сенсі резильєнтність виявляється ближчою до категорії *інституціональної еволюційності*, але з важливим акцентом на свідомому, проєктному характері цих змін, коли не будь-яка трансформація є проявом резильєнтності, а лише та, що водночас

посилює здатність системи витримувати нерівновагу і поглиблює її відповідність базовим цінностям та очікуванням суспільства. Таке розуміння інституціональної резильєнтності особливо продуктивне для аналізу державотворчих процесів і національної стійкості в умовах глибоких потрясінь – війни, радикальної цифровізації, зміни геополітичних орієнтацій, адже дозволяє вийти за межі логіки «повернення до стандарту» й натомість актуалізувати нові конфігурації інститутів, цінностей і практик здатні зробити політичну спільноту більш стійкою до майбутніх криз, не закриваючи при цьому простір для свободи, участі та розвитку. У такій перспективі інституціональна резильєнтність стає не лише технічною характеристикою системи управління, а й однією з ключових категорій теорії держави, що визначає траєкторії її еволюції в XXI столітті.

Національна стійкість дедалі більше розглядається як ключовий вимір сучасних державотворчих процесів, зокрема в Україні, де поєднуються одночасно війна, глибинна інституційна трансформація та інтеграція в європейський політико-правовий простір. У цьому контексті державотворення, на думку сучасних науковців, постає не просто як формальне конструювання органів влади та системи правових норм, а як тривалий процес інституційного налаштування політичної спільноти до функціонування в умовах постійної турбулентності, багатовекторних загроз і зовнішніх впливів [104-105].

Сучасні дослідження національної стійкості [91;93;106] вказують на те, що вона формується як системна властивість, що поєднує безпековий, політичний, інституційний, економічний і ціннісний виміри. У цьому полі державотворчі процеси розуміються як послідовні та взаємопов'язані зміни інституційної архітектури держави – її конституційного ладу, моделі публічного управління, механізмів участі громадян, конфігурації центр–регіони–громади, а також внутрішньої логіки функціонування ключових органів влади. Отже, питання стійкості держави невіддільне від питання того, наскільки її інститути здатні не просто зберігатися в умовах криз, а й

служувати носіями поступового, але незворотного перетворення політичної спільноти, тобто бути суб'єктами державотворення, а не лише інструментами управління.

Класичні підходи до інституційної резильєнтності в системі публічного управління роблять акцент переважно на здатності інституцій забезпечувати безперервність виконання основних функцій, оперативно відновлюватися після кризових потрясінь, мінімізувати втрати ресурсів та легітимності. У цьому розумінні резильєнтність часто ототожнюється з інституційною спроможністю, що проявляється як розгалужена система органів влади, з наявністю нормативно-правової бази, формалізованих процедур координації та реагування, впровадженням сучасних інструментів планування, моніторингу й цифрових рішень (позицій досліджень О.Руденко [107], О.Рось [108], Л.Жукової [109]. Державотворчий процес при цьому уявляється як послідовна раціональна модернізація інституційної системи, де кризи відіграють роль зовнішніх імпульсів, які виявляють слабкі місця та спонукають до корегувальних реформ, але цілісна логіка розвитку держави загалом залишається незмінною [110]. Такий підхід має важливі переваги: він дозволяє оперувати вимірюваними показниками (правова визначеність, стабільність інституцій, керованість процесів, швидкість відновлення після кризи), пропонує зрозумілу модель проектування реформ і систем національної стійкості.

Водночас, коли йдеться про державотворчі процеси в умовах глибоких трансформацій, як це відбувається в Україні під час війни та переорієнтації на європейські стандарти демократичної правової держави, така модель виявляється частково неефективною. Адже вона схильна фіксуватися на захисті існуючої конфігурації влади, розглядаючи державотворчі зміни передусім як удосконалення вже заданих інститутів, а не як можливість для їхнього якісного переосмислення та проектної еволюції. У запропонованій авторській інтерпретації інституційна резильєнтність у державотворчих процесах постає не лише як здатність системи «витримувати удари» та

відновлювати функціонування, а як структурована схильність інститутів до самооновлення через розширення множини можливих сценаріїв свого розвитку. Іншими словами, резильєнтні державотворчі інститути – це такі, що здатні перетворювати кризові ситуації, конфлікти інтересів та зовнішні впливи на каталізатори свідомої перебудови інституційної архітектури, включно з перерозподілом повноважень, зміною форм легітимації та поглибленням участі громадян.

Інтеграція такої логіки з українським контекстом дозволяє виокремити низку інституціональних парадоксів національної стійкості у державотворчих процесах (в авторській класифікації, на основі методології інституціональної парадигми О.Баштанник).

Перший парадокс можна позначити як *парадокс формально сильної, але фактично вразливої держави (парадокс інституціонального фасаду)*. В українському державотворенні тривалий час домінувала логіка нарощування формальних елементів інституціональної спроможності – утворення нових органів, прийняття численних стратегій, програм, концепцій, посилення нормативного регулювання практично всіх сфер. З одного боку, це створювало вигляд складної, професійно налаштованої системи публічного управління, здатної координувати євроінтеграційні реформи, забезпечувати безпеку, економічний розвиток і виконання міжнародних зобов'язань. З іншого боку, надлишкова формалізація, дублювання повноважень, слабка горизонтальна координація та відсутність реальних механізмів відповідальності за результати призводили до того, що в умовах гострих криз – від фінансово-економічних до воєнних – державні інститути виявлялися повільними, розрізненими й часто нездатними до оперативної колективної дії. Отже, для національної стійкості у державотворчих процесах принципово важливо не стільки збільшувати кількість інституційних ланок, скільки забезпечувати їх узгодженість, гнучкість та орієнтацію на довгострокові державотворчі цілі.

Другий парадокс – *парадокс централізованого державотворення через децентралізацію (парадокс децентралізації)*. Реформи децентралізації в Україні були проголошені як один із наріжних каменів сучасного державотворення, спрямованих на посилення суб'єктності громад, розвиток місцевої демократії та наближення моделі врядування до європейських стандартів. З одного боку, передача частини повноважень, фінансової бази та відповідальності на місцевий рівень мала посилити стійкість держави до багаторівневих загроз, зробити територіальні громади активними учасниками забезпечення національної безпеки, відновлення інфраструктури й соціальної згуртованості, особливо в умовах війни. З іншого боку, ключові стратегічні рішення, розподіл значних фінансових потоків, кадрова політика та системи державного моніторингу залишалися значною мірою централізованими, що зумовлювало формування моделі «керованої автономії»: місцеві інституції отримували розширений перелік завдань, але не завжди мали достатню свободу та ресурси для їх самостійного виконання. У результаті децентралізація виявляється водночас інструментом посилення національної стійкості та механізмом відтворення вертикально орієнтованого державотворення, в якому центр зберігає домінування у визначенні рамок місцевої політики.

Третій парадокс – *парадокс кризи легітимності як ресурсу державотворення (парадокс легітимності)*. Український досвід переконливо показує, що періоди різкого падіння довіри до інститутів влади, зростання протестних настроїв та делегітимізації існуючих еліт з одного боку загострюють уразливість держави, а з іншого – відкривають вікно можливостей для глибинних державотворчих змін. Коли парламент, уряд, судова система чи правоохоронні органи втрачають суспільну підтримку, це дестабілізує політичну систему, ускладнює ухвалення рішень, підриває міжнародну репутацію та створює додаткові ризики безпеці. Водночас саме в таких ситуаціях постає запит на переосмислення засад державної влади, реформу конституційної архітектури, оновлення політичних еліт та

механізмів підзвітності влади громадянам. Якщо інституційна система здатна інкорпорувати цей запит у формат контрольованих державотворчих процесів – через конституційні процедури, широкі суспільні консультації, інклюзивний політичний діалог, – тоді криза легітимності стає імпульсом до проєктної еволюції, а не до руйнації державності.

Четвертий парадокс – *парадокс цифрової державності як стійкості через вразливість (парадокс цифрового захисту)*. Цифровізація публічного управління, розвиток електронних сервісів, реєстрів, систем «держава в смартфоні» стали важливою частиною українського державотворчого проєкту і суттєво змінили конфігурацію відносин між державою, громадянами та бізнесом. З одного боку, цифрові інструменти підвищують прозорість і підзвітність влади, спрощують доступ громадян до послуг, створюють нові канали участі у виробленні політики та сприяють наближенню України до європейських стандартів відкритого врядування. Це прямо посилює національну стійкість, оскільки допомагає державі зберігати функціональність навіть у воєнних умовах, підтримувати довіру до інститутів та більш ефективно управляти кризами. З іншого боку, зростання залежності державотворчих процесів від цифрової інфраструктури підвищує їхню вразливість до кібератак, знищення чи підміни даних, зовнішнього контролю над критичними комунікаційними каналами. Умовно кажучи, чим більш «цифровою» стає держава, тим більш критичними є для її стійкості питання кібербезпеки, резервних (аналогових) каналів управління, суверенітету над даними та правових гарантій захисту цифрових прав громадян.

П'ятий парадокс – *парадокс мережевої участі в державотворенні (парадокс мережі)*, коли розширення кола акторів, залучених до вироблення публічної політики, водночас підсилює й розмиває інституційну відповідальність. Сучасна модель державотворчих процесів в Україні значною мірою базується на включенні до них не лише традиційних суб'єктів влади, а й органів місцевого самоврядування, громадських організацій,

волонтерських рухів, бізнесу, наукових та експертних спільнот, міжнародних партнерів. З одного боку, така мережевізація дозволяє залучати додаткові ресурси, знання та легітимацію рішень, що зміцнює національну стійкість і робить державотворчі процеси більш інклюзивними та адаптивними. З іншого боку, коли значна частина рішень виробляється у гнучких мережевих форматах – робочих групах, партнерських платформах, публічно-приватних проектах – виникає проблема чіткого розподілу відповідальності: складніше визначити, хто саме несе політичну, правову та моральну відповідальність за провали реформ, неготовність до загроз чи неефективне використання ресурсів. Якщо інституційний дизайн державотворчих процесів не передбачає прозорих механізмів фіксації і підзвітності як державних, так і недержавних суб'єктів, мережевий формат, що мав би посилювати стійкість, може породжувати хаос відповідальності.

Таким чином, інтеграція концепту інституціональної резильєнтності в аналіз державотворчих процесів дозволяє подивитися на національну стійкість не лише як на сукупність безпекових та управлінських заходів, а як на здатність держави до проєктивної еволюції в умовах множинних парадоксів. Формально потужна, але слабо скоординована інституційна система; децентралізація, що поєднує розширення повноважень громад із збереженням сильної центристської рамки; криза легітимності, яка одночасно підриває й оновлює державність; цифрова державність, що підвищує ефективність та оголює нові вразливості; мережеве державотворення, яке посилює участь, але потребує нових стандартів відповідальності, – усі ці суперечності не є відхиленнями від норми, а структурними рисами сучасної української державотворчої реальності. Розуміння й усвідомлена інституціоналізація цих парадоксів стають засадою для розроблення стратегій національної стійкості, в яких державотворчі процеси постають не як разова інституційна реформа, а як тривалий, відкритий і керований процес переосмислення самої моделі держави в координатах європейської інтеграції, безпекових викликів та внутрішньої еволюції українського суспільства

Саме тому пропонується розглядати *національну стійкість не як статичну «міцність» держави, а як результат взаємодії кількох вимірів, що по-різному проявляються в різних моделях врядування*. Дискусії про трансформацію публічного управління від класичної бюрократичної моделі до концепцій governance та належного врядування суттєво змінюють вихідні припущення про джерела стійкості. Така мережево-інтерактивна логіка створює нові ресурси для стійкості – соціальний капітал, гнучкість, здатність до самоорганізації, – але водночас породжує ризики розмитості відповідальності та ускладнення процесів ухвалення рішень. Для України, яка перебуває в умовах високої невизначеності та прямої воєнної агресії, це означає: опора лише на вертикаль влади є недостатньою, а надмірна мережевість без чітких механізмів підзвітності може бути небезпечною.

Паралельно розвивалася критика редукції публічного управління до логіки «послуг для клієнтів», притаманної NPM. Концепція Нового публічного сервісу наполягає на розумінні публічної влади як служіння громадянам і суспільству, а не лише як ефективного менеджменту ресурсів. У центрі цієї парадигми – публічна цінність, громадянство, етичний вимір діяльності службовців. Ідеї В.Вільсона щодо публічної цінності підкреслюють, що стійкість інститутів неможлива без ціннісної консолідації суспільства, без відчуття людьми, що держава втілює й захищає те, що для них справді важливо – свободу, гідність, справедливість, безпеку, майбутнє спільноти [111]. Європейські дослідники, зокрема Х. де Врі та В. ван де Валле, показують, що там, де демократичні цінності, довіра й громадянська участь стають ядром публічної політики, формуються більш стійкі моделі управління, здатні витримувати тривалі кризи [112-114]. Для українського контексту це особливо важливо, оскільки масштабна мобілізація, волонтерський рух і готовність громадян до тривалого спротиву спираються саме на ціннісно-громадянський вимір, а не лише на адміністративні чи матеріальні ресурси.

Разом із тим, у ХХІ столітті до цих двох «класичних» вимірів –

мережевого/належного врядування та публічної цінності – додається потужний цифровий вимір. Дослідження Дж. Фаунтейнф, В. Майер-Шенбергера, Б. Новека, а також практики естонської та сінгапурської моделей свідчать, що цифрове врядування (e-governance) перетворюється з інструментарію «оптимізації процедур» на структурний елемент державності [57;60]. Фактично, держава як цифрова платформа інтегрує розподілені дані, сервіси та актора, забезпечуючи можливість швидкого масштабування рішень, проактивного надання послуг, підтримки безперервності ключових функцій навіть за умов фізичних руйнувань чи вимушеної релокації. У відкритих реєстрах, цифрових ідентичностях, інтегрованих інформаційних системах закладено не лише зручність, а й новий формат стійкості – здатність підтримувати життєдіяльність держави та суспільства за рахунок цифрової інфраструктури.

Водночас, критики технократичної логіки цифровізації (переважно, Є.Морозов) попереджають про ризики «цифрового солюціонізму», коли складні суспільні проблеми зводяться до технічних завдань, а політичні й етичні дилеми – до питання налаштування алгоритмів. Надмірна віра в «нейтральність» даних та алгоритмів може маскувати нерівність доступу, дискримінаційні практики, небезпеку цифрового авторитаризму, коли потужні інформаційні системи та засоби аналітики стають інструментом тотального контролю, а не посилення резильєнтності демократичної спільноти [115-116]. Для України, де цифрові сервіси фактично стали одним із символів модернізації держави та важливим елементом підтримки суспільної стійкості під час війни [117], це означає необхідність поєднати амбіції «цифрової держави» з чіткою ціннісною й правовою рамкою.

У такому контексті національна модель державотворчих процесів має будуватися не як імпорт будь-якої окремої теоретичної парадигми, а як синтез кількох вимірів. Мережеве підказує, що стійкість в умовах поліструктурних криз досягається через взаємодію держави з громадянами, громадами, бізнесом, міжнародними партнерами – але вимагає механізмів

підзвітності та мета-врядування. Новий публічний сервіс та концепція публічної цінності (Д.Денхарт, Б.Боземан) наголошують, що без ціннісної консолідації, громадянської суб'єктності та етичної місії публічної служби ця взаємодія не матиме довгострокової стійкості. Одночасно, цифрове врядування додає інфраструктурно-технологічний вимір, завдяки якому держава здатна функціонувати в режимі безперервної кризи, спираючись на дані, інтероперабельні системи, кіберзахищені платформи.

Цифрове врядування може стати каркасом, який поєднує мережевий, ціннісно-громадянський та безпековий виміри державотворення в єдину національну модель, зорієнтовану на вирішення конкретних проблем, а не на відтворення абстрактних організаційних схем. Саме через цю багаторівневу екосистему цифрова держава здатна забезпечити не лише безперервність функцій, а й розвиток резильєнтності як ключової характеристики сучасної української державності (рис.1.7).



Рис.1.7. Формування нової парадигми державотворчих процесів в науці державного управління

Джерело: дослідження автора

Сучасна цифрова трансформація державного (публічного) управління потребує такого теоретичного осмислення, яке виходить за межі простого «оцифрування послуг» і розглядає зміни як переформатування самої державності. Йдеться про багатовимірний процес, у якому технологічні інновації, інституційні перетворення, зміна моделей взаємодії з громадянами та виклики національної стійкості взаємопов'язані й формують нову конфігурацію публічної влади. Щоб систематизувати цей процес, доцільно виокремити комплекс ключових вимірів (в авторському трактуванні) і в їх межах навести авторські поняття та визначення, які описують цифрову державу як динамічну, але структуровану систему.

Перший базовий вимір – це онтологія цифрової держави, відповідь на запитання, якою за своєю природою стає держава в умовах цифровізації. У цьому дослідженні держава розглядається не як жорстка бюрократична машина, а як багаторівнева відкрита система, у якій інститути, сервіси, норми й канали комунікації перебувають у постійній взаємодії. Особливу роль у цій структурі відіграє те, що пропонується визначити як «*цифровий дизайн державності*» – цілісну сукупність концептуальних рішень, інституціональних налаштувань та технологічних інструментів, за допомогою яких організовано реалізацію публічної влади в цифровому середовищі (сервіси, реєстри, інформаційні системи, алгоритми обробки даних, користувацькі інтерфейси та правила їхнього використання).

Цифровий дизайн державності (ЦДД), на нашу думку, має кілька ключових характеристик. По-перше, ЦДД є змінним: програмні рішення оновлюються, інтегруються нові платформи, змінюються протоколи взаємодії між органами влади, переосмислюються моделі надання публічних послуг. По-друге, ЦДД є розподіленим: елементи цифрового дизайну формуються різними суб'єктами – центральними органами виконавчої влади, органами місцевого самоврядування, державними підприємствами, приватними розробниками, що працюють у межах державних (публічних)

політик. По-третє, ЦДД є символічно навантаженим: саме через досвід користування цифровими послугами, взаємодії з електронними кабінетами, порталами, застосунками громадяни формують уявлення про те, чи є держава сучасною, зрозумілою й орієнтованою на людину, чи, навпаки, відсталою й закритою. У цьому сенсі цифровізація постає не лише як технічний процес, а як новий спосіб публічної присутності держави в житті людини – через спроектований, відтворюваний і змінюваний цифровий дизайн.

На цьому підґрунті постає потреба в окремому аналітичному конструкті, який би описував, як саме завдяки інституційним, правовим і цифровим рішенням відтворюється та змінюється державність. Такий конструкт позначимо як *«модель державотворчих процесів»*. Під моделлю державотворчих процесів у даній роботі розуміємо *концептуальну схему, що описує послідовність, взаємозв'язки та логіку ключових дій, рішень і перетворень, через які формується, змінюється й відтворюється державність – з урахуванням інституційних механізмів, правових норм, суспільних очікувань і параметрів цифрового дизайну*. Модель державотворчих процесів дозволяє інтегрувати в єдине ціле те, що зазвичай розглядається окремо: конституційні реформи, адміністративно-територіальні зміни, трансформації публічної служби, запровадження цифрових сервісів, формування нових каналів участі громадян. У запропонованій рамці цифровий дизайн державності виступає не лише як інструмент, а як середовище реалізації цієї моделі: через цифрові рішення конкретизуються, спрощуються або, навпаки, ускладнюються шляхи, якими громадяни й інституції беруть участь у державотворчих процесах.

Другий вимір – трансформація взаємодії між державою та громадянами в цифровому середовищі, й саме тут постає потреба осмислити нові правила й очікування, пов'язані з використанням даних, алгоритмів, електронних сервісів і багатоканальної комунікації. Для цього вводиться категорія *«цифрового суспільного контракту»*. Під *цифровим суспільним контрактом*

у даній роботі розуміємо *сукупність явних і неявних домовленостей між державою та громадянами щодо меж, принципів і цілей використання цифрових технологій у публічному управлінні*. До змісту такого контракту належать: загальновизнані правила збору, зберігання та обробки персональних даних; допустимі межі автоматизації прийняття рішень; прозорість механізмів, за якими цифрові системи впливають на доступ до послуг та ресурсів; наявність у громадян інструментів контролю, оскарження й корекції цифрових рішень. Цей контракт не може бути раз і назавжди зафіксованим; він постійно змінюється під впливом суспільних дискусій, розвитку технологій, а також кризових ситуацій, у яких держава змушена діяти в умовах високої невизначеності, але все одно має зберігати легітимність і довіру.

У межах цього ж виміру доцільно ввести поняття «формат керованої невизначеності». Під форматами керованої невизначеності пропонується розуміти такі сфери публічної діяльності, у яких неможливо повністю формалізувати всі можливі сценарії наперед, але від держави очікується забезпечення передбачуваних, справедливих і прозорих результатів. До таких форматів належать, наприклад, реагування на воєнні, техногенні чи гуманітарні кризи, управління масовими міграційними процесами, протидія інформаційним атакам, відновлення критичної інфраструктури після руйнувань. У цих ситуаціях цифровий дизайн державності має забезпечити такі рішення, які дозволяють швидко збирати актуальні дані, гнучко оновлювати аналітичні моделі й підтримувати прийняття рішень тоді, коли повної інформації немає, а діяти потрібно негайно. Модель державотворчих процесів у цьому разі задає логіку, в межах якої поєднуються надзвичайні повноваження, стандартні процедури та механізми суспільного контролю, а цифровий дизайн конкретизує технічні й організаційні форми реалізації цієї логіки.

Третій вимір стосується фактичного стану цифровізації державного (публічного) управління, тобто того, як реально побудований і функціонує

цифровий дизайн державності та які внутрішні суперечності він містить. На практиці йдеться про нерівномірність розвитку цифрових рішень у різних органах влади й секторах. Частина установ має продуманий цифровий дизайн – інтегровані реєстри, зручні електронні сервіси, налагоджені канали двосторонньої комунікації. Інші продовжують працювати на застарілих інформаційних системах або навіть переважно в паперовому форматі. Це створює структурну фрагментованість цифрової інфраструктури публічного управління, коли між окремими підсистемами немає належної взаємодії, а обмін даними відбувається повільно, з дублюванням та помилками.

У таких умовах виникає феномен, який пропонується визначити як *«цифровий розрив довіри»*. Під цифровим розривом довіри розуміється *ситуація, коли рівень довіри громадян до держави істотно залежить від того, з якими саме практиками й елементами її цифрового дизайну вони взаємодіють у конкретних життєвих ситуаціях*. Якщо людина отримує одну послугу швидко й прозоро через зручний електронний сервіс, а іншу – лише через тривалі офлайн-процедури з незрозумілими строками та вимогами, у її свідомості формується суперечливий образ держави – як модерної й ефективної в одних сферах та архаїчної й неефективної – в інших. Такий розрив небезпечний тим, що підриває цілісність легітимності державної влади: громадяни схильні формувати власну оцінку держави в цілому за найбільш травматичним досвідом, навіть якщо в інших аспектах цифровий дизайн є успішним. З погляду моделі державотворчих процесів це означає, що різні ланки державної системи рухаються за різними «траєкторіями модернізації», не утворюючи узгодженого цілого.

Четвертий вимір пов'язаний із якістю й характером цифрових змін. Тут важливо оцінювати не лише сам факт наявності електронних сервісів, а й те, наскільки змінюється зміст управлінських процесів, структура відповідальності та взаємодія з громадянами. У цьому контексті доцільно запровадити розрізнення «реального» та «квазі» цифрового дизайну (або, у більш широкому сенсі, реальної та квазі-цифровізації).

У цьому дослідженні під *реальним цифровим дизайном державності* розуміється такий стан організації цифрових рішень, за якого впровадження технологій супроводжується глибинною трансформацією процедур, скороченням зайвих етапів, спрощенням доступу до послуг, переглядом розподілу повноважень і постійним удосконаленням сервісів на основі зворотного зв'язку та аналізу даних. У термінах моделі державотворчих процесів це означає, що цифрові рішення не просто «обслуговують» уже наявні процедури, а стають механізмом їх переосмислення й оновлення.

Квазі-цифровий дизайн означає, навпаки, формальне перенесення наявних паперових процедур у цифровий формат без критичного перегляду їхньої доцільності, структури та навантаження на громадян. У такому випадку електронні форми дублюють паперові, кількість кроків залишається такою самою, а інколи навіть збільшується, бо додаються технічні складнощі. Це не підвищує ні ефективності, ні довіри, а лише створює ілюзію модернізації й консервує застарілу модель державотворчих процесів у новому технологічному «упакуванні». Щоб аналітично розрізняти ці стани, доцільно запровадити поняття «матриці публічної чутливості».

Під *матрицею публічної чутливості* в даній роботі розуміється система якісних та кількісних показників, за допомогою яких оцінюється здатність цифрового дизайну державності вчасно й адекватно реагувати на сигнали від громадян, зміни в зовнішньому середовищі та внутрішні збої самої інфраструктури. До таких показників можуть належати: середній час обробки звернень; частота й зміст оновлень електронних сервісів; здатність системи витримувати пікові навантаження; швидкість відновлення роботи після технічних інцидентів; наявність механізмів регулярного збору зворотного зв'язку від користувачів та врахування цього зворотного зв'язку в подальшому проєктуванні сервісів. Висока публічна чутливість є ознакою живого цифрового дизайну; низька свідчить про відрив цифрових рішень від реальних потреб людей. Водночас матриця публічної чутливості може

розглядатися як інструмент для емпіричної перевірки того, наскільки реальні практики відповідають задекларованій моделі державотворчих процесів.

П'ятий вимір пов'язаний із проблематикою стійкості та самовідновлення держави й суспільства в умовах війни, гібридних загроз, економічних та гуманітарних криз. Тут пропонується поняття «національної рамки самовідновлення». Під національною рамкою самовідновлення розуміється інтегрована здатність суспільства, інституцій публічної влади та економічних суб'єктів локалізувати наслідки кризових явищ, відновлювати критично важливі функції життєдіяльності та переходити до нового, більш організованого й стійкого стану, використовуючи результати кризи як ресурс розвитку. У цьому контексті цифровий дизайн державності виконує роль операційної пам'яті та інструменту координації. Саме через продумані цифрові рішення збираються дані про масштаби руйнувань, переміщення населення, потреби громад; на їх основі формується картина пріоритетів відновлення, розподіляються ресурси, здійснюється моніторинг виконання програм підтримки. Без якісного цифрового дизайну національний контур самовідновлення функціонує значно повільніше й менш скоординовано, а модель державотворчих процесів набуває хаотичного, фрагментованого характеру.

Важливо вказати на три основні аспекти. Перший – *наявність структурної стійкості інфраструктури*, що означає відсутність єдиних точок відмови, наявність резервних каналів зв'язку, систем резервного копіювання даних, альтернативних майданчиків для розміщення критичних сервісів. Другий – *функціональна гнучкість*, яка дає змогу в разі системної кризи тимчасово змінити пріоритети: обмежувати другорядні послуги й підтримувати максимально можливу роботу життєво важливих сервісів (реєстрація переміщених осіб, виплати, медичні послуги, безпека). Третій – *адаптивна прозорість*, тобто збереження мінімально необхідного рівня відкритості інформації й механізмів контролю навіть у режимах воєнного чи надзвичайного стану, що дозволяє не допустити зловживань під прикриттям

кризи. З точки зору моделі державотворчих процесів це описує, наскільки державотворення не зупиняється в умовах кризи, а переходить у режим прискореної, але керованої адаптації.

Шостий ключовий вимір цифрової трансформації – це архітектура взаємодії держави й громадян, яка поєднує цифрові та традиційні канали. Для її опису вводиться поняття «гібридної архітектури публічної взаємодії». Під гібридною архітектурою публічної взаємодії розуміється така організація системи надання послуг і комунікації, за якої цифрові та офлайн-канали розглядаються як взаємодоповнювані елементи єдиної логіки обслуговування громадянина, із можливістю безшовного переходу між ними. У межах такої архітектури електронні сервіси виконують роль основного, масового й швидкого каналу доступу до стандартних послуг, тоді як офлайн-формати зберігаються для складних або чутливих випадків, де потрібне індивідуальне консультування, пояснення чи елементи медіації. Важливо, що інформація про звернення громадянина, подані документи, етапи розгляду зберігається в межах єдиного цифрового дизайну державності. Це означає, що людина може, наприклад, почати процедуру онлайн, а завершити її в центрі надання адміністративних послуг без повторного подання даних, або навпаки – подати документи офлайн, а відстежувати статус і отримати результат у цифровому форматі.

Для оцінки якості такої архітектури доцільно говорити про «систему точок взаємодії держави і громадянина в умовах цифрового суспільства». Під системою точок взаємодії розуміється сукупність усіх контактів громадянина з державними інституціями (онлайн і офлайн) та узгодженість цих контактів між собою. У термінах моделі державотворчих процесів це означає, що участь громадянина в державотворенні – від базових адміністративних дій до форм участі в ухваленні рішень – проєктується як безперервний, логічно пов'язаний шлях, а не як набір випадкових епізодів.

Сьомий вимір стосується методологічних і практичних перспектив подальшого розвитку системи державотворчих процесів. Йдеться про перехід

від простого переліку цифрових інструментів до аналізу режимів цифрового врядування – стійких конфігурацій, у яких поєднуються технології, організаційні структури, правові норми та практики участі громадян. У цьому контексті модель державотворчих процесів стає центральним аналітичним інструментом: вона дозволяє зрозуміти, як саме нові режими врядування трансформують логіку формування та відтворення державності, які ролі відводяться різним акторам, як переосмислюється співвідношення між центром і місцевим самоврядуванням, між державою та громадянським суспільством. Такий підхід відкриває низку напрямів для майбутніх досліджень: вивчення нерівномірності цифровізації в різних галузях публічного управління; розробка практичних індикаторів для вимірювання публічної чутливості цифрового дизайну державності; моделювання того, як цифрові рішення впливають на здатність держави до самовідновлення в умовах війни та гібридних загроз; аналіз динаміки цифрового суспільного контракту, зокрема балансу між безпекою, ефективністю, приватністю та участю.

Запропонований авторський методологічний підхід дозволяє побачити цифрову трансформацію державного управління як багатовимірний процес інтегрованого розвитку державності, що включає: 1) формування цифрового дизайну державності як нового способу публічної присутності; 2) переукладання цифрового суспільного контракту й управління полями керованої невизначеності; 3) подолання структурної фрагментованості цифрової інфраструктури й цифрового розриву довіри; 4) перехід від квазі- до реального цифрового дизайну, що вимірюється через матрицю публічної чутливості; зміцнення національного контуру самовідновлення; 5) розбудову гібридної архітектури публічної взаємодії та узгодженої системи точок взаємодії держави і громадянина. У центрі – модель державотворчих процесів, що дозволяє осмислити цифрову державу не як набір технічних рішень, а як динамічний спосіб формування, зміни й відтворення державності в умовах тривалих викликів та історичних зламів.

1.3. Сутність та особливості формування системи публічного управління в умовах цифровізації: соціальний вимір цифрового суспільства

В умовах правового режиму воєнного стану в Україні формується унікальний контекст, у якому цифрові технології стають критичним інструментом забезпечення обороноздатності, безперервності функціонування органів влади, координації дій та захисту громадян.

Соціальний вимір цифровізації публічного управління в Україні в умовах воєнного стану набуває особливої ваги, оскільки саме через цифрові інструменти держава забезпечує мінімально необхідний рівень безпеки, координації та соціальної підтримки громадян. Відповідно до Закону України «Про правовий режим воєнного стану» № 389-VIII від 12.05.2015 р. [118] та Указу Президента України від 24.02.2022 № 64/2022 про введення воєнного стану цифрові технології стають складовою механізмів реалізації повноважень органів публічної влади щодо захисту населення, організації оборони, підтримання життєдіяльності територіальних громад та критичної інфраструктури. У цьому контексті соціальний аспект цифровізації неможливо розглядати окремо від питань безпеки, прав людини та національної стійкості.

В умовах воєнного стану цифрові технології виконують низку критичних соціальних функцій (на думку С.Домбровської та інш.) [119]. *По-перше*, вони формують інфраструктуру базової безпеки громадян. Через цифрові сервіси здійснюється оперативне інформування населення про загрози, маршрути евакуації, правила поведінки в умовах надзвичайних ситуацій; фіксуються воєнні злочини, порушення прав людини та пошкодження об'єктів інфраструктури, що надалі стає основою для правового реагування та міжнародної адвокації. Значна частина цих процесів спирається на інформаційно-комунікаційні системи органів виконавчої влади, роботу яких уряд зобов'язаний забезпечити навіть в умовах воєнного

стану. Це закріплено в урядових рішеннях щодо функціонування державних електронних систем, реєстрів та електронної системи охорони здоров'я під час війни, де прямо визначається необхідність збереження доступності ключових сервісів для населення. Таким чином, мова йде про цифрові управлінські платформи, які стають каналом реалізації базових соціальних прав – на інформацію, соціальний захист, охорону здоров'я – в умовах, коли традиційні механізми взаємодії з державою порушені чи обмежені.

Окремий сегмент становлять цифрові інструменти реєстрації та супроводу внутрішньо переміщених осіб (ВПО), оформлення соціальних виплат, субсидій, гуманітарної допомоги. Вони дозволяють зменшити транзакційні витрати для найбільш уразливих категорій населення, забезпечити прозорість розподілу ресурсів і створити єдину базу даних для координації між центральними та місцевими органами влади, міжнародними організаціями та волонтерськими ініціативами.

По-друге, зазначені цифрові платформи забезпечують самоорганізацію локальних спільнот і волонтерських мереж, виступаючи каталізатором горизонтальної взаємодії та зростання соціального капіталу. Через соціальні мережі, месенджери, краудфандингові та логістичні платформи громадяни координують евакуаційні ініціативи, збір і доставку допомоги, підтримку військових, взаємодію між громадами. У результаті формується новий тип трикутника взаємодії «держава – громадянин – спільнота», в якому цифрові інструменти виконують роль «комунікаційної тканини», що пов'язує офіційні державні програми з ініціативами самоврядного управління. Держава, з одного боку, делегує частину функцій соціальної підтримки волонтерським і громадським структурам, а з іншого – отримує через цифрові канали зворотний зв'язок щодо реальних потреб населення. Такий формат взаємодії сприяє підвищенню довіри до публічної влади за умови, що цифрові сервіси працюють стабільно, прозоро й орієнтовані на користувача.

Водночас, інтенсивна цифровізація в умовах війни породжує ризики соціальної фрагментації самого цифрового суспільства. Загалом, цифрова

нерівність виявляється не лише в різному рівні доступу до інтернету й комунікаційних пристроїв, але й у відмінностях у цифрових компетентностях, а також у різній готовності та можливості користуватися електронними сервісами. Частина громадян – насамперед молодші, мешканці великих міст, працівники сфер, пов'язаних із ІКТ, – активно інтегруються в нові цифрові канали взаємодії з державою. Інша частина – особи похилого віку, мешканці територій з пошкодженою інфраструктурою, соціально вразливі групи – залишаються в зоні традиційних, повільніших і менш прозорих процедур.

Це призводить до формування диференційованих режимів взаємодії з державою: для одних громадян держава постає як «цифровий сервіс», доступний у смартфоні, для інших – як бюрократична структура, до якої необхідно фізично добиратися, збирати паперові документи, проходити складні процедури і чекати невизначений час. У соціальному вимірі така асиметрія прямо впливає на відчуття справедливості, включеності та довіри до публічної влади, оскільки досвід взаємодії з державою стає залежним не стільки від формально гарантованих прав, скільки від цифрових можливостей конкретної людини чи громади. Цифрова нерівність накладається й на територіальні диспропорції – громади, що мають кращу телекомунікаційну інфраструктуру, доступ до цифрових освітніх і сервісних програм, спроможні швидше адаптуватися до воєнних викликів. Це створює ризик появи «цифрових периферій».

У такій ситуації розбудова національної моделі стійкості (НМС) через цифрові технології є можливою лише на основі цілеспрямованої політики цифрової інклюзії. Йдеться про комплекс заходів, спрямованих на: 1) розширення фізичного доступу до інтернету та цифрової інфраструктури, зокрема в сільських громадах і зонах, що постраждали від бойових дій; 2) адаптацію інтерфейсів державних електронних сервісів до потреб людей з інвалідністю, осіб похилого віку, ВПО, маломобільних груп населення; забезпечення базового рівня цифрових компетентностей, необхідного для

безпечного та ефективного користування цифровими сервісами (табл. 1.10).

Таблиця 1.10

Концептуалізація засад формування національної моделі стійкості в умовах цифрового суспільства

Параметр (соціальний вимір)	Традиційна система публічного управління (до інтенсивної цифровізації)	Система публічного управління в умовах цифровізації та війни (цифрове суспільство)	Наслідки для формування НМС / резильєнтності
1	2	3	4
Канали комунікації «держава – громадянин»	Переважно офлайн: особисті звернення, паперова кореспонденція, стац. приймальні	Домінування цифрових каналів – портали послуг, мобільні додатки, месенджери, соціальні мережі	Підвищення швидкості та масовості комунікації, залежність від ЦІ й навичок користувачів
Доступ до соціальних послуг і захисту	Фізична присутність у ЦНАП, органах соцзахисту; тривалі процедури; територіальність	Електронні послуги та реєстри: онлайн-реєстрація ВПО, соцвиплат, гуманітарної допомоги; дистанційний доступ	Зростання оперативності й прозорості, ризик виключення груп без доступу (цифрова нерівність)
Соціальна інтеграція / само-організація спільнот	Інституційна опора на формальні організації (ГО, ОСН, партії); повільна мобілізація	Самоорганізація через ЦП, волонтерські чати, соцмережі; швидка горизонтальна мобілізація	Посилення соціального капіталу й взаємодопомоги, вплив неформальних цифрових лідерів
Соціальна нерівність	Класичні форми: майнова, територіальна, освітня; менший вплив цифрового фактору	Додається цифрова стратифікація, розрив за доступом до інтернету, пристроїв, інтенсивністю користування е-сервісами	Формування «цифрових центрів» і «цифрових периферій»; ризик закріплення нерівності в доступі до прав і послуг
Режими взаємодії з державою	Уніфіковані – усі проходять через схожі офлайн-процедури	Диференційовані – частина населення взаємодіє через цифрові сервіси, частина – через офлайн-канали	Розшарування досвіду взаємодії з державою, що впливає на відчуття справедливості та рівності
Довіра до публічної влади	Формується переважно через офіційні інститути, ЗМІ, особистий досвід взаємодії	Суттєво залежить від якості цифрових сервісів, стабільності роботи платформ та онлайн-комунікації	Ефективні цифрові сервіси стають ресурсом легітимації влади; непрозорість – тригером недовіри
Роль цифрових компетентностей	Не є критичною умовою доступу до більшості базових послуг; потрібні для специфічних сфер	Стають базовою передумовою участі в цифровому суспільстві: від доступу до послуг до політичної активності онлайн	Цифрові компетентності – платформа для реформ, але без інституційних змін не гарантують якості управління

Продовження таблиці 1.9

1	2	3	4
Стан вразливих груп	Вразливість зумовлена соціально-економічними і територіальними чинниками	Додатковий вимір – цифрова вразливість (відсутність доступу, навичок, пристроїв, безпечної поведінки онлайн)	Необхідність цільових політик цифрової інклюзії як елементу соціальної й національної безпеки
Роль локальних спільнот і волонтерів	Обмежена інструментальною базою та можливістю швидко координувати дії; сильна залежність від офлайн-заходів	Потужні цифрові волонтерські й громадські мережі, здатні оперативно закривати прогалини держави	Зростання значення партнерств «державна – спільнота – волонтери» для НМС; потреба в інституційному визнанні їхньої ролі
Швидкість і масштаб реагування на кризи	Обмежені пропускну здатністю офлайн-каналів, ручними процедурами, територіальною прив'язаністю	Масштабовані цифрові сервіси, масові онлайн-сповіщення, централізовані реєстри, аналітика даних у близькому до реального часі	Значне підвищення оперативності, але одночасно зростання ризиків при збоях цифрової інфраструктури (єдині точки відмови)
Форма участі громадян у публічній політиці	Переважно офлайн: збори, слухання, паперові петиції, участь через організації	Е-петиції, онлайн-консультації, цифрові кампанії, мобілізація в соцмережах, краудфандинг/краудсорсинг рішень	Розширення каналів участі, але нерівний доступ до них; ризик домінування «цифрової активної меншості»

Джерело: розроблено автором

Аналіз соціального виміру цифрового суспільства, відображений у таблиці 1.9, показує насамперед, що цифровізація не просто «оцифровує» наявні управлінські процеси, а перебудовує самі умови взаємодії між державою та суспільством, отже комунікація «державна – громадянин» переходить у цифрове середовище. При цьому варто виокремити такі властивості цифрового суспільства.

1. Доступ до соціальних послуг стає дистанційним, але не для всіх однаково [120]. Раніше отримання соціальної допомоги, статусу ВПО, субсидій тощо вимагало фізичної присутності в органах влади [121]. У цифровому суспільстві значна частина цих процедур переводиться в

онлайн-формат, що скорочує черги й пришвидшує ухвалення рішень. Однак для тих, хто не має доступу до цифрових сервісів, бар'єри фактично зростають: система стає зручнішою для «цифрово включених» і складнішою для «цифрово виключених». При цьому спільноти отримують нові можливості самоорганізації.

2. У традиційних умовах мобілізація громади спиралась на формальні структури (громадські організації, партії, органи самоорганізації населення) і була повільною (Є.Бородін, О.Поступна)[122], (О.Кравцов, В.Баштанник) [123]. У цифровому суспільстві локальні спільноти та волонтерські мережі організовуються через онлайн-платформи, чати, соціальні мережі, що дає змогу швидко збирати ресурси, координувати допомогу, реагувати на кризові ситуації. Це посилює соціальний капітал, але й зміщує центр впливу від класичних інститутів до мережових ініціатив. При цьому цифрова нерівність стає новим показником соціальної стратифікації. До традиційних форм нерівності (економічної, територіальної, освітньої) додається цифрова стратифікація: різний доступ до інтернету, сучасних пристроїв, різний рівень цифрових компетентностей, різна інтенсивність користування е-сервісами. У результаті формуються «цифрові центри» (насичені сервісами й навичками) та «цифрові периферії», де люди залишаються в межах повільних, офлайн-процедур. Це безпосередньо впливає на доступ до прав і послуг.

3. Режими взаємодії з державою стають нерівномірними, адже у доцифрову епоху більшість громадян проходила приблизно однакові офлайн-процедури (Д.Саганович) [124]. У цифровому суспільстві виникають два різні режими: перший – для тих, хто користується цифровими сервісами (швидко, зручно, прозоро); другий – для тих, хто змушений взаємодіяти традиційно (повільно, складно, з більшими витратами часу і ресурсів). Це різко диференціює щоденний досвід «зустрічі з державою», отже – впливає на сприйняття соціальної справедливості й рівності.

4. Довіра до влади все більше залежить від якості цифрових сервісів, адже, якщо раніше довіра формувалась через класичні інститути (ЗМІ,

офіційні заяви, офлайн-досвід), то в цифровому суспільстві ключове значення має досвід користування електронними послугами. Стабільні, зручні, прозорі сервіси підвищують довіру й легітимність влади; кризи, непрозорі алгоритми, складні інтерфейси – її підривають. Таким чином, цифрова держава стає «обличчям» публічної влади.

5. Цифрові компетентності перетворюються на базову умову участі в суспільстві, оскільки у традиційній системі цифрові навички були важливі переважно для окремих професійних сфер [125]. У цифровому суспільстві вони стають необхідною умовою доступу до послуг, інформації, можливостей участі в публічному житті. Проте, як показав аналіз проведеного у межах дослідження експертного опитування, сам по собі високий рівень цифрової грамотності населення не гарантує якісного публічного управління – потрібні інституційні зміни з боку держави.

6. Вразливі групи отримують додатковий – цифровий – вимір вразливості, адже якщо раніше їхня вразливість визначалася переважно соціально-економічними чинниками, то тепер додається цифровий компонент: брак навичок, відсутність пристроїв, страх чи недовіра до онлайн-сервісів, відсутність адаптованих інтерфейсів. Це вимагає від держави політики цифрової інклюзії як частини соціальної політики та політики безпеки.

7. Роль локальних спільнот і волонтерів у системі стійкості зростає, оскільки цифрові інструменти дозволяють волонтерам і громадам швидко компенсувати прогалини держави – у логістиці, соціальній підтримці, комунікації. У цифровому суспільстві вони стають невід’ємними суб’єктами публічного управління, навіть якщо формально не входять до системи органів влади.

8. Реагування на кризи стає швидшим, але залежнішим від технологій, і масові сповіщення, електронні реєстри, аналітика даних дають змогу швидко реагувати на надзвичайні ситуації. Водночас збої цифрової інфраструктури стають критичними – коли ламається цифрова система,

«ламається» й значна частина управління.

9. Форми участі громадян у політиці цифровізуються, до класичних офлайн-форм (збори, слухання, зустрічі) додаються електронні петиції, онлайн-консультації, цифрові кампанії в соцмережах. Це розширює потенціал залучення, але водночас створює ризик, що політичний голос матиме насамперед «цифрово активна меншість», тоді як менш цифрово включені групи залишаться на периферії участі.

Цифровізація публічного управління, що традиційно розглядається у контексті технологічної модернізації та оптимізації адміністративних процесів, насправді виявляє глибоко вкорінену соціальну детермінованість, яку неможливо ігнорувати при формуванні НМС. Актуалізація соціального виміру цифрової трансформації зумовлюється не лише необхідністю забезпечення інклюзивності та доступності цифрових послуг, але й фундаментальними змінами в архітектурі взаємодії між державою та громадянами, що особливо гостро проявляються в умовах системних криз. Соціальний детермінізм цифровізації як науковий концепт передбачає визнання визначального впливу соціальних структур, процесів та очікувань на вектори, моделі, темпи та результати цифрової трансформації публічного управління, а також зворотного впливу цифровізації на соціальну тканину суспільства та його стійкість до викликів.

Такий концепт проявляється насамперед у тому, що технологічні рішення, впроваджені в системі публічного управління, неминуче відображають та відтворюють соціальні ієрархії, нерівності, культурні патерни та поведінкові настанови. Алгоритми та цифрові інструменти, що використовуються для автоматизації управлінських процесів, не є нейтральними – вони інкорпорують соціальні упередження, владні відносини та домінуючі картини світу. Це призводить до появи феномену «алгоритмічного відбитку соціуму» (algorithmic societal imprint), який можна визначити як *сукупність соціальних цінностей, норм та структурних нерівностей, закодovаних у цифрових системах управління*. Емпіричні

спостереження за впровадженням цифрових платформ в Україні демонструють, що навіть найбільш технічно досконалі рішення можуть відтворювати або навіть посилювати наявні соціальні диспропорції. Наприклад, алгоритми розподілу гуманітарної допомоги або компенсацій за зруйноване житло, що ґрунтуються на здатності користувача взаємодіяти з цифровими інтерфейсами, можуть систематично дискримінувати громадян з обмеженими цифровими навичками. В українському контексті правовий режим воєнного стану посилює такі процеси, коли доступ до критично важливих державних сервісів виявляється нерівномірним для різних соціальних груп – внутрішньо переміщених осіб, мешканців прикордонних територій, людей старшого віку, осіб з інвалідністю.

Практика соціального детермінізму цифровізації актуалізує необхідність формування науково обґрунтованої методології оцінки та трансформації цифрових інструментів з позиції їхньої соціальної справедливості та внеску в національну стійкість. У цьому контексті доцільно запропонувати авторську категорію «матриця соціальної чутливості цифрових рішень» (social sensitivity matrix of digital solutions) – багатовимірну аналітичну рамку, що дозволяє оцінювати вплив цифрових інструментів публічного управління на різні соціальні групи та соціальну згуртованість у цілому. На нашу думку, така категорія включає такі параметри: 1) доступність цифрових рішень для різних соціально-демографічних груп з урахуванням територіальних, вікових, освітніх та майнових диференціацій; 2) врахування культурного та ціннісного різноманіття при проєктуванні інтерфейсів і сценаріїв взаємодії; 3) соціальні наслідки автоматизованих рішень; 4) потенціал цифрового інструменту для посилення соціальної згуртованості та довіри; 5) механізми громадянської участі у формуванні, тестуванні та оцінці цифрових рішень. Емпіричне застосування матриці до аналізу цифрових сервісів, впроваджених в Україні під час повномасштабної війни, виявляє нерівномірність їх соціального впливу: з одного боку, вони суттєво спростили доступ до державних послуг для цифрово компетентної

частини населення, з іншого – створили додаткові бар'єри для вразливих категорій громадян, особливо в умовах вимушеної мобільності та руйнування інфраструктури.

Респонсивний внутрішній зміст цифровізації публічного управління проявляється у здатності цифрових систем та інструментів динамічно адаптуватися до мінливих соціальних потреб, очікувань та контекстів. Респонсивність у цьому випадку виходить за межі реактивної адаптації та набуває характеру проактивного передбачення соціальних запитів і потенційних точок напруги. Для концептуалізації цього феномену пропонується авторська категорія «цифрова соціальна чутливість до змін» (digital social sensitivity to change) – властивість цифрових систем публічного управління функціонувати в режимі постійної готовності до зміни соціальних умов, очікувань та взаємодій, що забезпечує безперервність надання публічних послуг навіть за умов системної кризи. Така властивість реалізується через управлінські механізми: 1) модульність архітектури цифрових платформ, що дозволяє швидко інтегрувати нові функціональності відповідно до соціальних потреб; 2) гнучкість алгоритмів, здатних враховувати зміни в соціальному контексті; 3) інтероперабельність даних та сервісів, що забезпечує безшовну інтеграцію різних компонентів цифрової екосистеми; 4) мультиканальність взаємодії, яка дає можливість громадянам обирати найбільш зручні для них способи доступу до публічних послуг; 5) механізми громадянської участі у процесах проєктування та оцінки цифрових рішень.

Український досвід цифровізації публічного управління в умовах воєнного стану надає потужний емпіричний матеріал для дослідження цифрової соціальної контингентності. Платформа «Дія», що до початку повномасштабного вторгнення функціонувала переважно як сервіс для надання адміністративних послуг, продемонструвала високий рівень *цифрової соціальної чутливості до змін*, швидко трансформувалась у багатофункціональний інструмент кризового менеджменту, що забезпечує

реєстрацію внутрішньо переміщених осіб, подання заявок на компенсацію за зруйноване майно, оформлення допомоги для постраждалих, інформування про повітряні тривоги тощо. Водночас емпіричні спостереження виявляють обмеження цифрової соціальної чутливості – окремі соціальні групи, зокрема люди старшого віку, особи з низьким рівнем цифрових компетентностей, громадяни, що мешкають у районах з обмеженим доступом до інтернету або електроенергії, стикаються зі суттєвими бар'єрами у доступі до цифрових сервісів навіть при їх технічній адаптивності.

Для подолання зазначених обмежень та забезпечення інтегрального соціального виміру цифровізації публічного управління необхідно впроваджувати підхід, який можна визначити як соціальну контекстуалізацію цифрової архітектури (*social contextualization of digital architecture*) – як наукову категорію, що визначає процес системного впровадження соціального контексту, включаючи структурні нерівності, культурні особливості, поведінкові патерни та групові очікування, у проєктування, розгортання та оцінку цифрових систем публічного управління. Соціальна контекстуалізація передбачає: 1) залучення соціологів, психологів, фахівців з інклюзії до розробки технічних завдань та оцінки прототипів цифрових рішень; 2) соціальне картографування громад та груп користувачів з виявленням специфічних потреб та бар'єрів; 3) дослідження практик взаємодії різних соціальних груп з цифровими інтерфейсами; 4) розробку соціально диференційованих сценаріїв застосування цифрових рішень з урахуванням особливостей різних груп; 5) формування комплексної інфраструктури підтримки, що включає як цифрові канали, так і фізичні точки доступу та консультування.

Емпіричний аналіз впровадження цифрових рішень в українському публічному управлінні демонструє, що найбільш успішні з них характеризуються високим рівнем соціальної контекстуалізації. Наприклад, реєстрація внутрішньо переміщених осіб через застосунок «Дія» доповнюється можливістю особистого звернення до центрів надання

адміністративних послуг, де громадяни можуть отримати підтримку у заповненні електронних форм, що робить процес доступним для людей з різним рівнем цифрових компетентностей. Водночас, інші цифрові інструменти, впроваджені без належної соціальної контекстуалізації, стикаються з низьким рівнем прийняття та використання, що зменшує їхню ефективність для забезпечення національної стійкості.

Формування соціально детермінованого підходу до цифровізації публічного управління вимагає суттєвої трансформації як концептуальних рамок, так і практичних методологій розробки та впровадження цифрових рішень в сучасній науці державного управління. Замість технологічного детермінізму, що розглядає цифрові інновації як самоцінний процес, необхідно впроваджувати підхід *соціотехнічної еволюції*, який визнає взаємозалежність та взаємовплив соціальних та технологічних систем. Це передбачає не лише адаптацію цифрових інструментів до соціальних реалій, але й трансформацію соціальних практик, інституціональних структур та культурних патернів під впливом цифровізації.

Досвід України в умовах воєнного стану демонструє, що національна стійкість у цифровому вимірі досягається не через просту технологічну модернізацію державного управління, а через комплексну інтеграцію цифрових систем у соціальну тканину суспільства. Коли цифрові рішення резонують із соціальними очікуваннями та практиками, вони стають потужним інструментом забезпечення безперервності публічних послуг, підтримки соціальної згуртованості та посилення інституційної довіри навіть в умовах екстремальних викликів. І навпаки, технічно досконалі, але соціально нечутливі цифрові системи можуть створювати додаткові лінії розломів і напруги, послаблюючи колективну стійкість суспільства.

Практична імплементація концепту соціального детермінізму цифровізації вимагає розвитку нових методологічних підходів та інституційних механізмів. На методологічному рівні необхідно впроваджувати інструменти соціальної оцінки впливу цифрових рішень

(digital social impact assessment), що дозволяють аналізувати потенційні соціальні наслідки впровадження цифрових систем ще на етапі їх проектування. На інституційному рівні доцільне створення спеціалізованих структур (рад, комітетів, комісій), які б забезпечували експертизу цифрових рішень з позиції їхнього соціального впливу та інтегрованості в соціальний контекст.

Інтеграція соціального детермінізму цифровізації в національну модель стійкості дозволяє переосмислити саму природу цифрової трансформації публічного управління – від технократичного процесу оптимізації адміністративних процедур до комплексного соціотехнічного феномену, що трансформує не лише інструменти управління, але й саму природу відносин між державою та суспільством. У цій перспективі цифровізація стає не просто технологічним доповненням до традиційних управлінських практик, а фундаментально новим способом конституювання публічної влади та забезпечення її легітимності в цифрову епоху.

Таким чином, соціальний детермінізм цифровізації публічного управління виступає не просто теоретичним концептом, а практичним інструментом забезпечення національної стійкості через формування респонсивних, соціально чутливих та контекстуально вкорінених цифрових екосистем. Запропоновані авторські категорії – матриця соціальної чутливості цифрових рішень, цифрова соціальна контингентність та соціальна контекстуалізація цифрової архітектури – створюють концептуальний каркас для розбудови теоретично обґрунтованих та емпірично валідних підходів до цифровізації, орієнтованих на посилення соціальної згуртованості, інклюзивності та колективної стійкості.

Концептуалізація та практичне втілення соціального детермінізму цифровізації дозволяє подолати дуалізм між технологічними та соціальними аспектами національної моделі стійкості, розглядаючи їх як взаємозалежні та взаємодоповнюючі елементи єдиної системи. Саме така інтегральна перспектива забезпечує формування цілісної, динамічної та адаптивної

системи публічного управління, здатної ефективно функціонувати в умовах гібридних загроз, системних криз та нестабільності, характерних для сучасного глобалізованого світу.

Отже, аналіз показав, що цифрове суспільство радикально змінює соціальні умови функціонування публічного управління: відкриває великі можливості для інтеграції, швидкої допомоги, прозорості й участі, але одночасно створює нові форми нерівності, уразливості та залежності від технологій. Тому формування системи публічного управління в цифровому суспільстві має спиратися не лише на технічні рішення, а й на цілеспрямовану соціальну політику цифрової інклюзії, підтримку цифрових компетентностей і інституційні механізми захисту тих, хто ризикує опинитися «поза цифровою державою».

Розглядаючи ці процеси в більш широкому контексті становлення цифрового суспільства, варто стверджувати, що йдеться не лише про зміну технічних інструментів комунікації, а про глибинну трансформацію соціальної структури держави, у межах якої відтворюються статуси, ролі, ідентичності та владні відносини. Цифрові управлінські платформи, електронні сервіси, інформаційно-комунікаційні системи стають для значної частини населення основним середовищем взаємодії з державою, отримання послуг, організації повсякденного життя. Водночас інша частина громадян через об'єктивні (територіальні, матеріальні, вікові, освітні, мовні) та суб'єктивні (рівень мотивації, цифрової тривожності, недовіри до держави) чинники залишається на периферії цих процесів, зберігаючи залежність від повільніших, менш прозорих і часто принизливих офлайн-процедур. У таких умовах цифрові технології, що декларуються як універсальний засіб розширення можливостей людини й підвищення якості публічного управління, фактично перетворюються на потужний механізм соціального сортування, коли доступ до ресурсів, послуг і каналів участі дедалі більше залежить від здатності особи орієнтуватися в цифровому середовищі, володіти відповідними навичками, мати матеріальний доступ до пристроїв та

інтернету. Це породжує нові лінії розмежування між «цифрово включеними» та «цифрово виключеними» громадянами й громадами, які з часом ризикують закріпитися на інституційному рівні, впливаючи на відтворення нерівності у міжпоколінньому вимірі.

За таких умов стає очевидним, що подолання зазначених суперечностей неможливе ані шляхом суто технічної модернізації державних інформаційних систем, ані через стихійне поширення цифрових сервісів на ринкових засадах. Необхідним є цілеспрямований вплив державної політики, яка б системно поєднувала розвиток цифрової інфраструктури з розширенням людського потенціалу її використання, орієнтуючись не лише на економічні показники, але й на соціальну справедливість, інклюзію та захист прав людини в цифровому середовищі. Інакше кажучи, цифровізація державного управління має супроводжуватися формуванням такої моделі взаємодії «держава – громадянин – спільнота», у якій кожна особа, незалежно від місця проживання, віку, соціального статусу чи стану здоров'я, матиме реальну, а не декларативну можливість користуватися цифровими інструментами на рівні, достатньому для реалізації своїх базових прав і свобод. Це, у свою чергу, передбачає переорієнтацію політики цифрового розвитку з вузького фокусу на технологічних інноваціях до людиноцентричної парадигми, де ключовим ресурсом виступають не стільки платформи та сервіси самі по собі, скільки спроможність громадян безпечно, відповідально й результативно їх використовувати. У такій парадигмі цифрові компетентності перестають бути допоміжним елементом освітньої чи кадрової політики й набувають статусу стратегічної умови соціальної цілісності, демократичної участі та національної стійкості, особливо в умовах війни, коли значна частина критично важливих процесів (евакуація, соціальний захист, комунікація з органами влади, доступ до медицини, освіти, гуманітарної допомоги) переноситься в онлайн-формат. Тому державна політика, спрямована на формування цифрового суспільства, має включати не лише розбудову мереж і сервісів, а й чітко окреслені нормативні

орієнтири щодо розвитку цифрових компетентностей як універсального соціального мінімуму, без якого неможливо гарантувати реальну, а не формальну рівність громадян перед цифровою державою. Саме на цьому перетині – між соціальними викликами цифровізації та необхідністю інституційної відповіді – постає потреба у концептуальному й правовому закріпленні державної політики у сфері цифрових компетентностей, яка б задала єдині рамки для дій органів влади, освітніх установ, роботодавців та громадського сектору, забезпечуючи скоординоване підвищення спроможності суспільства жити й взаємодіяти в цифровому середовищі.

На нормативному рівні орієнтири такої політики зафіксовані в Концепції розвитку цифрових компетентностей, схваленій розпорядженням Кабінету Міністрів України від 03.03.2021 № 167-р. У розпорядженні цифрова компетентність визначається як динамічна комбінація знань, умінь і навичок, що дає змогу особі безпечно, відповідально та результативно використовувати цифрові технології в усіх сферах життя. Концепція прямо наголошує на необхідності розвитку цифрових компетентностей не лише у працівників державного сектору, а й у широких верств населення – від здобувачів освіти до осіб похилого віку, що створює підґрунтя для формування більш інклюзивної цифрової взаємодії «держава – громадянин» [126]. Основною метою цієї Концепції є визначення пріоритетних напрямів і основних завдань з питань розвитку цифрових навичок та цифрових компетентностей, підвищення рівня цифрової грамотності населення, зокрема працездатних осіб, громадян похилого віку, малозабезпечених сімей, осіб з інвалідністю, інших вразливих груп населення, в умовах розвитку цифрової економіки та цифрового суспільства. Реалізація цієї Концепції передбачена на період до 2025 року.

Водночас, сам по собі високий рівень цифрової грамотності населення не є достатнім чинником публічно-управлінських реформ. Цифрові компетентності виступають платформою, на якій можливе впровадження складніших елементів загальносистемних державно-управлінських

перетворень – від електронної ідентифікації та електронних довірчих послуг до інструментів електронної демократії (електронні петиції, консультації з громадськістю, електронне голосування тощо). Без паралельної інституційної модернізації органів влади, зміни організаційної культури та оновлення правового регулювання цифрове підвищення компетентностей населення не трансформується автоматично в підвищення якості публічного управління.

Таким чином, соціальний аспект цифровізації системи публічного управління в умовах воєнного стану в Україні має подвійний характер: З одного боку, цифрові технології забезпечують: інфраструктуру базової безпеки, доступ до критично важливих соціальних послуг і захисту; нові форми самоорганізації громадян і спільнот, посилення соціального капіталу та горизонтальної взаємодії; можливість оперативного поєднання локальних ініціатив з державними програмами підтримки. З іншого боку, вони: поглиблюють наявні і створюють нові форми цифрової та соціальної нерівності; формують диференційовані режими взаємодії з державою, що впливають на відчуття справедливості та довіри; ризикують закріпити поділ на «цифрові центри» і «цифрові периферії», якщо політика цифрової інклюзії буде фрагментарною.

У цьому контексті соціальний вимір цифрової інтеграції та фрагментації спільнот виступає ключовим критерієм оцінки успішності цифрових реформ у сфері державного управління. Без системної підтримки цифрової інклюзії, розвитку компетентностей і зменшення структурної нерівності цифрові інструменти можуть одночасно посилювати як стійкість держави й суспільства, так і їхню внутрішню розшарованість, що суперечить стратегічним завданням формування національної моделі стійкості в умовах тривалої війни. Аналіз соціального виміру цифровізації в умовах воєнного стану дає змогу побачити подвійний ефект цифрових технологій: з одного боку, вони посилюють інтеграційні процеси, забезпечують базову безпеку громадян, розширюють можливості самоорганізації спільнот; з іншого – поглиблюють структурну нерівність, формують різні режими доступу до

публічних послуг і механізмів участі, створюють ризики соціальної фрагментації. Така амбівалентність не може бути адекватно осмислена лише в межах техніко-управлінського підходу, який розглядає цифровізацію як інструмент оптимізації діяльності органів влади. Вона вимагає ширшої аналітичної рамки, у межах якої цифрові технології постають не як зовнішній додаток до «традиційного» суспільства, а як середовище, в якому відбувається відтворення соціальних структур, норм, ідентичностей та владних відносин.

Саме тому наступним кроком є уточнення змісту поняття «цифрове суспільство», яке дедалі частіше використовується у вітчизняних нормативно-правових актах (зокрема, у Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки [127], Концепції розвитку цифрових компетентностей тощо), але не завжди супроводжується достатньо чітким теоретичним наповненням. Для цілей даного дослідження важливо не лише зафіксувати загальне визначення цифрового суспільства, а й показати, яким чином перехід до цифрового суспільства змінює умови формування та функціонування системи публічного управління, зокрема в екстремальному контексті воєнного стану та розбудови національної моделі стійкості.

1.4. Формування механізмів національного розвитку у межах НМС шляхом інтеграції цифрових технологій у систему державного управління

У межах НМС цифрові технології перестають бути лише інструментом технічної модернізації державних сервісів. Вони поступово перетворюються на канал формування нових механізмів національного розвитку, які поєднують цілі безпеки, соціальної згуртованості, економічного зростання й демократичної участі. Саме тому дослідження інтеграції цифрових технологій у систему державного управління доцільно проводити не тільки в категоріях «ефективності послуг», а й у категоріях стійкості та розвитку.

надходить повільно, часто в агрегованому вигляді, із великими часовими затримками (Л.Антонова) [130-131]. Статистичні звіти, паперові обліки, дискретні політичні цикли фактично формують формат управління з довгим «мертвим часом», що робить реакцію на кризу (зовнішню чи внутрішню) запізненою. Натомість, інтеграція цифрових технологій змінює цю конфігурацію – електронні реєстри, онлайн-кабінети, системи моніторингу інфраструктури, геоінформаційні платформи виступають як сенсори, які фіксують стан підсистем у режимі, наближеному до реального часу; захищені мережі зв'язку, мобільні та супутникові канали забезпечують передавання цих даних до центрів обробки; аналітичні платформи й панелі моніторингу виконують функції блоку обробки сигналів; рішення уряду, органів місцевого самоврядування й спеціалізованих служб стають елементами виконавчих механізмів [132]. У результаті формується низка замкнених контурів зворотного зв'язку різних рівнів – від загальнодержавного до локального, що підвищує як аналіз, так і керованість усієї системи.

Зростання функції моніторингу особливо виразно проявляється в галузях, де цифрові сенсори вже інтегровані в критичну інфраструктуру [133]. В енергетичній системі – це комплекси диспетчерського управління, датчики навантаження на підстанціях, «розумні» лічильники, дані з яких дозволяють операторам у режимі реального часу бачити структуру споживання, аварійні відключення, критичні перевантаження. При масованих ударах по енергетиці це означає, що система не «сліпа»: вона здатна локалізувати ушкодження, оперативно перебудовувати схеми постачання, балансувати навантаження між регіонами, мінімізуючи відхилення від цільового режиму (таблиця 1.10).

Таблиця 1.11

«Матриця моніторингу» НМС до та після інтеграції цифрових технологій

Вимір / параметр	Традиційний моніторинг НМС (до цифрової інтеграції)	Цифрово-інтегрований моніторинг НМС (на основі ЦТ)
Джерела даних («сенсори»)	Паперові звіти, періодична статистика, телефонні довідки, вибіркові інспекції	Е-реєстри, онлайн-кабінети, ГІС, мобільні застосунки, платформи звернень громадян
Частота оновлення	Низька – дані надходять із затримкою в тижні/місяці	Висока (оновлення близьке до реального часу)
Рівень деталізації	Агреговані показники по країні/регіону; мало даних на рівні громади чи домогосподарства	Деталізація до рівня громади, кварталу, об'єкта, домогосподарства (за потреби – до індивідуального рівня)
Просторова прив'язка даних	Обмежена, часто без точної геолокації; карти – статичні	Точна геоприв'язка (ГІС, інтерактивні мапи руйнувань, мереж, укриттів), динамічна просторово-часова картина
Типи показників	Переважно кількісні підсумкові (скільки постраждалих, скільки об'єктів тощо)	Поєднання кількісних та процесних: потоки міграції, динаміка навантаження, черги, часові ряди подій
Доступність для різних рівнів влади	Сегментований доступ; частина даних «замикається» на окремих відомствах	Регламентований міжвідомчий доступ; спільні панелі для уряду, регіонів і громад
Роль громад і локальних спільнот	Пасивні респонденти опитувань; рідко – ініціатори офіційних сигналів	Активні «сенсори» через платформи скарг, мапування проблем, волонтерські боти, локальний збір даних
Точність та повнота картини	Високий ризик спотворень: застарілі, неповні, несумісні дані	Більш повна й цілісна картина завдяки інтеграції кількох джерел та автоматизованій перевірці узгодженості
Своєчасність управлінських рішень	Рішення ухвалюються із запізненням, часто за «старою» інформацією	Можливе оперативне реагування та корекція політик на основі актуальних даних
Тип управління	Переважно управління «за програмою» з великим «мертвим часом»	Замкнуті контури зі зворотним зв'язком, можливістю адаптивного регулювання
Оцінка стану НМС	Фрагментарна «статична фотографія» ситуації	Динамічний, багатовимірний «образ стану» з можливістю простежити еволюцію у часі
Можливості прогнозування	Обмежені – здебільшого екстраполяція агрегованих трендів	Розширені (сценарне моделювання, короткострокові прогнози на основі даних)
Наслідки для стійкості (резильєнтності)	Висока ймовірність запізнилої реакції, «перегріву» окремих підсистем, недооцінки ризиків	Підвищена здатність завчасно виявляти загрози, точніше локалізувати проблеми й координувати відповіді

Джерело: дослідження автора

Аналогічні ефекти спостерігаються в соціальній сфері, де електронні кабінети одержувачів допомог, реєстри внутрішньо переміщених осіб, цифрова фіксація відвідувань центрів надання адміністративних послуг дають змогу бачити реальне навантаження на систему, профіль потреб, тривалість очікування, типові причини відмов. Таким чином, підвищується ранг «матриці моніторингу» НМС: держава й громади отримують якісно інший, більш деталізований і своєчасний образ власного стану.

Водночас, посилюється й керованість, тобто здатність регулятора, оперуючи доступними йому входами, переводити систему з одного стану в інший за прийнятний час. Цифрові платформи для нарахування й виплати допомог, інтегровані з банківськими системами, фактично перетворюються на виконавчі механізми: при ухваленні рішення про підтримку певної категорії населення інформація з реєстрів автоматично визначає коло одержувачів, а виплати ініціюються пакетно, скорочуючи часовий розрив між політичним рішенням і фактичним посиленням соціальної захищеності. Аналогічно, цифрові системи управління транспортом, сервіси навігації та мапування укриттів чи пунктів евакуації дозволяють місцевій владі й силовим структурам оперативно змінювати маршрути, режими роботи світлофорів, відкривати тимчасові пункти прийому людей, а населенню – миттєво одержувати сигнали про зміни. Це запобігає надмірним коливанням, пов'язаним із хаотичною, некоординованою реакцією.

Ключову роль відіграє і зворотний зв'язок, без якого будь-яка складна система управління втрачає здатність до самокорекції. У цифровому середовищі канали фідбеку набувають різних форм – від формалізованих електронних сервісів «повідом про проблему» до електронних петицій, громадських консультацій і аналітики соціальних мереж. Платформи, у межах функціонування яких мешканці фіксують локальні проблеми – перебої водопостачання, несправне освітлення, загрозливі об'єкти, – створюють локальні замкнені контури зворотного зв'язку, в яких сигнал про відхилення генерується безпосередньо в точці його виникнення, а виконавці працюють із

чергою інцидентів у цифровому вигляді. Аналогічно, при плануванні відновлення територій онлайн-опитування, інтерактивні мапи руйнувань, платформи громадського обговорення дозволяють зменшити систематичну похибку моделі розвитку, оскільки локальні знання та пріоритети включаються в процес прийняття рішень, а не ігноруються. Усе це скорочує затримки в контурі й наближує поведінку системи до цільового режиму, заданого стратегіями стійкого розвитку та відновлення.

У контексті *авторського підходу до поняття стійкості* власне національна стійкість проявляється через низку характеристик: здатність системи повертатися до прийнятних значень ключових показників після збурень, збереження стабільності за умов невизначеності параметрів і зовнішніх впливів, наявність механізмів адаптації й самоналаштування, достатній рівень резервування та дублювання критичних елементів. Цифрові технології потенційно підсилюють усі ці властивості:

- завдяки розгалуженій мережі сенсорів і каналів зв'язку система швидше виявляє відхилення;
- завдяки гнучким цифровим виконавчим механізмам (масові виплати, переналаштування інфраструктури, оперативна релокація послуг) вона скорочує тривалість і глибину кризових режимів;
- завдяки даним і моделям держава здатна переходити від реактивної до проактивної логіки управління ризиками.

Проте ці переваги реалізуються лише за умови належного інституційного «налаштування регулятора» – тобто розвиненого цифрового врядування з чітким розподілом повноважень, процедур координації та прозорими правилами використання даних. Саме в цій площині проявляється структурна проблема самої системи державного управління – *за наявності множини стратегій цифрової трансформації відсутнє цілісне бачення того, як ці стратегії працюють на результатність як системну мету.*

Велика кількість цифрових проєктів створюють локальні контури управління, але між ними бракує узгодженої ієрархії й єдиного «верхнього

контролера», який задавав би інваріантні орієнтири стійкості для різних секторів – енергетики, соціальної політики, безпеки, інфраструктури. Міністерства, агенції, органи місцевого самоврядування впроваджують окремі реєстри, платформи, сервіси, але без стандартизованих протоколів обміну даними, загальної моделі оцінки ризиків і спільної цільової функції щодо зменшення системної вразливості ці елементи не складаються в єдину захищену систему. З погляду базових концептів теорії управління, маємо низку частково керованих підсистем із власними, часом суперечливими цілями, і недостатньо синтезований надсистемний регулятор, покликаний координувати їхню взаємодію (А.Макурін) [134].

На цьому фоні цифрові компетентності суспільства відіграють подвійно амбівалентну роль. З одного боку, вони справді розширюють реальний ступінь свободи управління: громадяни, які вільно користуються е-сервісами, здатні швидко подавати заявки, надавати дані, брати участь у консультаціях, реагувати на сигнали небезпеки; посадовці з відповідними навичками не обмежуються механічним заповненням форм, а можуть інтерпретувати аналітику, ініціювати зміни в процедурах, застосовувати інструменти моделювання. З іншого боку, навіть високий рівень таких компетентностей не автоматично змінює структуру контурів управління. Якщо інституційні процедури лишаються інертними, орієнтованими на паперову логіку, якщо дані збираються, але не використовуються як підстава для коригування політик, якщо зворотний зв'язок із громадянами радше формальний, ніж дієвий, цифрові навички населення й чиновників частково втрачають свій потенціал, перетворюючись на внутрішній, але невикористаний ресурс системи.

Реальна практика підтверджує цю тезу. Навіть там, де населення активно користується мобільними застосунками, онлайн-банкінгом, цифровими каналами комунікації, нерідко зберігаються дублювальні паперові процедури, вимоги особистого відвідування установ, застарілі нормативні обмеження. Виходить, що контур управління на рівні

повсякденних взаємодій потенційно може працювати значно швидше й точніше, ніж дозволяє чинний регулятор. Умовно кажучи, «математична модель» припускає більш ефективне керування, але управлінський регулятор насичений нелінійними обмеженнями: бюрократичними бар'єрами, консервативними практиками, відсутністю політичної волі до зміни процедур. Те саме стосується й ситуацій, коли держава декларує цифрову участь громадян – через електронні петиції, онлайн-консультації, голосування, – але не вбудовує результати такої участі у формальні механізми бюджетного планування, стратегічного розвитку чи регуляторної політики (Г.Блінова) [135]. У такому випадку цифрові канали генерують зворотний зв'язок, проте він не замикає контур взаємодії (практично відсутня платформа), не змінює поведінку регулятора, і тому системно не впливає на стійкість.

Застосування авторської методології формування НМС до аналізу інтеграції цифрових технологій у державне управління дозволяє пояснити власне сам феномен національної моделі стійкості. Йдеться не лише про накопичення цифрових рішень і розширення спектра е-послуг, а про послідовне проектування контурів спостереження, впливу та зворотного зв'язку в системі державного управління таким чином, щоб система зберігала стабільність і була здатна до адаптації за широкого діапазону змінних параметрів. Особливі механізми національного розвитку в межах НМС формуються саме на перетині трьох вимірів: 1) технічного (цифрова інфраструктура як сукупність сенсорів, каналів і виконавчих пристроїв), 2) соціального (цифрові компетентності як потенціал залучення людей до цих контурів) та 3) інституційного (цифрове врядування як налаштований регулятор із чітко заданими цілями стійкості й розвитку). Поки один із цих вимірів істотно відстає, цифровізація лишається фрагментованою й не здатна повною мірою виконати функцію «нервової системи» НМС.

Отже, інтеграція цифрових технологій у державне управління створює передумови для якісно нових механізмів національного розвитку, але

реалізація цього потенціалу залежить від здатності держави й суспільства сприймати цифровізацію не як сукупність технічних проєктів, а як процес побудови адаптивних і багатоконтурних систем державного управління. Лише в цьому випадку цифрові сервіси, платформи й дані перестають бути набором розрізнених інновацій і починають працювати як інтегрована архітектура НМС, у якій цифрові компетентності населення, нормативне закріплення політики цифрового розвитку та інституційне оформлення цифрового врядування виступають взаємодоповнювальними складовими єдиного, науково обґрунтованого підходу до забезпечення стійкості та розвитку держави. У подальшому аналізі це відкриває простір для конкретизації інструментів – від нормативних актів до освітніх програм і технічних стандартів, – які мають узгоджуватися між собою як елементи комплексної схеми управління, а не випадкова, спорадична сума державних реформ у «цифровій» площині (навіть якщо такі реформи є реальними).

НМС доцільно формалізувати як складну керовану систему, яка має зберігати прийнятний рівень сукупності ключових показників навіть за умов тривалих і різноспрямованих потрясінь. Ідеться не лише про фізичну безпеку людей, а й про безперервність публічних послуг, працездатність критичної інфраструктури, рівень довіри та згуртованості у суспільстві, загальну економічну стабільність і зайнятість. Кожен із цих показників активно реагує, на нашу думку, на три групи чинників:

по-перше, на управлінські дії держави й органів місцевого самоврядування (рішення уряду, програми відновлення, регуляторні зміни, перерозподіл ресурсів),

по-друге, на внутрішню динаміку інститутів (інерційність бюрократії, стійкість звичних практик, культурні норми, що визначають готовність до самоорганізації, на можливість та реальну здатність громад),

по-третє, на зовнішні «силові впливи» – удари по енергосистемі, раптові хвилі внутрішньої міграції, інформаційні атаки, економічні потрясіння, природні катастрофи.

Очевидно, що безперервність публічних послуг залежить від цифровізації й резервування, від гнучкості процедур, від опору служб змінам, а також від таких збурень, як масові відключення електроенергії або гібридні кібератаки на реєстри й комунальні системи (Є.Красников) [136]. У державі, де цифрові механізми слабо розвинені, система управління спирається на повільні, фрагментарні й часто неточні сигнали про стан усіх цих показників. Реакція на зовнішні впливи базується переважно на паперовій статистиці, епізодичних інспекціях, річних звітах, поодиноких скаргах, а також на політичних циклах – від виборів до кампаній «показового» наведення ладу. Такий режим функціонування створює великі часові розриви між моментом, коли проблема реально виникає, і моментом, коли про неї дізнається керівництво та починає діяти. Наприклад, різке зростання навантаження на школи чи лікарні в окремому місті через наплив переселенців стає видимим для центральної влади лише після того, як місцева система вже працює на межі колапсу: черги, перевантажені класи, відсутність ліків, виснаження персоналу. Або дефіцит електроенергії, що спершу проявляється у вигляді локальних аварій, може залишатися непоміченим на національному рівні, доки не переростає у широкомасштабні відключення з політичними наслідками. У такому форматі вся система поводить як великий, інерційний об'єкт із довгими затримками у зворотному зв'язку: події на «полі» відбуваються швидко, а управлінська реакція приходить пізно й часто у формі надто грубих рішень.

Інтеграція цифрових технологій, на думку Г.Ортіної, змінює саму архітектуру державного управління [137]. На першому етапі з'являється набір сенсорів, які фіксують події й стани безпосередньо в точках їхнього виникнення:

- електронні реєстри, де в режимі майже реального часу оновлюються дані про населення, платників податків, одержувачів виплат, внутрішньо переміщених осіб, пошкоджене майно.
- інформаційні системи моніторингу в енергетиці, водопостачанні,

транспорті, які збирають показники з тисяч об'єктів; геоінформаційні карти, що відображають реальний стан доріг, мостів, укриттів, пунктів незламності;

- онлайн-кабінети, через які громадяни й бізнес постійно генерують сигнали – подають заяви, скарги, запити, звернення, – кожен із яких стає даними;

- мобільні застосунки, через які люди самі повідомляють про проблеми: від відсутності світла чи тепла у конкретному будинку до небезпечних об'єктів, руйнувань, фактів мародерства.

На наступному етапі ці дані мають бути передані до центрів прийняття рішень. Для цього розгортаються відповідні захищені цифрові канали зв'язку, міжвідомчі платформи обміну інформацією, інтегровані системи електронної взаємодії між міністерствами, регіональними адміністраціями, громадами. Наприклад, електронна система розподілу гуманітарної допомоги дозволяє областям і громадам вносити свої потреби, а центру – бачити сумарну картину, уникати дублювань, контролювати маршрут кожної партії вантажу. Аналогічно, міжвідомча платформа з даними про пошкоджену та відновлену інфраструктуру поєднує інформацію від дорожніх служб, енергетиків, місцевої влади, що дає змогу вибудовувати пріоритети ремонту не всліпу, а з урахуванням реальної завантаженості мереж і потреб населення.

Третім елементом такої архітектури стає блок обробки й аналізу урядової інформації. Це не лише статистичні зведення, а й інтерактивні панелі для уряду, регіонів і великих громад, де візуалізуються ключові показники: зміна кількості переселенців по населених пунктах, навантаження на медичні заклади, ступінь ушкодження житла, динаміка аварій у мережах, виконання планів відбудови. До цього додаються моделі прогнозу: наприклад, оцінюється, як збільшиться навантаження на школи й лікарні, якщо у певний регіон за кілька тижнів прибуде ще одна хвиля людей з прифронтових територій; чи витримає локальна енергосистема, якщо температури опустяться нижче прогнозу; як вплине закриття певних

підприємств на зайнятість та податкові надходження. Такі моделі дозволяють не лише бачити поточну картину, а й заздалегідь готувати керувальні рішення.

Четвертий елемент – виконавчий рівень, де рішення реалізуються через цифрові механізми. Коли ухвалюють рішення підтримати певну групу населення, наприклад сім'ї з дітьми в особливо постраждалих громадах, цифрові реєстри дозволяють швидко ідентифікувати потрібних отримувачів, банки – миттєво перерахувати кошти, а онлайн-кабінети – довести інформацію до людей. У сфері інфраструктури цифрові системи керування дають змогу перепідключити споживачів до інших ліній, змінити графіки постачання, автоматично переналаштувати режими роботи обладнання. Місцева влада за допомогою мобільних застосунків може централізовано інформувати мешканців про зміни в розкладах транспорту, роботі укриттів, пунктах видачі допомоги. В усіх цих випадках те, що раніше вимагало тижнів чи місяців, скорочується до днів, годин, а іноді й хвилин.

Як наслідок – формується кілька взаємопов'язаних контурів управління з позицій функціоналу НМС. На загальнонаціональному рівні центральні органи влади встановлюють довгострокові цілі, розподіляють ресурси, визначають загальні правила гри. На регіональному рівні області узгоджують між собою потреби й резерви громад, спрямовують допомогу туди, де система найбільше напружена, приймають проміжні рішення щодо логістики, розміщення людей, координації служб. На локальному рівні громади разом із волонтерами й місцевим бізнесом забезпечують щоденне функціонування шкіл, лікарень, транспорту, реагують на дрібні, але численні збурення – від аварій на мережах до конфліктів навколо розподілу допомоги. Кожен із цих рівнів має власні канали отримання сигналів, власні механізми впливу й свої горизонти планування.

При цьому саме цифрові технології дозволяють замкнути ці рівні між собою: дані знизу піднімаються вгору майже без посередників, а стратегічні рішення зверху швидко транслуються в конкретні дії на місцях [138]. Щоб

узагальнити логіку концептуалізації національної стійкості, доречно подати її у вигляді порівняльної таблиці, де зіставляються дві конфігурації: традиційна, по суті інерційна й слабо пов'язана, та багатоконтурна – цифрово інтегрована (таблиця 1.12).

Таблиця 1.12

Порівняльний аналіз систем управління стійкістю

Вимір / елемент	Традиційна інерційна система управління стійкістю	Багатоконтурна цифрово інтегрована система стійкості
Структура управління	Один домінуючий верхній рівень, слабкі горизонтальні зв'язки; громади – переважно «виконавці» рішень зверху	Три взаємопов'язані рівні (національний, регіональний, локальний) з власними контурами прийняття рішень і узгодженими ролями
Джерела інформації про стан системи	Паперові звіти, рідкісні інспекції, неформальні сигнали	Електронні реєстри, онлайн-кабінети, системи моніторингу інфраструктури, мобільні застосунки, платформи звернень
Швидкість зворотного зв'язку	Високі затримки: проблеми стають видимими лише в агрегованих звітах	Оперативний зворотний зв'язок: дані надходять постійно з усіх рівнів, у тому числі від громадян і волонтерів
Керувальні дії на національному рівні	Переважно нормативні зміни, програми «на рік», що погано враховують поточну динаміку	Гнучкі програми з можливістю оперативної корекції, масові цифрові виплати, централізоване керування окремими інфраструктурними режимами
Роль регіону	Транзитний рівень між центром і громадами, часто з обмеженими власними інструментами	Активний координаційний центр, що балансує потреби й ресурси громад, управляє навантаженням на інфраструктуру, працює з даними в реальному часі
Роль громади	Виконання інструкцій і звітування «наверх»; слабка можливість формувати власні рішення	Повноцінний контур управління з цифровими інструментами збору даних, планування, комунікації з мешканцями й волонтерами
Реакція на кризи безпеки (удари, загрози)	Запізнілі рішення, відсутність повної картини, хаотичне залучення ресурсів	Оперативна локалізація ушкоджень, пріоритезація критичних об'єктів, узгоджені дії між рівнями, інформаційна підтримка населення в цифрових каналах
Реакція на гуманітарні збурення (міграція, нестача послуг)	Нерівномірний розподіл навантаження, диспропорція громад, конфлікти через розподіл державної допомоги	Кероване розміщення людей, прозорий розподіл підтримки, постійне коригування програм на основі актуальних даних

Продовження таблиці 1.12

Вимір / елемент	Традиційна система стійкості	інерційна управління система стійкості	Багатоконтурна цифрово інтегрована система стійкості
Вплив на довіру та згуртованість	Часте відчуття безпорадності й несправедливості, посилення розриву між центром і місцями		Поява відчуття залученості та впливу, зростання довіри до цифрових сервісів і до рішень, що спираються на видимі дані
Загальна здатність утримувати ключові показники в прийнятних межах	Схильність до затяжних криз, коли система «перегрівается», а відновлення триває довго		Збільшення стійкості: швидке виявлення проблем, гнучка реакція, краще узгодження дій між рівнями, менші втрати від збурень

Джерело: дослідження автора

Якщо система державного управління працює як єдина багатоконтурна модель, усі три рівні реагують узгоджено: держава швидше виділяє кошти й спрощує процедури, область розподіляє навантаження між громадами, громади організовують розселення та інтеграцію людей. У такому форматі національна модель стійкості постає як багатоконтурна система, в якій цифрові технології не є самодостатньою «панацеєю», але радикально змінюють правила гри, дозволяють побудувати розгалужену мережу зворотних зв'язків, скоротити часові затримки, зробити видимими ті параметри, які раніше залишалися прихованими або оцінювалися приблизно.

Водночас без належної узгодженості між контуром національного рівня, контуром регіональної координації й локальними контурами громад, без чіткої фіксації ролей, відповідальності та процедур координації, навіть найсучасніші сенсори, канали та аналітика не перетворюються на реальну стійкість. Саме тому подальший розвиток НМС вимагає не лише розширення цифрової інфраструктури (як пропонує В.Філатов [139], а й послідовного налаштування всієї багатоконтурної архітектури управління так, щоб кожен рівень – від уряду до громади – бачив свою частину картини, мав інструменти впливу й водночас залишався інтегрованим у цілісний, узгоджений механізм національного розвитку.

Управління локальними спільнотами зазнає суттєвої трансформації під впливом цифрових технологій. Міські, сільські та регіональні волонтерські мережі дедалі частіше функціонують як цифрово опосередковані спільноти практики, використовуючи чати в Telegram і Viber, краудфандингові платформи, локальні гео-сервіси та інші інструменти мережевої комунікації. На рівні територіальних громад це проявляється, зокрема, у запровадженні онлайн-форм для збору заявок на допомогу вразливим групам (наприклад, літнім людям), окремих каналів та чатів для координації волонтерів і водіїв, які здійснюють розвезення гуманітарних наборів, а також інтерактивних таблиць і реєстрів, що фіксують факти надання допомоги конкретним домогосподарствам ((В.Ковтун)[140].

Формально такі практики не належать до сфери класичного державного управління, проте фактично вони виконують функції ко-продукування (co-production) публічних послуг та підтримання життєво важливих функцій територіальної громади (Д.Саганович [141], Є.Легеза [142]). У контексті розбудови НМС це означає, що цифрово опосередковані форми самоорганізації населення компенсують обмежені можливості органів влади в умовах кризи і, тим самим, стають невід'ємною складовою реальної архітектури стійкості.

Звідси випливає важливий аналітичний висновок – *цифрові технології створюють значний потенціал для посилення НМС саме завдяки поєднанню «вертикального» виміру (державні цифрові платформи, офіційні реєстри, аналітичні системи) та «горизонтального» виміру (волонтерські й громадські ініціативи, самоорганізація спільнот, локальні цифрові мережі).* Адже якщо держава свідомо проектує свої цифрові рішення як інтероперабельні до ініціатив знизу, це створює ефект синергії, коли цифрова інфраструктура підсилює, а не витісняє місцеву активність.

Натомість там, де цифрові системи проектуються як закриті, жорстко централізовані, із мінімальним простором для взаємодії з громадськими ініціативами, цифровізація ризикує лише відтворити існуючі бюрократичні

ієрархії в оновленій технологічній формі (Є.Красников та інш.)[143]. У такому разі внесок цифрових рішень у національну модель стійкості залишається обмеженим, а потенціал локальних спільнот щодо адаптації й координації ресурсів використовується не повною мірою (таблиця 1.13).

Таблиця 1.13

Цифрові практики локальних спільнот у контексті НМС

Рівень / вимір	Тип цифрових практик	Основні суб'єкти	Емпіричні прояви (типові приклади з практики громад України)	Внесок у НМС / стійкість
Горизонтальний (локальні спільноти, волонтерські мережі)	Чати в Telegram / Viber для координації допомоги	Волонтерські групи, активісти, мешканці громади	Оперативний збір запитів на допомогу; розподіл завдань між волонтерами; швидке інформування про безпекову ситуацію чи потреби населення	Підвищення адаптивної спроможності громади; скорочення часу реакції; мобілізація «тонких» локальних знань
Горизонтальний	Онлайн-форми (Google Forms тощо)	Ініціативні групи, ОСН, НУО	Створення реєстрів потреб (літні люди, ВПО, сім'ї з дітьми); пріоритизація допомоги на основі зібраних даних	Формування баз даних на місцевому рівні, що підсилюють адресність підтримки та прозорість розподілу ресурсів
Горизонтальний	Інтерактивні таблиці / локальні реєстри допомоги	Координатори волонтерів, представники громад, НУО	Ведення обліку наданих гуманітарних наборів; позначення домогосподарств, які вже отримали допомогу; мінімізація дублювання	Підвищення ефективності використання ресурсів; можливість аналітики потреб громади в динаміці
Вертикальний (державна, місцеве самоврядування)	Державні цифрові платформи (портали послуг, е-реєстри, аналітичні панелі)	Центральні органи влади, ОМС	Надання електронних послуг ВПО, допомоги постраждалим; використання аналітичних систем для моніторингу міграції, навантаження на інфраструктуру	Забезпечення структурованої інформаційної основи для рішень; масштабованість практик на національний рівень
Зона перетину вертикального й горизонтального вимірів	Інтероперабельні рішення та відкриті API / формати даних	Держава, громади, НУО, ІТ-спільнота	Узгодження форматів обліку ВПО, гуманітарної допомоги; можливість завантаження даних з локальних ініціатив до державних систем	Формування єдиної екосистеми даних, що поєднує офіційні та громадські джерела; ко-продуктування публічних послуг
Організаційний вимір (управлінські моделі)	Мережеве управління (network governance) та цифрове співврядування	Органи влади, громади, НУО, бізнес	Спільні координаційні штаби онлайн; включення волонтерських даних у муніципальне планування; спільні цифрові карти ресурсів	Переорієнтація з «державоцентричної» моделі на мультиакторну, посилення соціального капіталу й довіри

Джерело: розроблено автором

Подальший аналіз, однак, показує, що реальна експозиція цифрової трансформації публічних інститутів є суперечливою. З одного боку, кількість стратегій, програм, дорожніх карт, концепцій цифрового розвитку постійно

зростає. У кожній галузі – освіті, охороні здоров'я, соціальній сфері, безпеці, інфраструктурі – з'являються власні цифрові плани, власні платформи й реєстри, й це створює враження багатовимірного руху вперед. З іншого боку, коли дивитися крізь призму резильєнтності, стає видно, що ці стратегічні документи не взаємодоповнюють одне одного в єдиній логіці стійкості. Наприклад, цифрова трансформація в освіті часто орієнтується на впровадження електронних журналів, дистанційного навчання, платформ тестування. В охороні здоров'я пріоритетами стають електронні медичні картки, телемедицина, електронні рецепти. У соціальній політиці – електронні кабінети одержувачів допомог, цифрові механізми субсидій. Кожен із цих напрямів є важливий, але в більшості випадків питання резильєнтності – тобто здатності системи продовжувати функціонувати в умовах масштабних криз, відновлюватися після кібератак, тривалих відключень світла, руйнування фізичної інфраструктури – лишається на периферії. Наявні стратегії цифровізації відповідають на запит «як зробити зручніше й швидше», а не на питання «як забезпечити, щоб система не зруйнувалась й була здатна самооновлюватися в умовах кризи».

У результаті формується ситуація, коли багатоваріантність стратегій цифрової трансформації поєднується з відсутністю цілісного, надгалузевого бачення резильєнтності як головного критерію успіху. Окремі проекти запускаються, працюють, іноді навіть демонструють вражаючі результати, але не вбудовуються в спільну архітектуру НМС, і головне – принципово не можуть бути туди інтегровані. За відсутності єдиного підходу до пріоритезації ризиків, дублюються функції, накопичуються несумісні технічні рішення, витрачаються ресурси на паралельні платформи, а користувачі губляться в множині «кабінетів», логінів і паролів. З погляду НМС це означає, що країна має велику кількість цифрових елементів, але не має стійкої системи. Основа цієї проблеми лежить у слабкій розвиненості цифрового врядування як окремої інституціональної підсистеми НМС. Формально з'являються органи, відповідальні за цифрову трансформацію,

ухвалюються закони про електронні послуги, електронні комунікації, електронні довірчі послуги. Але розмежування повноважень, механізми координації, правила прийняття рішень про запуск нових сервісів чи реєстрів часто лишаються нечіткими. У підсумку різні міністерства замовляють розробку власних ІТ-систем, ОМС створює галузеві структури – ще інші, а спроби інтегрувати це в єдину логіку відбуваються постфактум і з великими втратами. На жаль, воєнний стан загострив такі проблеми (таблиця 1.14).

Таблиця 1.14

Цифрові практики локальних спільнот у НМС в умовах воєнного стану

Рівень / вимір	Ключові цифрові практики	Внесок у стійкість / НМС	Ключові ризики та умови ефективності
Горизонтальний – базова безпека і допомога населенню	Чати в Telegram/Viber для оповіщення, координації укриттів, розподілу гуманітарної допомоги	Швидка мобілізація місцевих ресурсів; підтримання базових життєвих функцій громади (їжа, ліки, укриття); «тонка» локальна обізнаність	Ризики витоку чутливої інформації, дезінформації; залежність від адміністраторів чатів. Ефективність потребує мінімальних правил модерації й базової цифрової грамотності учасників
Горизонтальний – підтримка вразливих груп	Онлайн-форми для заявок на допомогу літнім людям, ВПО, сім'ям з дітьми; інтерактивні списки отримувачів допомоги	Більш адресний розподіл ресурсів; зниження соціальної напруги; формування первинних локальних реєстрів потреб	Ризики порушення конфіденційності, неповноти даних (ті, хто «поза цифрою»). Потрібні прості формати (мобільні форми, підтримка офлайн-реєстрації із подальшим оцифровкою)
Вертикальний – державні цифрові сервіси у кризі	Використання державних платформ (е-документи, е-виплати, реєстри ВПО) як «опорного каркасу» для доступу до прав і послуг	Забезпечення базової юридичної видимості громадян (е-документи), доступу до фінансової підтримки; національна уніфікація даних	Ризик перевантаження систем, кіберударів, централізованих «вузьких місць». Потрібні резервні рішення (офлайн-процедури, дублювання даних, розподілена інфраструктура)
Перетин вертикального й горизонтального – координація даних	Передача агрегованих даних волонтерів у системи ОМС/держави (наприклад, про потреби ВПО, гуманітарні запаси) через стандартизовані шаблони	Підвищення точності планування на місцевому й національному рівнях; зменшення дублювання допомоги; зміцнення довіри між владою й громадою	Ризик недовіри між акторами, різної якості даних. Умови ефективності: мінімальні, але зрозумілі стандарти обміну, прозорість використання даних, зворотний зв'язок до спільнот
Організаційний вимір – кризове співврядування	Створення спільних кризових штабів (онлайн), де ОМС, волонтери, НУО й бізнес використовують спільні карти, таблиці, чати для рішень	Швидше узгодження дій; зниження фрагментації між формальними й неформальними ініціативами; формування практик мережевого управління	Ризики конкуренції за вплив, проблема некоректного нормативного регулювання. Потрібне базова формалізація суб'єктності (хто за що відповідає), протоколи безпеки, мінімум інституційної підтримки з боку ОМС

Джерело: розроблено автором

Типовим і водночас концептуально показовим для розбудови НМС є концептуальний формат управління даними. У межах правового режиму воєнного стану, визначеному Конституцією України та Законом України «Про правовий режим воєнного стану», масиви даних про населення, критичну інфраструктуру, економічну активність, переміщення ресурсів та осіб набувають статусу не лише адміністративного ресурсу, а й ключового елемента національної безпеки та стійкості. Держава акумулює значні обсяги такої інформації у розрізнених реєстрах та інформаційних системах, однак правила доступу, інтероперабельності, режиму зберігання та використання даних, а також баланс між вимогами безпеки й захистом персональної інформації залишаються фрагментарно врегульованими.

Емпірично це проявляється, зокрема, у тому, що частина реєстрів (наприклад, пов'язаних із критичною інфраструктурою чи обороноздатністю) фактично набуває статусу «стратегічних» і максимально закривається навіть для органів місцевого самоврядування, які відповідають за щоденне забезпечення життєво важливих функцій громад. Інші системи (окремі реєстри внутрішньо переміщених осіб чи обліку гуманітарної допомоги) працюють у напіввідкритому режимі, коли центральні органи влади і міжнародні донори мають доступ до агрегованих даних, тоді як місцеві актори покладаються на неформальні витяги, скриншоти чи неофіційні «експортовані» таблиці; треті ж інформаційні системи створюються як тимчасові або пілотні проєкти (електронні платформи для фіксації пошкодженого житла, муніципальні ГІС-рішення для планування відбудови, локальні облікові системи гуманітарної допомоги на базі хмарних сервісів), правовий режим яких у контексті воєнного стану залишається невизначеним – відсутні чітко закріплені в законодавстві або підзаконних актах норми щодо статусу цих даних, кола розпорядників і користувачів, строків і порядку зберігання, вимог до резервування та захисту.

У практиці державного управління воєнного часу це породжує низку суперечностей. По-перше, центральні органи виконавчої влади, посиляючись

на особливості правового режиму воєнного стану, розширюють коло суб'єктів, яким надається доступ до певних масивів інформації (наприклад, військовим адміністраціям чи окремим силовим структурам), а також спрощують окремі процедури обміну даними. По-друге, місцеві органи влади, волонтерські та гуманітарні організації часто залишаються «за межами» формалізованої інфраструктури даних і вимушені покривати інформаційні прогалини через створення неофіційних таблиць, чат-ботів, реєстрів на базі комерційних або хмарних сервісів, що не мають належного правового захисту. Так, у низці громад облік потреб внутрішньо переміщених осіб та наданої їм допомоги фактично вівся у вигляді електронних таблиць, створених волонтерами або працівниками ЦНАПів, які дублювали, коригували чи навіть випереджали державні реєстри; при цьому ні режим обробки персональних даних, ні порядок доступу до цих масивів у разі кіберінциденту чи евакуації органу влади не були чітко визначені.

Для НМС принциповим є нормативне закріплення цілісної «політики даних», адаптованої до режиму воєнного стану: по-перше, має бути визначено перелік наборів даних, що визнаються критично важливими для забезпечення стійкості (наприклад, дані про розміщення населення, стан об'єктів критичної інфраструктури, логістику постачання, розташування укриттів, реєстри ушкодженого та зруйнованого майна); по-друге, необхідно чітко розподілити відповідальність між суб'єктами владних повноважень за формування, оновлення, резервування та захист цих даних, включно з визначенням ролі військових адміністрацій, органів місцевого самоврядування, державних підприємств-адміністраторів реєстрів і приватних постачальників цифрових рішень; по-третє, потребують правового закріплення режими й сценарії доступу до критично важливих даних в умовах надзвичайних ситуацій і воєнного стану, зокрема тимчасове розширення прав доступу для уповноважених суб'єктів «на місцях» (служб порятунку, медичних закладів, комунальних підприємств, гуманітарних координаційних центрів) із одночасним запровадженням чітких процедур

журналювання операцій, аудиту та притягнення до відповідальності за зловживання. Нарешті, необхідні ефективні процедури контролю за дотриманням прав людини у сфері персональних даних та механізми незалежного нагляду (наприклад, з боку уповноважених органів із захисту персональних даних чи спеціалізованих парламентських інституцій), здатні діяти й у режимі воєнного стану.

За відсутності такої системної, чітко визначеної та емпірично вкоріненої «політики даних» цифрові проєкти в умовах воєнного стану здебільшого залишаються інструментами розв'язання поточних операційних завдань – обліку отримувачів допомоги, формування звітності для донорів, технічної підтримки окремих адміністративних процедур, – але не перетворюються на нормативно й інституційно закріплений каркас довгострокової стійкості. У результаті навіть там, де створюються технологічно розвинені системи збору й обробки інформації (наприклад, платформи для подання заявок на компенсацію за зруйноване житло чи єдині інформаційні системи управління гуманітарними потоками), їхній внесок у НМС обмежується часовими рамками конкретного проєкту або донорської програми: відсутність чітко визначеного правового режиму даних, процедур інтеграції з іншими реєстрами та правил використання інформації в поствоєнний період не дозволяє перетворити ці інструменти на стійку інфраструктуру управління ризиками і відновленням.

До цього додається проблема легітимності цифрових рішень, яка в умовах розбудови НМС набуває не технічного, а насамперед інституційно-правового й соціально-психологічного виміру. Коли держава запускає новий електронний сервіс – наприклад, платформу для реєстрації воєнних збитків, подання заявок на компенсацію за зруйноване житло, оформлення статусу внутрішньо переміщеної особи чи отримання цільових тимчасових виплат – громадяни очікують не лише зручності інтерфейсу, а й прозорих «правил». Йдеться про базові елементи процедурної справедливості: зрозумілу логіку роботи алгоритму обробки заявок; чітко

визначені критерії прийняття рішень; відкрити інформацію про те, які саме державні органи або посадові особи мають доступ до персональних і чутливих даних; якими нормативними актами регулюється цей доступ, у які строки розглядають звернення, яким є формат офіційної відмови та як саме можна оскаржити результат в адміністративному або судовому порядку.

В українському контексті це особливо помітно на прикладі цифрових сервісів, що впливають на розподіл дефіцитних ресурсів у воєнний час: якщо громадяни не розуміють, чому одна сім'я отримала компенсацію чи допомогу раніше, а інша – пізніше або зовсім не отримала, сам факт наявності «розвинутого» електронного інструменту не гарантує довіри, а інколи навіть посилює відчуття несправедливості. За відсутності чітко артикульованих процедур і публічно доступних роз'яснень будь-який інформаційний збій, медіаповідомлення про зловживання чи чутки в соціальних мережах (наприклад, про «ручне втручання» чиновників у чергу на компенсацію, «пріоритет для своїх» або «фільтрування» заявок за політичною чи регіональною ознакою) швидко підривають легітимність сервісу. У досвіді воєнного часу можна спостерігати, як поодинокі публічні скандали навколо окремих електронних інструментів – підозри в «роздачі» виплат «не тим», сумніви в достовірності даних реєстрів, повідомлення про витоки персональної інформації – поширюються на сприйняття цифрового врядування в цілому, актуалізуючи уявлення про корупційний вплив «за лаштунками» інтерфейсу.

У такій конфігурації цифрові технології не зміцнюють НМС як систему, орієнтовану на довіру й передбачуваність, а навпаки – стають ще одним джерелом інституціональної недовіри, підривають відчуття справедливості розподілу ресурсів і рішень та сприяють формуванню «цифрового цинізму», коли будь-яке електронне нововведення сприймається як потенційний інструмент маніпуляції. Так логіка аналізу неминуче приводить до питання про роль цифрових компетентностей, однак ідеться не лише про «вміння користуватися застосунком». На перший погляд може

здатися, що достатньо навчити громадян завантажувати електронні сервіси, проходити е-ідентифікацію, заповнювати онлайн-форми, прикріплювати скани документів – і проблема «цифрового виключення» буде суттєво пом'якшена, а довіра до е-послуг автоматично зросте. Дійсно, емпіричні спостереження за перебігом освітніх ініціатив – від всеукраїнських проєктів на кшталт «Дія. Цифрова освіта» та масових онлайн-курсів для різних вікових груп до локальних програм цифрової грамотності в бібліотеках, центрах надання адміністративних послуг, хабах громадських організацій – засвідчують високий попит на базові навички роботи з цифровими інструментами [144]. Там, де люди впевнено володіють елементарним набором операцій (створити електронну скриньку, встановити мобільний застосунок, пройти реєстрацію в кабінеті користувача, подати онлайн-заяву, відстежити її статус), ризик формального виключення з цифрових сервісів справді зменшується, а доступ до публічних послуг у віддалених чи постраждалих громадах стає більш реалістичним. Проте з наукової перспективи стає очевидно, що «цифрова компетентність» у контексті НМС не зводиться до інструментальних умінь: вона включає також розуміння базових принципів функціонування інформаційних систем (що таке персональні та чутливі дані, як вони обробляються й хто є їхнім розпорядником), знання своїх прав і процедурних гарантій (право на доступ до інформації, право на оскарження автоматизованого рішення, механізми захисту від дискримінації в алгоритмічних процесах), а також елементи критичного мислення й медіаграмотності (перевіряти джерела інформації, усвідомлювати можливість маніпуляцій через фейкові «електронні сервіси»).

Крім того, досвід воєнного часу демонструє, що не менш важливими є цифрові компетентності не лише громадян, а й самих представників органів влади та місцевого самоврядування: від того, чи здатні вони коректно працювати з електронними системами, пояснювати громадянам логіку процедур, документувати й комунікувати виняткові ситуації, залежить сприйняття цифрових рішень як справедливих і надійних. Так, у громадах,

що зазнали руйнувань, засвідчують, що там, де посадовці фактично виконували роль «цифрових перекладачів» для вразливих груп (людей старшого віку, внутрішньо переміщених осіб, осіб з інвалідністю), рівень довіри до е-сервісів був істотно вищим, а кількість конфліктних ситуацій і скарг – помітно нижчою (таблиця 1.15).

Таблиця 1.15

Ключові виміри впливу легітимності та цифрових компетентностей на стійкість публічного врядування

Вимір / аспект	Характерні прояви (з тексту)	Значення для НМС	Ключові ризики / виклики
Легітимність цифрових сервісів	Запуск державою електронних сервісів для реєстрації збитків, компенсацій, статусу ВПО, тимчасових виплат; очікування «прозорих правил гри»	Легітимні е-сервіси стають опорою для довіри до публічної влади, забезпечують передбачуваність рішень та сприйняття їх як справедливих	За відсутності чітких правил та публічних роз'яснень цифрові сервіси сприймаються як непрозорі й політично/корупційно вразливі
Прозорість алгоритмів і процедур	Питання: як працює алгоритм, хто бачить дані, за якими критеріями ухвалюються рішення, як і де можна оскаржити результат	Чітко прописані алгоритми, критерії та процедури оскарження забезпечують процедурну справедливість і зміцнюють інституційну довіру	Складність або прихованість правил сприяє підозрам у «ручному втручанні», дискримінації, маніпуляціях чергою чи пріоритетами
Комунікація та чутки / скандали	Інформаційні відмови, скандали в медіа, чутки в соцмережах щодо «роздачі не тим», витоків даних, «пріоритету для своїх»	Проактивна комунікація й публічні пояснення механіки сервісу формують стійку довіру до цифрових рішень у кризових умовах	Відсутність системної комунікації робить сервіси вразливими до інформаційних атак і чуток, формує «цифровий цинізм» у громадян
Базові цифрові компетентності громадян	Уміння завантажити застосунок, пройти е-ідентифікацію, заповнити онлайн-форму, подати заяву, відстежити статус	Зниження ризику цифрового виключення; реальне використання е-послуг навіть у віддалених/постраждалих громадах	Соціальні групи без базових навичок фактично втрачають доступ до цифрових сервісів, поглиблюючи нерівність у доступі до державної підтримки
Розширені громадянські цифрові компетентності	Розуміння статусу й обробки персональних даних, знання прав (доступ, оскарження, недискримінація), елементи критичного мислення та медіаграмотності	Дозволяють громадянам усвідомлено користуватися е-сервісами, захищати свої права та відрізняти офіційну інформацію від чуток	Без таких компетентностей навіть формально доступні сервіси можуть викликати страх, недовіру, відмову від користування або піддавання маніпуляціям
Цифрові компетентності представників влади	Здатність чиновників і працівників ОМС коректно працювати з системами, пояснювати процедури, документувати винятки, комунікувати з громадянами	Компетентні посадовці стають «перекладачами» складних цифрових процесів для громадян, підсилюючи сприйняття сервісів як надійних і справедливих	Низька цифрова компетентність публічних службовців призводить до помилок, неформальних обхідних практик, суперечливих роз'яснень і втрати довіри
Вплив на стійкість та НМС у цілому	Поєднання рівня легітимності сервісів, цифрових навичок громадян	За наявності прозорих правил і розвинених компетентностей	За їхньої відсутності цифрові проєкти залишаються поверховими

	і компетентності влади у практиці воєнного часу	цифровізація стає інституційною опорою НМС, підсилює довіру та керуваність у кризі	технічними інструментами, що можуть послаблювати інституційну стійкість і поглиблювати недовіру

Джерело: розроблено автором

Отже, без розвитку комплексних – громадянських, адміністративних, управлінських – цифрових компетентностей, доповнених прозорими правовими рамками й належною комунікацією, цифровізація ризикує залишитися поверховим технічним проєктом, що не підсилює, а інколи й послаблює стійкість інститутів, на яких має ґрунтуватися НМС.

Однак, якщо застосувати більш суворий аналітичний підхід, стає видно, що сам по собі високий рівень цифрових компетентностей не змінює характер державного управління. Люди можуть прекрасно орієнтуватися в інтернеті, користуватися мобільними додатками, створювати онлайн-кампанії, але якщо інституційне середовище лишається закритим, непрозорим, негнучким, цифровізація лише переносить старі практики в нове середовище. Наприклад, громадяни вміють реєструвати електронні петиції, але органи влади формально «беруть їх до відома» без реальних наслідків; або ж люди активно заповнюють онлайн-опитування, але результати не мають помітного впливу на політику. У такому випадку цифрова компетентність населення радше підсилює відчуття фрустрації: «ми все робимо правильно, але нас не чують».

На конкретних прикладах це видно досить виразно. Громадянин в невеликому місті вміє користуватися смартфоном, спілкуватися з дітьми по відеозв'язку, навіть читати новини в Telegram. Але коли намагається оформити субсидію онлайн, стикається з тим, що система вимагає додаткові довідки, не приймає частину документів, пропонує звернутися до офлайн-віконечка. Формально її цифрові компетентності достатні, але реальна доступність послуги визначається не ними, а логікою організації сервісу й тим, наскільки державна система готова працювати в безпаперовому режимі. Навпаки, у громаді, де місцева влада усвідомлено спрощує процедури, забезпечує консультаційну підтримку, координує

волонтерів, що допомагають заповнювати заявки, навіть люди з мінімальними цифровими навичками отримують реальний доступ до е-послуг.

Звідси другий важливий висновок дисертаційного дослідження – цифрові компетентності є платформою, на якій тільки можливо вибудовувати елементну базу загальносистемних державноуправлінських перетворень, але вони не є їх визначальним рушієм автоматично, лише у форматі цифрового рішення. Без масового оволодіння суспільством цифровими навичками держава не може легітимно переводити критично важливі послуги онлайн, але й за наявності таких навичок нічого не змінюється, якщо не перебудовуються інституціональні механізми прийняття рішень, підзвітності та розподілу ресурсів. Це означає, що в науковому аналізі важливо чітко розрізняти два рівні управлінського контексту. Перший рівень – індивідуальний, який поєднує все, що вміє окрема людина, як вона користується цифровими інструментами, які має когнітивні й мотиваційні установки. Другий – системний, що детермінує, які правила діють у державних інститутах, хто ухвалює рішення щодо пріоритетів цифровізації, як оцінюють ефекти цифрових проєктів, як інтегрують цифрові інструменти в загальну логіку НМС. Якщо аналіз обмежується лише першим рівнем, виникає варіант вважати, що «освіта вирішить усе». Якщо ж зосереджуватися лише на системному рівні, можна недооцінити реальний людський вимір – страхи, обмеження, нерівність доступу.

На перетині цих двох рівнів і формується поле цифрового врядування, якого сьогодні в Україні бракує в цілісному вигляді. Де-факто цифрове врядування вже відбувається, органи влади погоджують між собою проєкти, місцеві громади обирають, яким сервісам довіряти, громадські організації здійснюють моніторинг цифрових прав. Проте де-юре механізми координації, участі, контролю, розв’язання конфліктів інтересів прописані лише частково. Саме тому цифрові технології поки що впливають на НМС радше стихійно, ніж як результат усвідомленого системного проєктування.

Якщо концептуалізувати логіку такого підходу, можна простежити послідовний алгоритм цифровізації. По-перше, цифрові технології надають державі та локальним спільнотам нові інструменти швидкої комунікації, координації, аналізу даних і надання послуг, тобто створюють матеріальну основу для національної стійкості. По-друге, спосіб, у який держава інтегрує ці технології, залежить від наявної множинності стратегій цифрової трансформації, що без системного бачення резильєнтності веде до фрагментації та неефективного використання ресурсів. По-третє, слабкість інституціонально визначеного цифрового врядування призводить до розривів між окремими елементами цифрової екосистеми, знижує довіру, загострює вразливості. По-четверте, цифрові компетентності населення, хоча й є критично важливим ресурсом, не запускають управлінські реформи автоматично, а лише роблять можливим перехід до нової моделі публічного управління, якщо інституційні передумови для цього створені.

У цьому сенсі ключове завдання подальших досліджень і практичних політик полягає не в тому, щоб протиставляти «технології» й «людей» або «цифрові навички» й «інститути», а в тому, щоб описати й спроектувати їхню взаємодію саме в координатах НМС. Лише така інтегрована перспектива дає шанс використати цифровізацію не як чергову хвилю модернізаційних гасел, а як реальний інструмент підсилення здатності суспільства вистояти, адаптуватися й розвиватися в умовах тривалих і багатовимірних криз.

Висновки до розділу 1

1. Багатовимірна природа стійкості публічного управління в умовах цифровізації вимагає інтеграції інституційних, ціннісних, мережових та технологічних вимірів. Аналіз еволюції моделей управління (від веберівської бюрократії через новий публічний менеджмент до належного врядування) показує, що стійкість (резильєнтність) не є статичною властивістю, а динамічним процесом адаптації до криз, де ключовими елементами

виступають не лише формальні процедури, але й цифрові інструменти (платформи, дані, ШІ) та громадянська участь. У контексті України це проявляється в необхідності переходу від фрагментованої цифровізації до єдиної екосистеми, де стійкість забезпечується через баланс між централізованим контролем і горизонтальними мережами, що дозволяє протистояти гібридним загрозам і відновлюватися після шоків.

2. Формування національної моделі стійкості (НМС) на основі проблемного підходу передбачає переосмислення державотворчих процесів як відповіді на конкретні виклики, з акцентом на цифровий дизайн державності. НМС є не абстрактною конструкцією, а сукупністю проблемних полів (наприклад, управління даними, цифровий розрив, легітимність), де стійкість досягається через інтеграцію цифрових технологій у конституційно-правовий, економічний та соціальний виміри. Авторський концепт «цифрового дизайну державності» (як сукупності сервісів, реєстрів і алгоритмів) підкреслює, що цифрова трансформація перетворює державу на гнучку систему, здатну до самовідновлення, але вимагає подолання фрагментації та забезпечення публічної чутливості для підвищення довіри громадян.

3. Управління даними в умовах правового режиму воєнного стану є ключовим елементом національної безпеки та стійкості, але фрагментарність регулювання створює системні ризики. На основі емпіричного аналізу реєстрів і інформаційних систем (наприклад, даних про населення, інфраструктуру та гуманітарну допомогу) у розділі обґрунтовано необхідність цілісної «політики даних» у НМС, яка включає перелік критично важливих наборів, розподіл відповідальності, режими доступу та процедури контролю. Відсутність такої політики призводить до вразливостей (наприклад, неінтегрованих пілотних проєктів), тоді як її впровадження перетворює дані на опору для довгострокової стійкості, адаптованої до криз, з балансом між безпекою та захистом персональних прав.

4. Легітимність цифрових рішень залежить від прозорості алгоритмів, процедур і комунікації, що є передумовою для запобігання недовірі та посилення стійкості в цифровому суспільстві. Аналіз проблем легітимності (з прикладами електронних сервісів для реєстрації збитків, компенсацій та статусу ВПО) показує, що відсутність чітких правил і регламентів (критеріїв рішень, доступу до даних, механізмів оскарження) породжує підозри в маніпуляціях і «цифровий цинізм», підриває сутність НМС. Запропоновано легітимність визначити ресурсом для інституційної довіри, особливо в умовах воєнного стану, де цифрові інструменти можуть або зміцнювати справедливість, або посилювати нерівність.

5. Цифрові компетентності акторів (громадян, чиновників, влади) є базовою умовою для реалізації НМС, але їх ефективність залежить від інституційних змін і подолання цифрового виключення. На основі порівняльного аналізу (традиційних vs. цифрових систем) та емпіричних прикладів (освітні ініціативи, як «Дія. Цифрова освіта») доведено, що компетентності виходять за межі інструментальних навичок. Без системної інтеграції (баланс між індивідуальним і системним рівнями) вони не запускають реформи, а лише створюють потенціал; у контексті України це вимагає політики цифрової інклюзії для вразливих груп, щоб уникнути розриву та забезпечити адаптивність публічного управління в кризах.

Основні результати дослідження, що наведені у цьому розділі, були опубліковані у фахових наукових виданнях галузі знань «Публічне управління і адміністрування, та включені до списку опублікованих праць [].

РОЗДІЛ 2

ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ МОДЕЛІ
СТІЙКОСТІ В УМОВАХ ЦИФРОВОГО СУСПІЛЬСТВА

2.1. Національна модель стійкості: визначення, особливості та основні складники

У сучасних умовах радикальної невизначеності, війни, масштабних криз та трансформацій поняття стійкості поступово виходить за межі свого традиційного, переважно технічного або психологічного змісту й набуває чітко вираженого екзистенційного виміру. Це особливо виразно проявляється в сфері державного управління, де стійкість розглядається вже не лише як здатність інституцій функціонувати в умовах кризи, а як здатність суспільства й держави зберігати сенс, гідність, суб'єктність і здатність до розвитку навіть під тиском граничних загроз. Таким чином, тема екзистенційного змісту стійкості набуває принципового значення для теорії та практики публічного управління, оскільки торкається фундаментальних засад взаємодії держави та громадян у ситуаціях, коли поставлено під сумнів самі основи їхнього спільного буття.

У класичних моделях державного управління стійкість здебільшого інтерпретувалася як стабільність інститутів, надійність процедур, відновлюваність базових функцій держави після криз. Такий підхід можна позначити як функціональний, адже він фокусується на безперервності надання публічних послуг, роботі органів влади, підтриманні правопорядку, стабільності економічних і адміністративних процесів. Безперечно, такий вимір є необхідним – держава, яка втрачає елементарну працездатність, не може ні гарантувати безпеку, ні забезпечувати розвиток. Однак досвід глибоких суспільних травм, масових втрат, війни, гуманітарних катастроф показує, що функціональної стійкості недостатньо для того, щоб суспільство справді вистояло. Можлива ситуація, коли адміністративна система

продовжує працювати, але громадяни переживають глибоку екзистенційну кризу, втрачають відчуття сенсу, довіру до інституцій (рис.2.1).



Рис. 2.1. Категорії та поняття інституціонального концепту стійкості
Джерело: дослідження автора.

Саме тут постає потреба в осмисленні екзистенційного змісту стійкості, який пов'язаний з питаннями людського буття: як жити в умовах невизначеності й небезпеки, як зберегти гідність перед обличчям приниження й насильства, як підтримувати відчуття сенсу в ситуації, коли руйнуються звичні орієнтири, інституції, простір і час повсякденного життя. Для державного управління це означає, що завдання влади полягає не лише в організації захисту інфраструктури чи розробці планів безперервності роботи органів влади, а й у створенні таких умов, за яких людина і спільнота зможуть витримувати зустріч із граничними ситуаціями, не втрачаючи

власної суб'єктності.

З позицій сучасних концепцій інституціоналізму (Д.Марч, Д.Олсен, Р.Пірсон, Е.Остром) [145-148] Національна модель стійкості як інституціональна платформа (National model of resilience as an institutional platform) – це не просто сукупність окремих секторних політик у сфері безпеки, економіки, соціального захисту, екології чи управління кризами. Йдеться про вищий рівень організації держави й суспільства, на якому задаються спільні правила гри, механізми взаємодії, формати прийняття рішень і способи оновлення інститутів. Саме як інституціональна платформа НМС визначає, яким чином у державі формуються та взаємодіють суспільні інститути (social institutions), яким є інституціональний формат державотворення (institutional format of state-building), яке інституціональне середовище (institutional environment) оточує ключових акторів, через які механізми впливу та змін (mechanisms of institutional influence and change) здійснюється державна політика, і якою є інституціональна формула стійкості (institutional formula of resilience), що забезпечує життєздатність держави в умовах різноманітних викликів [149].

У межах цієї платформи суспільні інститути розглядаються не як ізольовані сектори, а як взаємопов'язані вузли єдиної системи. Держава, ринок, громади, освітні заклади, медіа, релігійні організації, громадські об'єднання вибудовуються в певну інституційну архітектуру, де кожен інститут має власну роль, сферу відповідальності й водночас пов'язаний з іншими формальними і неформальними відносинами. Формується розподіл функцій і відповідальності: одні інститути координують кризове реагування, інші відповідають за інформаційну або енергетичну стійкість, а також – за соціальну підтримку та згуртованість. Важливим є те, що НМС ініціює форми їх взаємодії: постійні координаційні платформи, міжвідомчі ради, формати «державна – громади – бізнес – громадянське суспільство», механізми обміну даними й спільного планування. Завдяки цьому зменшуються «провали відповідальності», мінімізується конфлікт інтересів і

дублювання функцій, а секторна політика не «розсипається» на набір несумісних ініціатив.

Інституціональний формат державотворення в межах НМС фіксує, яким чином організована влада, як розподіляються повноваження між рівнями управління та гілками влади, наскільки реальною є участь громадян у прийнятті рішень. Це включає баланс централізації та децентралізації, статус і вплив місцевого самоврядування, механізми контролю за виконавчою владою, роль парламенту й судів, форми прямої демократії (В.Стрельцов) [150]. Якщо система публічного управління є надто централізованою, уразливість центру може паралізувати всю державу; але якщо надто фрагментованою, складно забезпечити координацію й цілісну відповідь на загрози. НМС як інституціональна платформа орієнтується на збалансований формат: стратегічні рішення – на національному рівні, адаптація й реалізація – на регіональному та місцевому, за умови існування дієвих каналів зворотного зв'язку знизу догори.

Інституціональне середовище (institutional environment), у якому діють суб'єкти, охоплює як формальні правові норми, так і неформальні практики, традиції, уявлення про справедливість та допустимі способи дій (О.Руденко) [151]. Від якості правопорядку, стабільності й передбачуваності правил, рівня довіри до інститутів залежить, наскільки суб'єкти в системі публічного управління здатні діяти раціонально й довгостроково, не спираючись на тіньові механізми чи насильство (Т.Чубара) [152-153]. У стійкій системі (в інституціональному розумінні) закони й реальні практики достатньо збігаються, щоб забезпечити правову визначеність; кризи не руйнують базові правила гри, а їх корекція здійснюється через передбачені, легітимні процедури. Там, де між формальними нормами і реальними практиками прірва, зростають транзакційні витрати, поширюється правовий нігілізм, знижується довіра, а отже, підривається інституційний фундамент стійкості.

Ключовою складовою НМС є комплекс **механізмів впливу, змін і реалізації політик** (за методологією А.Мерзляк, Р.Рудницька, О.Сидорчук,

О.Федорчак [154;155;156]. Ми пропонуємо авторські визначення категорії «механізми».

Механізми інституціонального впливу (mechanisms of institutional/state influence) – це регулювання, санкції, податки, ліцензування, субсидії, інформаційні кампанії, програми підтримки, через які держава й інші інститути спрямовують поведінку акторів у бік стратегічних цілей, у тому числі цілей стійкості. *Механізми інституційних змін* (mechanisms of institutional change) – це процедури розробки й ухвалення реформ, зміни законів, оновлення організаційних структур і процедур. Вони мають бути водночас достатньо гнучкими, щоб дозволити адаптацію до нових викликів, і достатньо стабільними та легітимними, щоб не перетворювати кожен кризу на руйнівну революцію правил гри. *Механізми реалізації політик* (institutional mechanisms of state policy implementation) – це вся інфраструктура виконання рішень: міністерства, служби, агенції, місцеві ради, цифрові сервіси, протоколи міжвідомчої взаємодії. Саме через них НМС проявляється на рівні конкретних дій, послуг, рішень на місцях.

Завершальним концептуальним рівнем є інституціональна формула стійкості (institutional formula of resilience), яка узагальнює всі попередні елементи в єдину логіку. Вона поєднує характеристики інституціонального середовища, формат державотворення, функціональний стан суспільних інститутів і баланс між ними, механізми впливу та змін, інституціональні витрати й виклики, а також інституційні механізми реалізації та стійкості державних політик. Через цю формулу можна описати, які саме конфігурації інституційних параметрів забезпечують високу життєздатність системи навіть за умов сильних шоків, а які – роблять її вразливою.

Якщо формалізувати інституціональну формулу стійкості у вигляді формалізованої моделі, можна умовно позначити:

IE – інституціональне середовище (Institutional Environment),

IF – інституціональний формат державотворення (Institutional Format),

IS – функціональний стан базових інститутів (Institutional State),

IB – інституціональний баланс (Institutional Balance),

IMinf – механізми інституційного впливу (Influence Mechanisms),

IMchg – механізми інституційних змін (Change Mechanisms),

IC – інституціональні витрати (Institutional Costs)

Ich – інституціональні виклики (Institutional Challenges),

IPimpl – інституціональні механізми реалізації політик (Implementation Mechanisms),

IPres – інституціональні механізми стійкості політик (Policy Resilience Mechanisms)

NR – інтегральний рівень національної стійкості (National Resilience).

Тоді на концептуальному рівні є можливість представити НМС у вигляді формульного підходу:

$$NR=f(IE, IF, IS, IB, IMinf, IMchg, IC, Ich, IPimpl, IPres).$$

Це не математична функція у класичному сенсі, а модельна відповідність, яка фіксує залежність рівня стійкості від поєднання інституційних параметрів. Зміст цієї моделі полягає в тому, що якісне інституціональне середовище з високим рівнем правопорядку, довіри й передбачуваності множить позитивний ефект реформ і політик, тоді як дефектне середовище зводить їхню результативність нанівець.

Збалансований інституціональний формат державотворення визначає, наскільки система здатна до колективних дій у кризі (за Т.Боасом) [157]. Функціональний стан інститутів визначає, чи можуть суди, правоохоронні органи, оборонний сектор, місцеве самоврядування, фінансові регулятори виконувати свої функції без функціональної зупинки (А.Гавриленко, І.Юхно, В.Черниш)[158]. При цьому інституціональний баланс не допускає ані монополізації влади одним центром, ані хаотичної фрагментації, що унеможлиблює координацію. Механізми впливу й змін забезпечують коригування поведінки акторів і адаптацію правил без руйнування самої системи, а механізми реалізації політик і їхньої стійкості дають змогу зберігати наступність стратегій навіть під час політичних змін.

Важливим елементом формули є інституціональні витрати та інституціональні виклики. У дисертації витрати показують, якою ціною підтримуються й реформуються інститути; якщо ця ціна надмірна або розподілена неефективно, сама підтримка інституцій може стати фактором нестабільності. Інституціональні виклики – корупція, правовий нігілізм, захоплення держави приватними інтересами, тіньові практики – задають рівень внутрішнього напруження в системі (А.Макурін, О.Акімов, А.Помаза-Пономаренко, Л.Сергієнко [159-161]).

Таким чином, НМС як інституціональна платформа є цілісною конструкцією, у якій з'єднуються структури, правила, механізми й цінності. Вона не обмежується технічним набором антикризових заходів, а описує спосіб організації життя суспільства, за якого інститути можуть адаптуватися, навчатися, координувати дії та підтримувати життєздатність держави за умов багатоаспектних викликів. Формалізована інституціональна формула стійкості дає можливість не лише концептуально описати цю систему, а й практично діагностувати її стан, виявляти вузькі місця та проектувати інституційні зміни, спрямовані безпосередньо на підвищення національної стійкості.

На першому рівні – *макрорівні*, НМС детермінується такими поняттями:

1) інституціональне середовище (institutional environment) – сукупність формальних правил (законів, норм, процедур) і неформальних практик, які визначають «правила гри» для всіх учасників суспільного життя. Інституціональне середовище формує рамки для дій держави, ринку, громади, громадянського суспільства;

2) інституціональний формат державотворення (institutional format of state-building) – конкретний тип організації влади, розподілу повноважень, співвідношення централізації й децентралізації, участі громадян. Саме він визначає, як держава проектує й реалізує політику стійкості, наскільки вона відкрито комунікує та залучає різні інститути;

Ці два елементи створюють фон, на якому розгортається дія НМС – й саме ці елементи визначають, наскільки гнучко та передбачувано можуть реагувати інститути на кризи, якою мірою допускаються зміни та інновації.

Другий рівень – це *суспільні інститути* (social institutions) – держава, ринок, громадянське суспільство, сім'я, освіта, церква, медіа тощо. Саме вони є носіями правил, норм, очікувань і практик, які структуровано організовують суспільне життя. Ключові категорії тут:

3) функціональний стан базових соціальних інститутів (функціональна автономність) (Functional state of basic social institutions (functional autonomy)) – показує, наскільки інститути здатні виконувати свої основні функції (забезпечення безпеки, правопорядку, освіти, соціальної підтримки) без надмірного зовнішнього тиску, політизації чи захоплення приватними інтересами. Функціональна автономність є важливою передумовою стійкості;

4) інституціональний баланс (institutional balance) – співмірний розподіл впливу між ключовими інститутами, який запобігає як хаосу (коли ніхто ні за що не відповідає), так і домінації одного актора (монополія держави, олігархів, силових структур тощо). Баланс означає, що різні інститути взаємно стримують і доповнюють одне одного;

Отже, цей рівень НМС безпосередньо визначає, чи є система здатною до саморегуляції у кризових умовах, чи потребує постійного «ручного управління». Також для стійкості важлива не тільки «наявність» інститутів, а й характер їхньої взаємодії:

5) система взаємовпливу інститутів (нормативно-правові відносини) (system of inter-institutional influence (normative-legal relations)) – це сукупність юридичних і організаційних зв'язків, через які інститути координують дії, узгоджують інтереси, розподіляють повноваження й відповідальність. Отже, йдеться про закони, регламенти, процедури, міжінституційні договори;

6) механізми інституціонального впливу (державного впливу) (vechanisms of institutional (state) influence) – це способи, якими держава,

використовуючи свої повноваження, спрямовує поведінку інших інститутів: регулювання, ліцензування, стимулювання, санкції, державні програми тощо;

Тобто, НМС як інституціональна платформа має забезпечити таку побудову взаємовідносин, за якої інституційний тиск держави не руйнує автономність інститутів, а навпаки – зміцнює їхню спроможність діяти відповідально і скоординовано в умовах загроз.

Третій важливий рівень – *динаміка інституційних трансформацій*:

7) інституціональні витрати (institutional costs) – ресурси, які держава витрачає на підтримання, зміну чи функціонування інститутів (час, кошти, адміністративні зусилля, політичний капітал), адже надмірні витрати, неефективна структура витрат можуть ставати джерелом уразливості;

8) механізми інституціональних змін (mechanisms of institutional change) – способи оновлення правил гри: реформи, інституційні інновації, поступові корекції, революційні зміни. Структура НМС повинна передбачати наявність керованих, легітимних і прозорих механізмів інституційних змін, щоб адаптація до викликів не руйнувала базові засади системи.

9) інституціональні виклики (institutional challenges) – це напруження, кризи, дефекти у роботі інститутів (корупція, правовий нігілізм, захоплення держави приватними інтересами, неформальні практики, що суперечать праву), які загрожують стійкості;

На основі функціональної імплементації цих категорій в практичну діяльність НМС детермінується як динамічна модель, на основі постійної адаптації та реформування. При цьому важливим «операційним рівнем» є:

10) інституціональні механізми реалізації політики держави (institutional mechanisms of state policy implementation) – інститути, процедури, організаційні форми, за допомогою яких політичні рішення перетворюються на практичні дії й результати (міністерства, служби, агенції, суди, місцеве самоврядування, інструменти е-урядування тощо);

11) інституціональні механізми стійкості державних політик у межах НМС (institutional mechanisms of resilience of public policies within the NMR) –

конкретні «захисні» інструменти, що забезпечують безперервність, передбачуваність і адаптивність політик під час криз – правові запобіжники, резервні процедури, горизонтальні мережі взаємодії. Саме через ці механізми НМС «проявляється» у реальній практиці державного управління й впливає на здатність системи не лише ухвалювати, а й утримувати та оновлювати стратегічні рішення.

Узагальненням усієї системи виступає *інституціональна формула стійкості* в авторському трактуванні (Institutional formula of resilience) – *концептуальне поєднання складників: середовища, формату державотворення, функціонального стану інститутів, балансу між ними, механізмів впливу та змін, витрат і викликів, а також інституційних механізмів стійкості політик*. Ця формула задає логіку побудови НМС – які інститути мають ключове значення, яким має бути баланс влади й автономії, які механізми впливу дозволені, як управляти витратами та змінами (таб.2.1).

Таблиця 2.1

Категорії та поняття інституціонального концепту НМС

Категорія / поняття	Визначення (теоретичний зміст)	Функція в структурі НМС
1	2	3
Категорії інституціонального концепту стійкості	Узагальнювальний метарівень, що позначає систему ключових термінів для стійкості як інституціонального феномену	Слугує концептуальною «рамкою» для побудови моделі, в якій усі інші елементи пов'язуються в цілісну теорію
Суспільні інститути	Стабілізовані форми організації суспільного життя (держава, громада, медіа тощо), що закріплюють норми та ролі	Є базовими носіями стійкості, через них реалізуються функції безпеки, розвитку, інтеграції та контролю
Інституціональне середовище	Сукупність формальних і неформальних правил, норм, традицій і практик, які визначають «правила гри» для акторів	Визначає загальні рамки здійснення політики стійкості, рівень передбачуваності та довіри в суспільстві
Інституційно-нальний формат державотворення	Конкретний спосіб організації влади, розподілу повноважень і взаємодії держави з суспільством	Задає загальну архітектуру НМС: ступінь централізації, участі громадян, відкритості та горизонтальної взаємодії
Функціональна автономність	Рівень здатності інститутів виконувати свої основні функції незалежно від надмірного тиску чи захоплення вузькими інтересами	Визначає, наскільки окремі інститути є опорами стійкості, а не джерелами додаткових ризиків

Продовження таблиці 2.1

1	2	3
Інституціональний баланс	Співвідношення впливу та повноважень між ключовими інститутами, що запобігає монополізації чи хаосу	Забезпечує взаємне стримування й доповнення інститутів, створює умови для гнучкої взаємодії
Система взаємовпливу інститутів (нормативно-правові відносини)	Сукупність правових і організаційних зв'язків між інститутами (закони, регламенти, договори, процедури)	Каналізує взаємодію інститутів у керовані, передбачувані форми, забезпечуючи координацію й узгодження інтересів.
Механізми інституціонального впливу (державного впливу)	Інструменти, через які держава впливає на поведінку інших акторів: регулювання, санкції, стимули, програми	Дає змогу державі коригувати поведінку інститутів у напрямку цілей стійкості, не руйнуючи їхньої автономії
Інституціональні витрати	Ресурси (фінансові, часові, організаційні, політичні), які витрачаються на підтримку та зміну інститутів	Дозволяють визначити «ціну» стійкості; надмірні або неефективні витрати можуть знижувати стійкість
Механізми інституціональних змін	Форми й інструменти оновлення правил гри: реформи, інновації, перегляд процедур, зміна структур	Забезпечують адаптацію системи до нових викликів, зберігаючи її безперервність і легітимність
Інституціональні виклики	Проблеми, дефекти та кризи в роботі інститутів (корупція, недовіра, правовий нігілізм тощо)	Визначають «слабкі місця» НМС, на які мають бути спрямовані реформи та антикризові заходи
Інституціональні механізми реалізації політики держави	Організації, процедури й інструменти, через які політичні рішення втілюються у практичні дії	Перетворюють стратегії стійкості на конкретні програми й результати на рівні громад, регіонів, секторів
Інституціональні механізми стійкості державних політик	Спеціальні інституційні «запобіжники» та резервні процедури, що забезпечують безперервність і адаптивність політик	Утримують політики життєздатними під час криз (зміна умов, урядів, загроз), не допускаючи їхнього колапсу
Інституціональна формула стійкості	Концептуальна конфігурація ключових елементів інституційної системи, що забезпечують стійкість	Синтезує всі інституційні компоненти НМС в єдину логіку, на основі якої можна проєктувати й оцінювати політику
Національна модель стійкості (НМС) як інституціональна платформа	Інтегрована система принципів, інститутів, механізмів і правил, через які забезпечується стійкість держави й суспільства	Є загальною рамкою, в межах якої конструюються, узгоджуються й реалізуються всі інституційні елементи стійкості

Джерело: узагальнено автором

Важливо зауважити, що екзистенційна стійкість національної держави залежить від того, наскільки держава й інститути допомагають громадянам побачити й утримувати сенс спільного життя, сенс боротьби, спротиву, відбудови, взаємної підтримки. У цьому контексті доцільно розрізняти функціональну та екзистенційну стійкість у системі державного управління. *Функціональна стійкість* означає здатність органів влади, публічних служб, систем безпеки, охорони здоров'я, освіти тощо забезпечувати свою роботу навіть у надзвичайних умовах, швидко відновлювати порушені функції, підтримувати керованість процесів. *Екзистенційна стійкість* стосується іншої площини: чи здатна політична спільнота – держава разом із громадянами – зберегти й розвинути відчуття власної гідності, свободи, відповідальності, чи здатна вона перетворити травматичний досвід не лише на статистику втрат, а на джерело глибшого саморозуміння, солідарності, ціннісного оновлення.

З позицій формалізації екзистенційної стійкості варто вказати на наявні теоретичні підходи. Аналіз наукових праць демонструє багатогранний підхід до вивчення формування національної стійкості, охоплюючи різні аспекти: інформаційно-психологічні чинники, механізми державного управління, цифрові ініціативи та правові основи електронного врядування. На думку В.Бондаря [162], національна стійкість є невіддільною частиною системи національної безпеки, зокрема, через вплив інформаційно-психологічного чинника, що підвищує здатність адаптуватися до динамічного середовища загроз. О.Резнікова [96] зосереджується на необхідності вдосконалення методів управління для забезпечення стійкості в мінливому безпековому середовищі. Як зазначає В.Александров [163], підтримка національної стійкості потребує стратегічного й тактичного планування в межах публічного управління. Комплексний підхід, розроблений З.Ковалем і С.Пововим [164], передбачає поєднання стратегій активної оборони та стійких асиметричних дій в умовах інформаційно-психологічної епохи.

Регулювання цифрових процесів є ще одним важливим аспектом

формалізації екзистенційної стійкості. Аналіз законодавства показує, що Україна зробила суттєві кроки в напрямку цифровізації, включаючи ухвалення низки нормативних актів, які створюють необхідні правові засади для розвитку цифрових платформ, гарантування кібербезпеки та захисту даних. Закон України «Про основні засади забезпечення кібербезпеки України» [165] – основний, що визначає головні положення у сфері підтримки кібербезпеки, установлює права та обов’язки суб’єктів у сфері захисту інформації, а також встановлює правила взаємодії державних органів та приватного сектору для підвищення стійкості до кіберзагроз. Закон України «Про електронні довірчі послуги» [166] забезпечує правові основи для використання електронних довірчих послуг, таких як електронні підписи, печатки та інші методи автентифікації в цифровому середовищі. Це сприяє створенню безпечного середовища для обміну інформацією та підвищенню довіри до електронних процесів. Закон України «Про захист персональних даних» [167] визначає основні принципи обробки персональних даних та створює умови для їхнього захисту; сприяє гарантуванню конфіденційності, безпеки та контролю за обробкою персональної інформації, що є важливим для дотримання прав людини в цифровому суспільстві. Закон України «Про електронні комунікації» [168] регулює питання функціонування електронних комунікаційних мереж та послуг, сприяючи створенню конкурентного середовища на ринку цифрових послуг, що забезпечує їхню доступність та якість для всіх категорій користувачів.

Гармонізація із міжнародними стандартами є визначальним елементом державного управління у формуванні цифрової стійкості. У контексті європейської інтеграції Україна активно адаптує національне законодавство до норм Європейського Союзу (ЄС). Зокрема, упровадження положень Загального регламенту захисту даних (GDPR) [169] стало значним кроком у підвищенні рівня захисту персональних даних і забезпеченні прозорості цифрових процесів. Крім того, Україна бере участь в ініціативах Організації Об’єднаних Націй (ООН), спрямованих на розвиток інформаційного

суспільства, таких як Цілі сталого розвитку [170], що охоплюють цифрову інклюзію та доступ до інформаційних технологій.

Національна гармонізація із міжнародними стандартами також передбачає дотримання рекомендацій Міжнародного союзу електрозв'язку (ITU) [171] щодо розвитку цифрової інфраструктури, зокрема широкосмугового інтернету, та участь у глобальних ініціативах із кібербезпеки. Це сприяє інтеграції України у світову цифрову екосистему, забезпечуючи доступ до передових технологій і знань. Інституційні механізми забезпечення цифрової стійкості в Україні базуються на координації діяльності органів державної влади, приватного сектору, наукових установ та громадянського суспільства. Держава відіграє центральну роль у створенні умов для ефективного функціонування цифрового середовища, включаючи розвиток законодавчої бази, стимулювання інновацій та забезпечення захисту інтересів громадян.

Співпраця між органами влади на національному рівні доповнюється партнерством із міжнародними організаціями, такими як Європейська комісія, НАТО та ООН, що дає можливість інтегрувати кращі світові практики у сферу цифрової трансформації. Зокрема, участь у міжнародних проєктах, таких як European Interoperability Framework (EIF) [172], допомагає гармонізувати цифрові послуги з європейськими стандартами. Таким чином, гармонізація із міжнародними стандартами, розвиток інституційних механізмів та ефективна діяльність органів державного управління є важливими елементами національної моделі цифрової стійкості

Дослідження М.Міляєвої [173] підкреслює важливість адаптації нормативного середовища для впровадження електронного врядування, яке має вирішальне значення для ефективності державного управління. Держава активно інвестує в розвиток цифрової інфраструктури, яка є базовою умовою для забезпечення доступу до сучасних технологій у всіх регіонах країни. Завдяки доступу до різноманітних державних електронних послуг громадяни матимуть змогу активно брати участь у суспільному житті та демократичних

процесах, а бізнес – ефективно розвиватися та адаптуватися до сучасних умов [173, 42]. Важливими напрямками є розширення мережі широкосмугового інтернету, упровадження 5G-технологій та модернізація центрів обробки даних. Інвестиції в ці сфери сприяють подоланню цифрової нерівності, що є основним викликом для багатьох країн, включно з Україною. У рамках проєкту EU4DigitalUA спільно з ЄС та естонською Академією електронного управління, Україна продовжує розбудову інфраструктури цифрового уряду, електронних державних послуг, кібербезпеки та захисту даних, використовуючи цифрові інструменти для подолання викликів, пов'язаних із війною. На початок квітня 2024 року було завершено впровадження трьох компонентів проєкту ЄС із бюджетом 10 млн євро, які стосуються розвитку інтероперабельності та інфраструктури цифрового уряду, створення електронних послуг та підтримки кібербезпеки [174].

За підтримки EU4DigitalUA впродовж чотирьох років було масштабовано систему «Трембіта», що дало змогу здійснити 5 млрд безпечних обмінів даними між державними інформаційними системами завдяки модернізації десяти основних державних реєстрів. Також було створено платформу Diia.Engine, упроваджено 59 вебсервісів та 66 вебклієнтів на основі цієї системи. Крім того, проєкт EU4DigitalUA долучився до розвитку 54 електронних послуг, серед яких: «е-Підприємець», «uResidency», цифрові COVID-сертифікати, витяги про несудимість, можливість подання заяви про укладання шлюбу в «Дії» тощо [174].

А.Богоніс [175] акцентує на викликах цифровізації, які потребують інноваційних підходів до їхнього подолання. Міжнародний досвід, представлений у дослідженнях S.Abbasi та B.Jung [176], висвітлює важливі ініціативи цифрового здоров'я, спрямовані на формування стійкості до пандемій. Виклики цифрової трансформації та шляхи їхнього вирішення обговорюються в роботах F. Brunetti та співавторів [177], які пропонують багатосторонні стратегії для адаптації до сучасних умов. Загалом,

екзистенційна стійкість передбачає, що держава, яка прагне зміцнити екзистенційну стійкість, не «готує» громадян до ролі «ресурсу» або «об'єкта захисту», а визнає їхні страждання, дає мову для проговорення травми, створює практики пам'яті, підтримує волонтерські й солідарні ініціативи як простори, де народжується новий сенс спільного буття. Особливо важливим є усвідомлення того, що екзистенційна стійкість громадян прямо пов'язана із суб'єктністю самої держави. Якщо управлінські рішення ухвалюються в логіці закритості, маніпуляції, приховування правди, заперечення масштабів страждання, то формується атмосфера екзистенційної дезорієнтації: люди відчують себе зрадженими, обманутими, позбавленими можливості бути співтворцями спільного майбутнього. Натомість відкритість, діалогічність, визнання болю й помилок, здатність влади брати на себе відповідальність за прийняті рішення створюють умови для того, щоб громадяни могли залишатися суб'єктами, а не жертвами обставин. У цьому сенсі прозорість та підзвітність публічного управління мають не лише правовий чи організаційний, а й глибоко екзистенційний вимір.

Розглядаючи екзистенційний зміст НМС в контексті державного управління, важливо звернути увагу на феномен колективних наративів і пам'яті. Суспільство, яке проходить через війну, окупацію, масові втрати, неминуче формує певні способи розповідати про свій досвід. Ці наративи можуть або підтримувати екзистенційну стійкість (коли підкреслюють гідність, солідарність, здатність вистояти), або, навпаки, відтворювати безсилля й жертвенність (коли акцент робиться лише на стражданні й безнадії). Держава через освітню політику, медіапростір, культуру пам'яті, символічні практики (пам'ятники, дні пам'яті, публічні церемонії) суттєво впливає на те, який характер набувають ці наративи. Якщо публічна влада свідомо сприяє формуванню образу суспільства як спільноти, здатної до відповідального вибору, взаємної підтримки, моральної витривалості, вона вносить свій внесок у зміцнення екзистенційної стійкості нації.

Водночас екзистенційний вимір стійкості має прояв і на рівні самих

інституцій державного управління. Публічні службовці, військові, працівники критичної інфраструктури, освітяни та медики нерідко опиняються в умовах граничної емоційної й моральної напруги. Їхня здатність залишатися суб'єктами, не вигорати остаточно, не втрачати почуття професійної й людської гідності напряду впливає на цілісність системи управління. Тому концепція стійкості має включати не лише технології кризового менеджменту, а й системи підтримки, супервізії, етичних кодексів, професійних спільнот, де працівники можуть осмислювати власний досвід, говорити про складні моральні дилеми, знаходити сенс у своїй роботі. Без цього ризик перетворення публічної служби на механічне виконання інструкцій, позбавлене глибокого відчуття значущості, є надто високим.

Важливим аспектом екзистенційного змісту стійкості є також співвідношення індивідуального й колективного. Людина шукає сенс не в ізоляції, а у взаємодії з іншими. Для державного управління це означає, що підтримка горизонтальних зв'язків, розвиток громад, сприяння самоорганізації є не лише інструментами децентралізації чи участі, а й ключовими умовами екзистенційної стійкості суспільства. Там, де люди відчують себе частиною живого «ми», їхня здатність витримувати страх, втрату, невизначеність істотно зростає. Тому політика стійкості має включати розвиток громадянського суспільства, інститутів співучасті, підтримку локальних ініціатив, які стають просторами для сенсотворення та взаємної підтримки.

Отже, екзистенційний зміст стійкості в контексті державного управління полягає в переході від розуміння стійкості як суто функціональної характеристик системи до усвідомлення її як здатності держави й суспільства разом витримувати зустріч із граничними вимірами буття – смертю, стражданням, невизначеністю, провинною, свободою – без втрати внутрішньої цілісності, гідності та суб'єктності. Для публічної влади це означає необхідність поєднувати технократичні інструменти управління ризиками з гуманітарно-екзистенційним підходом, у центрі якого – людина

як носій сенсу, свободи, відповідальності. Саме інтеграція цих вимірів дає змогу говорити про національну стійкість не лише як про здатність «вижити», а як про здатність продовжувати жити по-людськи, відновлювати й примножувати простір людської гідності навіть у найтяжчих історичних випробуваннях.

Формування національної НМС є фундаментальним завданням державного управління в епоху тотальної невизначеності та системних загроз. Перехід від фрагментарного, секторального реагування на кризи до створення інтегрованої, цілісної системи, що забезпечує довготривалу безпеку й розвиток нації, вимагає не лише практичних рішень, а й глибокого теоретичного переосмислення самого поняття стійкості. Акцепт ефективного функціонування сучасної НМС полягає у розумінні, що розвиток і захист держави залежить від реальної взаємодії основних сфер суспільного життя: економіки, соціальної політики, екології, політичного устрою та безпеки. У стійкості немає містики – на ній безпосередньо відображається процес державотворчих реформ, управління ресурсами, єдності спільноти, ефективності рішень і наявності ціннісних підвалин.

Зміцнення національної стійкості можливе лише шляхом цілеспрямованого розвитку кожної з базових підсистем і побудови ефективного механізму взаємозв'язків між ними. Важливо визнати, що жоден загальний рівень стійкості суспільства чи держави не може бути вищим за рівень стійкості її складових структурних елементів. Інакше кажучи, міцність та здібність країни долати виклики безпосередньо залежать від стану економіки, соціального клімату, якості інституцій, кондиції довкілля, оборонного потенціалу, злагодженості громад, та від системи цінностей, що скріплює їхній розвиток. Тому теоретичні засади формування НМС мають ґрунтуватися на низці системних принципів, які визначають і стратегічний напрямок державної політики, і організаційну структуру прийняття рішень, і філософію державного управління.

2.2. Принципи формування національної моделі стійкості у форматі цифрового суспільства

Розвиток на власних засадах національної моделі стійкості у форматі цифрового суспільства потребує логічного пояснення не лише у конструкції «як має функціонувати НМС», а насамперед – «що саме вона являє собою в умовах цифрової трансформації». Звернення до онтології у цьому контексті є не даниною абстрактній теоретизації, а методологічною передумовою подальшого викладу, і дає змогу зафіксувати, що цифрове суспільство змінює саму природу національної стійкості – з властивості окремих інститутів вона перетворюється на емерджентну характеристику складної, мережевої, багаторівневої системи державного (публічного) управління. Саме тому принципи формування НМС мають виводитися не з традиційних уявлень про стабільність та ієрархію, а з онтологічних особливостей нової реальності, де доведеної ключової ваги набувають інституційна спроможність держави, адаптивність її організаційних структур і здатність до багаторівневої координації.

Цифрова трансформація докорінно змінює онтологічний статус соціальних систем, трансформує значну частину суспільних взаємодій, управлінських процесів та безпекових викликів у принципово новий вимір, гібридний простір, де фізична і віртуальна реальності не просто співіснують, а утворюють нерозривну цілісність з власною логікою становлення і розвитку. У цьому просторі національна стійкість як феномен суспільного розвитку набуває нових онтологічних характеристик, що вимагають глибинного переосмислення самого способу її концептуалізації та практичного забезпечення.

Якщо традиційно національна безпека і стійкість розглядалися крізь призму територіальності, матеріальних ресурсів та централізованих ієрархій (дослідження Н.Нижник, Г.Новицького, В.Голуб, Г.Фердмана [178-181], то цифрове суспільство породжує новий тип вразливостей і можливостей, де

визначальними стають інформаційні потоки, мережеві структури та розподілені системи управління.

У цифровому суспільстві сама природа держави як інституту зазнає фундаментальних трансформацій. Суверенітет, ідентичність, легітимність – ці базові категорії державності набувають нового змісту, коли цифрові технології розмивають кордони, створюють транснаціональні спільноти і формують альтернативні джерела суспільної довіри. Варто вказати на дослідження М.Кастелса, щодо появи «мережевого суспільства», транснаціональних спільнот і нових форм влади та ідентичності, які змінюють роль і природу держави [182], також С.Сассен, яка аналізує, як глобалізація та цифрові мережі змінюють конфігурацію суверенітету, перерозподіляють владні повноваження та послаблюють традиційні державні кордони [183]. У таких умовах національна модель стійкості постає не лише як набір інституційних механізмів та антикризових протоколів, а як онтологічна основа існування держави в новому типі реальності – цифровому (як варіант у багатьох дослідників – діджиталізованому), мережевому, постійно змінюваному. Отже, фактично спостерігається становлення принципово нової форми буття суспільних систем, де стійкість визначається не стабільністю структур, а їхньою здатністю до безперервної самоорганізації та адаптації.

Особливість цифрової онтології полягає в тому, що вона радикально змінює темпоральні та просторові параметри безпекових викликів. Загрози виникають і поширюються зі швидкістю інформаційних потоків, кризи набувають трансграничного характеру, а ланцюжки причинно-наслідкових зв'язків стають настільки складними, що традиційні лінійні моделі реагування виявляються принципово неадекватними. У цьому контексті сама категорія стійкості потребує нового онтологічного статусу – не як здатності повертатися до попереднього стану (резильєнтності в класичному розумінні), а як спроможності до проактивної самоорганізації та випереджувальної трансформації в умовах постійної невизначеності.

Національна модель стійкості в цифровому суспільстві не може базуватися на презумпції передбачуваності загроз та уніфікованих протоколах реагування. Її онтологічним підґрунтям стає визнання принципової непередбачуваності складних систем та здатність до безперервної адаптації через формування багаторівневих і багатовимірних зв'язків між державою, громадянським суспільством, бізнесом та міжнародними структурами. Ми маємо справу з парадигмальним зрушенням: від розуміння стійкості як протидії загрозам до її тлумачення як неперервного процесу становлення нових форм суспільної організації, здатних відповідати на виклики, що постійно еволюціонують.

Отже, у процесі становлення НМС ключовими елементами забезпечення національної безпеки та ефективного реагування на кризи є інституційна спроможність держави, адаптивність її організаційних структур і здатність до багаторівневої координації. Інституційна спроможність у цифровому контексті набуває статусу онтологічної категорії, що відображає не просто наявність формальних інституцій, а їхню здатність функціонувати як цілісний живий організм, спроможний сприймати, аналізувати та реагувати на зміни в режимі реального часу. Адаптивність структур перетворюється з операційної характеристики на буттєву ознаку системи, що визначає саму можливість її існування в умовах постійних змін і гібридних загроз. Багаторівнева координація постає як нова форма колективної суб'єктності, де єдина воля та стратегічне бачення реалізуються не через вертикальні директиви, а через гармонізацію дій численних автономних учасників. Така онтологічна трансформація вимагає принципово нових підходів до формування національної моделі стійкості, заснованих не на статичних структурах та чітких ієрархіях, а на динамічних мережах взаємодії, здатних до самоорганізації та еволюції. У цифровому форматі стійкість перестає бути властивістю окремих інституцій чи систем – вона стає емерджентною характеристикою всього суспільства як складної адаптивної системи, де технологічні, соціальні, політичні та економічні елементи

утворюють єдину екосистему безпеки і розвитку.

У цьому контексті звернення до принципів формування національної моделі стійкості у форматі цифрового суспільства набуває не суто нормативного, а засадничо-онтологічного характеру. Йдеться не просто про визначення бажаних управлінських підходів чи організаційних рішень, а про фіксацію тих базових засад, які випливають із самої природи сучасного суспільства як цифровізованої, мережевої, високодинамічної системи. Принципи НМС у такому ракурсі мають розглядатися як концептуальні орієнтири, що відображають внутрішню логіку функціонування і розвитку цієї системи, задають рамки допустимих інституційних конфігурацій і визначають умови, за яких стійкість може взагалі бути досягнута та підтримана. Саме тому подальший аналіз буде спрямований на виокремлення й обґрунтування ключових принципів формування національної моделі стійкості у форматі цифрового суспільства, які кореспондують із визнаною онтологічною реальністю непередбачуваності, мережовості та багаторівневості сучасних соціальних систем. Ці принципи покликані забезпечити узгодження між інституційною спроможністю держави, її організаційною адаптивністю та ефективною багаторівневою координацією, перетворюючи НМС на цілісну інституціональну рамку, здатну інтегрувати різні ресурси і суб'єктів у єдину екосистему національної безпеки та розвитку. На цій основі доцільно перейти до їх системного викладу.

1. *Відповідно до принципу системної залежності* національна стійкість являє собою відображення якості та взаємодії базових підсистем держави: економічної, соціальної, екологічної, політичної, безпекової. Будь-яке послаблення однієї з них з часом неминуче проявиться як зниження життєздатності держави загалом. Відповідальне управління мусить спиратися на системний моніторинг, аналіз та прогнозування стану цих підсистем, виявлення потенційно найбільш уразливих точок. Для цього впроваджується система індикаторів та індексів, які фіксують якість інституцій, динаміку економіки, суспільну згуртованість, стан довкілля, рівень готовності до

надзвичайних ситуацій (таблиця 2.2).

Таблиця 2.2

Формалізація змісту системної залежності для концепту НМС

Підсистема	Роль у стійкості держави	Ключові індикатори/індекси	Типові ризики/вразливості	Механізм моніторингу та управління
Економічна	Забезпечення ресурсної та виробничої основи, здатність до відновлення	ВВП, рівень зайнятості, резерви, темпи зростання, індекс конкурентоспроможності, рівень диверсифікації економіки	Залежність від окремих секторів, криза банків, зовнішня заборгованість, падіння інвестиц. клімату	Економічний моніторинг, раннє попередження ризиків, розробка антикризових резервів та стратегій
Соціальна	Формування людського капіталу, соціальної згуртованості, стійкості громад	Індекс людського розвитку (HDI), рівень нерівності, доступ до освіти і медицини, рівень довіри, демографічна динаміка	Відтік кадрів, криза систем охорони здоров'я, нерівність, соціальна ізоляція, міграція	Соціологічні опитування, моніторинг добробуту, стратегія соціальної інтеграції, підтримка вразливих груп
Екологічна	Гарантування тривалих природних ресурсів та придатності території	Індекс екологічної ефективності, рівень забруднення, стан водних/земельних ресурсів, рівень ризику катастроф	Деградація довкілля, природні катастрофи, скорочення ресурсів, кліматичні зміни	Екологічний моніторинг, оцінка екологічних ризиків, впровадження «зелених» технологій і адаптаційних заходів
Політична	Підтримання легітимності, довіри та стійкості державних інститутів	Індекс верховенства права, індекс демократії, рівень довіри до влади, показники корупції, політична стабільність	Кризи легітимності, політична фрагментація, корупція, ерозія довіри, зовнішній вплив	Моніторинг політичної стабільності, аудит інституцій, підтримка комунікації з громадянським суспільством
Безпекова	Фізичне збереження державності, громадська та стратегічна безпека	Глобальний індекс миру, рівень злочинності, оборонний бюджет, готовність до надзвичайних ситуацій, кібер-інциденти	Війна, тероризм, кіберзагрози, зниження обороноздатності, надзвичайні ситуації	Система раннього реагування, територіальна оборона, аудити безпеки, тренування і симуляції

Джерело: розроблено автором

Принцип системної залежності у формуванні НМС є однією із основних інтелектуальних опор, що дозволяє не лише теоретично осмислити феномен стійкості, а й впровадити його у практику державного управління. Національна стійкість у сучасних умовах є не просто здатність державних інституцій чинити опір зовнішнім і внутрішнім викликам, а й результат

якісної взаємодії фундаментальних підсистем: економічної, соціальної, екологічної, політичної та безпекової. У функціональній цілісності цих сфер полягає не лише потенціал до виживання, а й до розвитку, стратегічної перебудови під тиском змін, адаптації до нових ризиків та сценаріїв майбутнього.

Розглядаючи економічну підсистему, слід зважати не тільки на базові макроекономічні показники, такі як ВВП чи темпи індустріального розвитку, а й на здатність економіки швидко адаптувати виробництво, створювати додану вартість, впроваджувати інновації та підтримувати зайнятість навіть у кризові періоди. Розглядаючи економічну підсистему, слід зважати не тільки на базові макроекономічні показники, такі як ВВП чи темпи індустріального розвитку, а й на здатність економіки швидко адаптувати виробництво, створювати додану вартість, впроваджувати інновації та підтримувати зайнятість навіть у кризові періоди. Емпіричні дослідження І.Квеліашвілі у сфері державного управління бюджетною системою доводять, що саме якість правових механізмів бюджетного регулювання та прозорість процедур розподілу ресурсів визначають спроможність держави підтримувати критичні галузі в умовах шоків, не допускаючи деструктивних перекосів у структурі видатків [184-187]. Аналіз фінансово-економічної безпеки підприємств показує, що ті суб'єкти, які поєднують жорсткий контроль за ризиками з проактивною інвестиційною та інноваційною політикою, краще витримують турбулентність ринкового середовища й зберігають зайнятість.

Розглядаючи економічну підсистему, слід зважати не тільки на базові макроекономічні показники, такі як ВВП чи темпи індустріального розвитку, а й на здатність економіки швидко адаптувати виробництво, створювати додану вартість, впроваджувати інновації та підтримувати зайнятість навіть у кризові періоди. У працях професора І.Квеліашвілі підкреслюється, що саме така адаптивність формує економічну стійкість, яка є ключовим компонентом національної стійкості як здатності держави витримувати та поглинати зовнішні й внутрішні шоки без втрати керованості та

стратегічного курсу. З правового боку вирішальним є якісний інституційний дизайн бюджетної сфери: прозорість норм, узгодженість повноважень і механізмів контролю визначають, чи стає бюджет інструментом посилення стійкості, а не лише перерозподілу ресурсів. На мікрорівні економічна стійкість пов'язана з фінансово-економічною безпекою підприємств, що забезпечується системним моніторингом ризиків, належним корпоративним управлінням і підтримкою інноваційної активності. Водночас ефективні комунікаційні стратегії державних органів, зокрема в митній сфері, знижують транзакційні витрати, сприяють детінізації та формують передбачуване регуляторне середовище, інтегруючи окремі галузеві й регіональні практики у цілісну архітектуру національної стійкості [187].

Додатковим чинником стійкості виступають комунікаційні стратегії на стику держави та бізнесу, зокрема в митній сфері: узгоджені інформаційні потоки, прогнозовані процедури та цифрові канали взаємодії скорочують транзакційні витрати, зменшують корупційні ризики й підвищують передбачуваність регуляторного середовища для інвесторів. Надмірна залежність від одного чи декількох секторів, критична зовнішня заборгованість або падіння інвестиційної привабливості можуть швидко перейти з економічної сфери у соціальний чи навіть політичний вимір. Відтак, системний економічний моніторинг із застосуванням індексів конкурентоспроможності, рівня диверсифікації економічної діяльності, показників зайнятості та стійкості банківського сектору дозволяє своєчасно фіксувати ознаки наближення кризових явищ, і не лише реагувати на них, а й упереджувати їхні наслідки. Наявність антикризових резервів і розробка сценаріїв швидкого реагування є компонентом економічної стійкості.

У соціальній підсистемі теоретики та практики управління все більше визнають, що рушієм стійкості виступає не лише «міцна» інституціональна структура, а й якість людського капіталу, рівень суспільної згуртованості, розвиток освіти, охорони здоров'я, наявність механізмів соціальної підтримки. Відтік кваліфікованих кадрів, поглиблення соціальної нерівності,

зростання ізоляції уразливих груп або демографічна криза становлять потенційно кризові процеси, які можуть радикально знизити не лише соціальну, а й політичну, економічну і безпекову стійкість (І.Хожило, О.Бобровська) [188]. Саме тому важливо впроваджувати універсальні показники, зокрема Індекс людського розвитку, рівень доступу до освіти й медицини, соціологічні індекси довіри й добробуту, демографічну динаміку і міграційні тренди. Глибоке розуміння цих параметрів дає змогу не просто стабілізувати соціальне поле у гострі моменти, а й формувати стратегії соціальної інтеграції, сприяти розвитку громадянського суспільства та розширювати можливості для самоврядування людей і спільнот.

Екологічна підсистема в контексті національної стійкості все частіше розглядається не як обмеження для економічного розвитку, а як передумова тривалої життєздатності країни, її територій і населення. Забруднення довкілля, деградація ґрунтів, скорочення запасів чистої води, неконтрольована урбанізація або кліматичні зсуви можуть у перспективі породжувати цілі «ланцюги уразливості», які змінюють структуру зайнятості, міграцію, підвищують ризик соціальних протестів чи навіть міжрегіональних конфліктів. Тому застосування індексів екологічної ефективності, картографування екологічних ризиків, впровадження екомоніторингу та екологічних адаптивних технологій є не менш важливими, ніж зміцнення енергетичних чи економічних підсистем. Екоінвестиції, розвиток «зеленої» економіки і просвіта у сфері сталого розвитку мають входити до стратегічного ядра національної моделі стійкості (Г.Блінова) [189].

Політична підсистема є своєрідною «нервовою системою» НМС. Її здатність до саморегуляції, вирішення конфліктів, акумуляції і легітимації влади, оперативної адаптації інституцій до нових викликів визначає, чи зможе країна проходити через кризи без втрати єдності й довіри. Індекси верховенства права, рівня корупції, політичної стабільності, демократії є вимірниками здоров'я державного організму. Тривала політична нестабільність, зростання рівня недовіри до уряду, кризи представництва чи

прояви системної корупції можуть ініціювати ланцюгові реакції й паралізувати потенціал антикризового управління (М.Пірен) [190]. Постійний моніторинг політичного поля, розвиток комунікативних стратегій між владою та громадянським суспільством, проведення аудитів ефективності інституцій, побудова інклюзивних механізмів участі та контролю – як базові елементи політичної стійкості.

Безпекова підсистема формує основу національного виживання, виступає очевидним прототипом стійкості. Йдеться не лише про традиційну оборону, а й про розвиток системи реагування на надзвичайні ситуації, кібербезпеки, тероризм, стратегічний аналіз складних ризиків і багаторівневу систему захисту – від особистого, локального до державного (Н.Драгомирецька, І.Колосовська) [191;192]. Глобальний індекс миру, дані про злочинність, оборонний бюджет, індекси кіберзагроз, рівень інтегрованості сил територіальної оборони та швидкодія систем екстреного реагування – все це базові кількісні й якісні індикатори стійкості у сфері безпеки. Якщо безпекова система страждає від недофінансування, відсутності координації, монополізації інформації чи недостатнього рівня підготовки населення, слабкість може швидко поширюватись на всі інші сфери – від політичної (колапс довіри до влади) до економічної (зупинка виробничого процесу, втеча інвесторів, блокада логістики).

Важливим висновком щодо значення принципу системної залежності для НМС є необхідність не розглядати підсистеми у відриві одна від одної. Їх взаємні зв'язки, надбудови та зони перетину стають критично значущими під час багатокomпонентних криз [193]. Наприклад, екологічна катастрофа (повінь, пожежа) може зруйнувати економіку регіону, спровокувати масову міграцію, створити політичний конфлікт і поставити під удар безпекову систему. Або ж тривала політична криза може заблокувати якісне функціонування економічних і соціальних програм, підривати громадську згуртованість і гальмувати реформування критично важливих секторів.

Кожній із підсистем відповідає своя окрема система індикаторів і

методів аналізу, але для підвищення національної стійкості потрібна інтегрована система моніторингу, яка дозволяє виявляти «слабкі місця» на стиках підсистем та прогнозувати виникнення системних ризиків завдяки міждисциплінарному аналізу. Це передбачає створення міжвідомчих центрів, використання складних інформаційних платформ, залучення до моніторингу не лише державних, а й громадських організацій; кооперацію з міжнародними експертами у сфері ризик-менеджменту.

Відповідальне державне управління на основі принципу системної залежності включає запровадження не тільки інструментів фіксації параметрів (індекси, показники), а й запобіжних механізмів: форсайт-досліджень, сценарного планування, тестування систем на вразливість, моделювання розгортання криз. Це передбачає вміння швидко мобілізувати переваги стійких підсистем для компенсації вразливостей інших, інвестувати в ті вузькі місця та зв'язки, котрі є потенційними «точками прориву» системної кризи. Усі ці моменти втілюються в єдину практику стратегічного державного управління, що сприймає країну як багаторівневу систему із складними горизонтальними та вертикальними взаємозалежностями. Справжня стійкість виникає лише там, де моніторинг стану основних підсистем, глибокий аналіз зон ризику, а також готовність до швидкого управлінського реагування, спрямованого не на латання, а на підсилення основ фундаменту.

Варто підкреслити, що принцип системної залежності є основною гарантією актуальності і практичної дієздатності національної моделі стійкості. Там, де держава обмежується «відносинами успіху» (квазі-успіх) лише в одній сфері – економіці, безпеці, чи в соціальній сфері, – на стратегічному горизонті це обов'язково призводить до ускладнення проблем у решті підсистем. Тільки постійний перегляд взаємодії всіх основ, націлений на збереження балансу, дає змогу розвивати національні системи так, щоб жодна із ланок не стала вирішально слабкою «точкою прориву» загальної стійкості. Державна політика у даній парадигмі має бути не реактивною (за

принципом «чекаємо на кризу й реагуємо»), а превентивною, стратегічною, націленою на розвиток сильних і «вразливих» ланок одночасно. Тільки за таких умов слід говорити про справжню національну стійкість у комплексному розумінні цього поняття.

2. *Принцип цілісності та інтегративності.* Формально, національна стійкість – це цілісна властивість соціоприродної системи, а не сума окремих елементів. Надійність і живучість життєдіяльності досягаються лише тоді, коли встановлюється продуктивний діалог і співпраця між секторами. Якість служб у сфері економіки має погоджуватися з екологічними пріоритетами; соціальна політика повинна бути узгоджена з тенденціями демографічного розвитку й безпековими потребами; політичні реформи мають враховувати потреби збереження громадської довіри і національної ідентичності. Для цього створюються інтегровані платформи, що координують політику, основою яких є цифровий контур управління.

Принцип цілісності та інтегративності посідає фундаментальне місце в архітектоніці національної моделі стійкості, особливо в умовах цифрового суспільства. Його сутність полягає в тому, що стійкість розглядається не як сума окремих політик, інструментів чи секторних реформ, а як емерджентна властивість цілісної соціоприродної системи. У цій системі економічні, соціальні, політичні, безпекові, екологічні й цифрово-інформаційні підсистеми тісно переплетені й постійно взаємодіють. Слабкість або дисфункція будь-якої з них неминуче відбивається на загальній здатності держави і суспільства витримувати удари, адаптуватися до змін і відновлюватися після криз. У традиційній, секторальній логіці державного управління кожен блок політики, економічний, соціальний, екологічний, оборонний, гуманітарний – розвивається відносно автономно. Таке «інституційно ізольоване» мислення історично було зручним із погляду бюрократичної організації, але в умовах високої взаємозалежності й цифрової взаємопов'язаності воно створює системні вразливості. Економічні рішення, ухвалені без урахування екологічних ризиків та довгострокових

демографічних трендів, можуть сформувати підґрунтя для майбутніх соціальних і політичних криз. Політичні реформи, які ігнорують вимір суспільної довіри й національної ідентичності, здатні підірвати легітимність інститутів та ускладнити реалізацію навіть добре продуманих безпекових стратегій.

У цифровому суспільстві вимога до цілісності та інтегративності посилюється багаторазово (Г.Ортіна) [194]. По-перше, тому що зростає швидкість поширення кризових імпульсів: кіберінцидент або інформаційна атака можуть майже миттєво трансформуватися в економічну дестабілізацію, кризу довіри до інститутів, заворушення у фізичному просторі. По-друге, тому що зменшується «видимість» традиційних кордонів між секторами: цифрові платформи одночасно є економічною інфраструктурою, інформаційним середовищем, політичним майданчиком та об'єктом безпеки. По-третє, тому що дані й алгоритми стають новим системоутворюючим фактором, який пов'язує різні політики в єдиний контур прийняття рішень.

Отже, цілісність в межах НМС не може розумітися лише як декларативна «узгодженість» документів чи формальна міжвідомча координація. Йдеться про структурну вимогу: планування розвитку, безпеки та цифрової трансформації має здійснюватися в інтегрованому форматі, з урахуванням системних ефектів у різних підсистемах. Наприклад, економічна політика, орієнтована на інтенсивну індустріалізацію, повинна одразу оцінюватися крізь призму екологічної стійкості, кліматичних зобов'язань, впливу на здоров'я населення та навантаження на систему охорони здоров'я. Соціальна політика розглядатися у зв'язку з демографічним старінням, міграційною динамікою, потребами сектору безпеки й оборони, цифровими навичками населення.

Інтегративність, у свою чергу, означає здатність держави та суспільства виробляти узгоджені рішення на перетині кількох сфер, залучаючи до цього не лише різні органи влади, а й бізнес, науково-освітнє середовище, громадянське суспільство та місцеві громади. У форматі цифрового

суспільства формуються нові платформи для такої інтеграції, зокрема, електронні платформи спільного планування, системи обміну даними між відомствами, центри ситуаційної обізнаності, де аналізується інформація з різних джерел у режимі реального часу. Це дає змогу виявляти системні ризики раніше, ніж вони переростають у масштабні кризи, і обирати політики, які одночасно підсилюють кілька вимірів стійкості, а не посилюють один за рахунок руйнування іншого (таблиця 2.3).

Таблиця 2.3

Узагальнені виміри національної стійкості та їх інтерпретація

Компонента	Коротка інтерпретація	Домінуючі індикатори (приклади)	Орієнтовна частка поясненої варіації, %
Інституційно-управлінська	Якість державного управління, ефективність інститутів, спроможність до координації	Рівень довіри до органів влади; індекси верховенства права; швидкість ухвалення рішень; ступінь міжвідомчої взаємодії	25–30
Соціально-демографічна	Стан людського капіталу, соціальна згуртованість, демографічна динаміка	Структура населення за віком; рівень освіти; показники бідності й нерівності; участь громадян у громадському житті	15–20
Економічно-інфраструктурна	Сталість економічного розвитку та живучість критичної інфраструктури	Диверсифікація економіки; рівень зайнятості; стан транспортної, енергетичної, цифрової інфраструктури	15–20
Безпеково-оборонна	Спроможність гарантувати внутрішню й зовнішню безпеку	Обороздатність; ефективність сектору безпеки; рівень злочинності; готовність системи цивільного захисту	10–15
Екологічно-кліматична	Здатність системи зберігати природні ресурси та адаптуватися до кліматичних змін	Якість повітря й води; стан екосистем; викиди парникових газів; частота екстремальних погодних явищ; витрати на адаптацію	10–15
Цифрово-інформаційна	Розвиток цифрових сервісів, кіберстійкість та якість інформаційного середовища	Рівень цифровізації послуг; кіберінциденти; медіаграмотність; поширення дезінформації; доступ до інтернету	10–15

Джерело: дослідження автора

Показник «Частка поясненої варіації» вказує, який відсоток загальної мінливості всіх початкових показників для НМС охоплює одна така узагальнена компонента (дослідження проведене у межах теми НДР «Забезпечення стійкості, ревіталізації та розвитку територій і громад в Україні» (ДР 0122U002375)

Важливою передумовою реалізації принципу цілісності є переосмислення самого об'єкта державного управління (І.Сафаров) [195]. Отже, національна стійкість розглядається як характеристика цілісної соціоприродної системи, де громадяни, інститути, інфраструктура, природне середовище, технологічні мережі та інформаційні потоки утворюють єдину екосистему [196]. Фактично, аналітика стійкості має спиратися не лише на параметри окремих секторів, а й на інтегровані індикатори, які відображають їхню взаємодію: ступінь кореляції між економічними та екологічними ризиками, взаємозв'язок між рівнем довіри до інститутів та швидкістю відновлення після криз, вплив цифрової нерівності на соціальну згуртованість тощо. У такій логіці, як показують наші дослідження, набуває сенс групування численних показників стану системи у відносно незначну множину узагальнених вимірів, які дозволяють побачити структуру національної стійкості і визначити, як саме реалізується принцип цілісності [197]. Це дає змогу перейти від хаотичного переліку окремих індикаторів до цілісного бачення, в якому різні аспекти стійкості системно пов'язані між собою.

Представлені узагальнені виміри показують, що принцип цілісності передбачає не механічне додавання секторних індикаторів, а їх інтеграцію у взаємопов'язані блоки, які відображають структурні основи національної стійкості. Вони також демонструють, що жоден із вимірів не може забезпечити стійкість сам по собі: навіть високий рівень економічного розвитку не гарантує здатності до ефективного реагування на кризи, якщо інституційні механізми координації слабкі, суспільна довіра низька, а

цифрове середовище вразливе до маніпуляцій. Далі важливо показати, як принцип цілісності та інтегративності змінює сам характер публічної політики: від фрагментованих рішень до інтегрованих стратегій, які одночасно працюють у кількох вимірах стійкості. Це особливо важливо для цифрового суспільства, де значна частина взаємодій відбувається у мережових форматах, а кордони між секторами розмиті (рис.2.2).

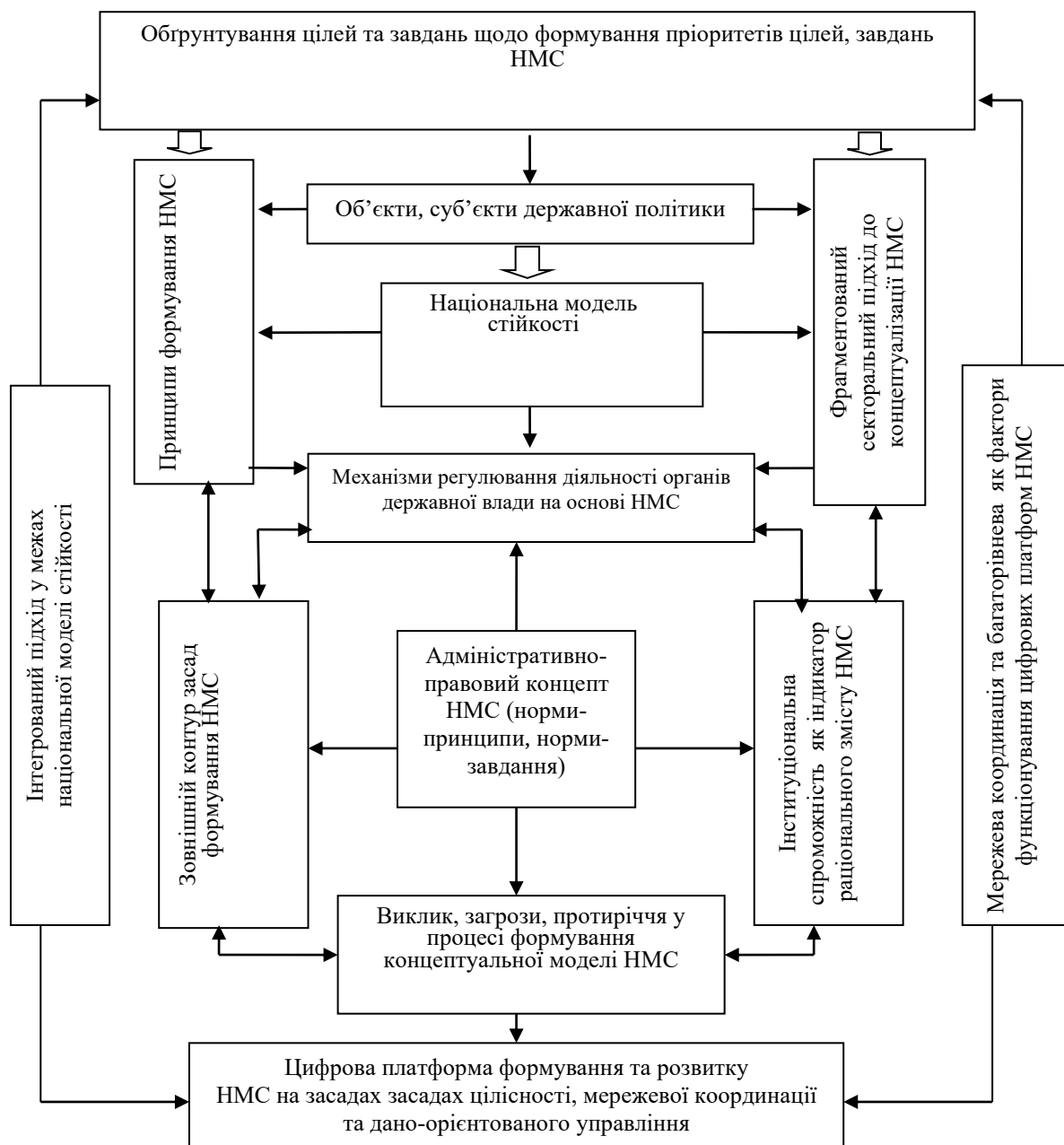


Рис. 2.2. Дескриптивна модель змісту принципу цілісності та інтегративності у структурі НМС

Джерело: розроблено автором

Для ілюстрації якісної різниці між фрагментованим та інтегрованим підходами до формування НМС доцільно розглянути порівняльну таблицю 2.4 організації механізмів державного управління в низці ключових сфер .

Таблиця 2.4

Реалізація принципу цілісності та інтегративності в основних сферах
формування державної політики

Сфера / вимір	Фрагментований (секторальний) підхід	Інтегрований підхід у межах національної моделі стійкості	Наслідки для національної стійкості
Економічна політика	Орієнтація на зростання ВВП без урахування екологічних, соціальних і безпекових обмежень	Поєднання цілей зростання з екологічною та енергетичною стійкістю, врахування впливу на громади	Зниження вразливості до шоків, зменшення структурних дисбалансів
Екологічна та кліматична політика	Реактивні заходи, локальні проєкти без зв'язку з економічним і просторовим плануванням	Вбудовування екологічних цілей у стратегії розвитку, інфраструктурні інвестиції, містобудування	Запобігання екологічним кризам, стає управління ресурсами
Соціальна політика й демографія	Підтримка вразливих груп без стратегічного бачення людського капіталу та міграційних трендів	Комплексні програми, що поєднують освіту, охорону здоров'я, зайнятість, демографічну та міграційну політику	Підтримка людського потенціалу, зменшення соціальної напруги
Безпека, оборона та цивільний захист	Оборонні й правоохоронні заходи ізольовані від економіки, освіти, місцевого самоврядування	Мережеві моделі «системної оборони», інтеграція можливостей громад, бізнесу, освітніх і наукових інституцій	Формування суспільної стійкості, підвищення спроможності до тривалої протидії загрозам
Політичні реформи та інституційна довіра	Технічні зміни інституцій без урахування довіри, ідентичності, участі громадян	Реформи, що поєднують інституційний дизайн із механізмами залучення громадськості й збереження ідентичності	Зміцнення легітимності, зниження ризиків дестабілізації
Цифрова трансформація та інформаційна безпека	Цифровізація як технічний проєкт, відокремлений від безпеки, прав людини, соціальної політики	Комплексний підхід: е-сервіси, кібербезпека, захист даних, медіаграмотність, протидія дезінформації	Підвищення довіри до цифрових рішень, стійкість інформаційного простору
Просторова (регіональна) політика	Централізовані програми, які ігнорують місцеві ризики, потенціали й ідентичності	Стратегії, побудовані на місцевих діагнозах стійкості, інтегровані в загальнонаціональну рамку	Збалансований розвиток територій, посилення стійкості громад

Джерело: розроблено автором

Принцип цілісності та інтегративності забезпечує функціонування НМС як єдиної соціосистеми, у якій економічні, соціальні, політичні, безпекові, екологічні та цифрові виміри розглядаються у взаємозв'язку, а не ізольовано. Реалізація цього принципу перетворює цифрову платформу НМС на простір інтегрованого управління, де дані, інститути й стейкхолдери поєднуються в єдиний контур аналізу, планування та реагування. Реалізація цього принципу мінімізує конфліктність політик, підвищує узгодженість рішень і робить національну стійкість емерджентною властивістю всього суспільства, а не окремих секторів.

3. *Принцип субсидіарності та розподіленої відповідальності* є одним із ключових організаційних засадничих принципів функціонування НМС, особливо в умовах цифрового суспільства й тривалих кризових впливів. Його зміст полягає в тому, що завдання мають вирішуватися на тому спроможному рівні, де такі рішення є максимально ефективними, та наявними виступають реальна компетентність, ресурси, довіра й знання територіального контексту. При цьому органи управління більш високого порядку не підміняють собою локальні спільноти, а створюють для них рамкові умови, координують, підтримують і беруть на себе лише ті функції, які об'єктивно не можуть бути виконані на базовому рівні. Разом з тим, важливо вказати, що субсидіарність – це вертикально-інтегрований принцип, і може передбачати розподіл повноважень як на базові управлінські рівні – рівень ОМС, так і на рівень інститутів ЄС.

У самоврядному концептуальному підході національна стійкість перестає бути функцією лише «владної вертикалі», а виступає як складник трансформації інститутів громадянського суспільства (О.Кравцов, В.Баштанник, С.Кандзюба, О.Титаренко) [198-200]. Адже мова йде про мережу громад, локальних спільнот, організацій і відповідальних громадян, які здатні самостійно оцінювати ризики, планувати розвиток, формувати локальні стратегії безпеки й брати участь у відновленні після криз. Розподілена відповідальність означає не перекладання обов'язків держави на

громадян, а чіткий розподіл ролей і повноважень між рівнями управління з одночасним посиленням їхньої взаємодії та взаємної підзвітності.

У цифровому суспільстві цей принцип набуває особливої ваги. З одного боку, цифрові платформи дозволяють організувати масштабовану участь громадян і громад у плануванні та моніторингу політик: від електронних петицій, партисипативного бюджетування й краудсорсингу рішень до локальних систем раннього попередження, де мешканці самі фіксують ризики, інциденти й потреби. З іншого боку, цифрові інструменти дають змогу державі забезпечити прозорий доступ до даних, стандартів, рекомендацій, що є необхідною умовою для усвідомленої та відповідальної участі місцевого рівня в реалізації НМС [201].

Принцип субсидіарності передбачає наявність комплексу рівнів управління стійкістю – національного, регіонального, місцевого та рівня організацій/домогосподарств, між якими розподіляються функції аналізу ризиків, планування, реагування та відновлення. Кожен із цих рівнів має власну зону компетенції, однак жоден не може бути повністю автономним: національний рівень задає нормативну рамку, фінансові інструменти та загальну архітектуру НМС; регіональний – інтегрує міжмуніципальні ресурси; місцевий – забезпечує безпосередній контакт із населенням і територією; організації та громадяни – є останньою лінією адаптації, самоорганізації та самооборони. Розподілена відповідальність у такій системі означає також розподілену спроможність, адже, на думку британських дослідників Н.Бродхарста та Н.Грея, не лише повноваження, а й ресурси, дані, компетентності, інституціональні механізми мають бути розгорнуті «по мережі» [202]. Інакше субсидіарність перетворюється на псевдодецентралізацію, коли на місцевий рівень передаються завдання без належних інструментів для їх виконання, що, своєю чергою, підриває довіру до держави й демотивує громадянську участь (таблиця 2.5).

Таблиця 2.5

Компоненти реалізації принципу субсидіарності та розподіленої
відповідальності в НМС

Компонента	Коротка інтерпретація	Ключові індикатори (приклади)	Орієнтовна частка внеску в загальну стійкість, %
Інституційно-правова	Ступінь закріплення субсидіарності, автономії громад і розподілу повноважень у законодавстві та політиках	Конституційні норми щодо місцевого самоврядування; закони про децентралізацію; повнота компетенцій громад; наявність чітких мандатів	20–25
Організаційно-управлінська	Якість механізмів багаторівневого управління та координації між рівнями влади і стейкхолдерами	Наявність спільних координаційних органів; регулярність вертикальних і горизонтальних нарад; формалізовані процедури взаємодії	15–20
Фінансово-ресурсна	Забезпеченість місцевого рівня ресурсами для виконання переданих повноважень	Частка власних доходів місцевих бюджетів; гнучкість фінансових інструментів; доступ громад до державних і донорських програм	15–20
Соціально-капітальна	Рівень довіри, самоорганізації та участі громадян і спільнот у вирішенні суспільних завдань	Участь у громадських слуханнях і місцевих ініціативах; індекси соціальної довіри; кількість активних ГО та ініціативних груп	15–20
Цифрово-інформаційна	Розвиненість цифрових інструментів участі, прозорості та доступу до даних для місцевих акторів	Доступ громад до відкритих даних; наявність локальних цифрових платформ; рівень використання е-сервісів та електронних консультацій	10–15
Безпеково-громадська	Залучення громад, волонтерських та місцевих структур до забезпечення безпеки, реагування та відновлення	Кількість місцевих планів цивільного захисту; участь волонтерів у кризових ситуаціях; готовність громад до самоорганізації під час загроз	10–15

Джерело: розроблено автором

Для аналітичного опису реалізації принципу субсидіарності в НМС доцільно виокремити кілька узагальнених компонент, які відображають різні аспекти розподіленого управління стійкістю: інституційно-правовий,

У вимірі цифрового суспільства окремого значення набуває цифрово-інформаційна компонента, адже без доступу до актуальних даних, без навігації у потоках інформації й без електронних каналів зворотного зв'язку реалізація субсидіарності суттєво обмежена (О.Ахмедова) [203]. Цифрова платформа формування та розвитку НМС у такому разі має слугувати не лише інструментом централізованого збору даних, а середовищем для локальної участі, спільного моделювання ризиків та узгодження рішень. Перехід від ієрархічної моделі управління до моделі, заснованої на субсидіарності й розподіленій відповідальності, змінює характер роботи всіх ключових секторів: від безпеки й оборони до соціальної політики, економіки, просторового розвитку та цифрової трансформації

У розширеному форматі (з позицій ефективності) принцип субсидіарності та розподіленої відповідальності в національній моделі стійкості означає, що рішення ухвалюються й реалізуються на тому рівні, де це дає найбільший ефект для стійкості держави й суспільства в цілому, з урахуванням наявності наднаціональних механізмів управління. Йдеться не лише про пріоритет «найнижчого спроможного рівня», а про функціонально обґрунтований вибір між наднаціональним, національним, регіональним, місцевим, організаційним рівнями та рівнем домогосподарств і громадян. Критеріями такого вибору виступають відповідність завдання повноваженням відповідного рівня, наявність організаційної та кадрової спроможності, достатність ресурсів, доступ до релевантних даних, знання локального і транскордонного контексту, швидкість реагування, масштаби зовнішніх ефектів (у тому числі міждержавних), а також легітимність і довіра до суб'єкта, що ухвалює рішення.

У такій інтерпретації субсидіарність перестає бути жорстким правилом «максимального делегування повноважень вниз» і перетворюється на динамічний механізм розміщення завдань у тій точці багаторівневої системи, де поєднання спроможності, інформаційної забезпеченості та контекстуальної обізнаності забезпечує найкращий результат. Стратегічні

рішення, що визначають загальні рамки національної стійкості, стандарти безпеки, базову архітектуру критичної інфраструктури, як правило, залишаються на національному рівні, оскільки вимагають загальнодержавного бачення, узгодженості політик і врахування зовнішньополітичного виміру. Водночас частина таких рішень дедалі частіше «піднімається» на наднаціональний рівень – там, де мова йде про транскордонні загрози (кліматичні зміни, енергетична безпека, кібербезпека, міграційні потоки, спільна оборона), спільні ринки, інтегровані транспортні коридори, наднаціональні стандарти кризового реагування та спільні інфраструктурні проекти. У таких випадках ефективність досягається саме завдяки координації, солідарному розподілу ресурсів і виробленню спільних правил на рівні союзів, альянсів чи інтеграційних об'єднань.

Натомість рішення, пов'язані з організацією повсякденної життєдіяльності, локальної безпеки, соціальної підтримки вразливих груп, розвитку місцевої економіки та інфраструктури, ефективніше ухвалювати та реалізовувати на рівні громад, організацій і локальних спільнот, де є безпосереднє знання території, населення та специфіки ризиків. Регіональний рівень відіграє роль проміжної ланки, що інтегрує міжмуніципальні ресурси, вирішує питання, які виходять за межі однієї громади, але не потребують безпосереднього втручання держави чи наднаціональних структур (наприклад, регіональна логістика, просторове планування, координація медицини та освіти). Організаційний рівень (бізнес, установи, інфраструктурні оператори) забезпечує операційну стійкість у конкретних секторах, тоді як домогосподарства та громадяни є останньою лінією адаптації, самоорганізації та самозахисту.

Наднаціональний рівень у цій архітектурі не «дискримінує» національний чи локальний рівні управління, а доповнює їх там, де характер загроз і викликів об'єктивно перевищує можливості окремої держави. Наднаціональні інституції можуть ефективніше координувати відповіді на системні кризи (масштабні війни, регіональні конфлікти, пандемії, глобальні

фінансові шоки), формувати спільні стандарти та режими обміну даними, інвестувати в інфраструктуру, що перетинає кордони, розробляти рамкові політики, у межах яких національні та місцеві рівні вже конкретизують власні рішення. Передача частини управлінських повноважень на наднаціональний рівень у цьому випадку не є втратою суверенітету, а радше його функціональною модернізацією: держава делегує частину рішень туди, де вони можуть бути реалізовані ефективніше й забезпечити вищий рівень стійкості для всього об'єднання, зберігаючи при цьому контроль над виконанням, імплементацією і адаптацією до національного контексту.

Умовою реалізації такого «спроможно-інституціонального» розуміння субсидіарності, розширеного до наднаціонального виміру, є наявність публічноуправлінського механізму, який дозволяє не інтуїтивно, а даноорієнтовано оцінювати, на якому рівні те чи інше рішення буде найрезультативнішим. Цю функцію в умовах цифрового суспільства бере на себе цифрова управлінська платформа формування та розвитку НМС, інтегрована з наднаціональними просторами даних і спільними інформаційними системами. Така платформа акумулює інформацію про спроможності кожного рівня (кадрові, фінансові, інституційні, технічні), про якість виконання завдань у минулому, про навантаження на різні ланки системи, а також про територіальний, міжрегіональний і транскордонний контекст. На основі таких даних стає можливим регулярно переоцінювати розподіл повноважень як усередині держави, так і між національним і наднаціональним рівнями: посилювати роль тих рівнів, які демонструють високу результативність, і водночас ідентифікувати ділянки, де потрібні додаткові ресурси, навчання, інституційна підтримка чи, навпаки, тимчасова централізація в наднаціональних структурах.

Цифрова управлінська платформа виконує не лише функцію технічної інфраструктури, а й роль простору спільного моделювання та координації рішень між усіма рівнями – від наднаціонального до локального. Вона дозволяє різним суб'єктам управління бачити загальну «картину стійкості»,

оцінювати, як рішення в одній сфері або на одній території впливають на інші, будувати сценарії розвитку подій, формувати узгоджені відповіді на загрози, які часто мають транскордонний характер. Через неї наднаціональні стратегії, директиви, стандарти та спільні цілі «перекладаються» на мову конкретних національних і локальних завдань, а зворотний потік даних знизу догори – від громад і національних урядів до наднаціональних органів – дозволяє коригувати політики, уникати «сліпих зон» і зменшувати ризик того, що наднаціональні рішення відірвуться від реальної ситуації на місцях.

Водночас, авторська інтерпретація субсидіарності через призму «найбільш ефективного рівня управління» (В.Гройман, В.Роман) [204-205] з урахуванням наднаціонального виміру несе в собі й додаткові ризики. Адже під її «прикриттям» може відбуватися як легітимація надмірної централізації в руках національних урядів (при цьому вітчизняний парадокс – «реформа децентралізації» фактично приводить до побудови централізованого механізму управління), так і надмірної «зовнішньої» централізації на рівні інтеграційних об'єднань, коли ключові рішення віддаляються від громадян і локальних спільнот. Протилежна ситуація – коли національним і місцевим рівням формально передаються численні завдання в рамках наднаціональних політик, але без належної фінансової, технічної та регуляторної підтримки, що породжує «квазі-субсидіарність як «вгору», так і «вниз» і підриває довіру як до держави, так і до наднаціональних інститутів. Додатково зростає ризик фрагментації політик, коли різні рівні, керуючись власними уявленнями про «ефективність», приймають несумісні рішення без достатньої координації, а також проблема асиметрії інформації та спроможностей між локальними, національними й наднаціональними акторами.

Щоб мінімізувати ці ризики, принцип субсидіарності в контексті нашої інтерпретації «найбільш ефективного рівня» має бути чітко інституалізований як у національній, так і в наднаціональній архітектурі управління. Це означає фіксацію прозорих критеріїв визначення ефективного рівня для різних типів рішень, створення постійно діючих міжрівневих

механізмів координації та консультацій (у тому числі міждержавних), запровадження правил, за якими передача завдань завжди супроводжується відповідним перерозподілом ресурсів, повноважень і відповідальності, а також забезпечення цифрової прозорості розподілу функцій і результатів. Важливо, щоб було зрозуміло, які саме завдання доцільно й легітимно розміщувати на наднаціональному рівні, які – залишати в компетенції держави, а які – максимально передавати регіонам, громадам та організаціям, і щоб цей розподіл регулярно переглядався на основі емпіричних даних і досвіду кризового реагування. Факти ми інтегруємо зміст національних механізмів стійкості і формат європейського врядування. При цьому важливо зазначити, що таке поєднання є доцільним з урахуванням низки принципів-концептів

- 1) імплементації основ європейського врядування в національну практику [206];
- 2) розподілу повноважень між національними державами і інститутами ЄС (принцип наднаціоналізму)[207];
- 3) принципу спільного формування європейської політики (певною мірою – міжурядовість) [208];
- 4) стійкості до викликів, визначених членством в ЄС [209];
- 5) субтериторіальності управління [210].

Таким чином, у поглибленому ефективнісному розумінні, доповненому наднаціональним виміром, принцип субсидіарності та розподіленої відповідальності формує для НМС рамку, в якій повноваження, ресурси й задачі не просто «спускаються вниз» або «концентруються в центрі» (національному чи наднаціональному), а гнучко розміщуються в тій точці багаторівневої системи, де забезпечують найвищий результат для національної та спільної (наднаціональної) стійкості. Цей результат досягається не завдяки домінуванню якогось одного рівня, а завдяки координованій взаємодії всіх рівнів, підтриманій цифровими інструментами, прозорими правилами гри й постійним аналізом даних. У підсумку

субсидіарність перестає бути абстрактним політичним гаслом і набуває рис практичного механізму оптимізації рішень у складній, динамічній та мережевій системі забезпечення стійкості, в якій наднаціональний, національний і субнаціональні рівні взаємно підсилюють один одного.

4. *Принцип динамічної адаптації та проактивності.* Загалом, справжня стійкість – не просто здатність системи відновлювати характеристики до попереднього стану після кризи, а здатність адаптуватися до змін та навіть випереджати їх завдяки трансформаціям системи управління. Отже, публічна політика має бути націлена на проактивне передбачення ризиків через стратегічне прогнозування, сценарне планування, регулярні навчання та стрес-тести. Такий підхід вимагає рішучості змінювати застарілі елементи системи, перебудовувати організацію суспільства задля підготовки до нових загроз. Причому ключовими стають інвестиції в інженерні, соціальні, економічні та освітні інновації.

Принцип динамічної адаптації та проактивності переорієнтовує НМС – від уявлення про стійкість як «повернення до норми» після удару до розуміння її як здатності системи постійно змінюватися, навчатися й випереджати загрози. У традиційному підході стійкість часто ототожнюється зі здатністю відновити попередній стан після кризи, мінімізувати збитки й повернутися до «звичного функціонування». Натомість у динамічній логіці стійкість означає, що суспільство й держава не просто витримують удари, а використовують кризи та пов'язані з ними навчальні ефекти як імпульс до трансформацій: оновлюють інститути; змінюють структуру економіки; удосконалюють просторову організацію, управлінські практики, цифрову інфраструктуру, моделі освіти й соціальних відносин. Така стійкість є не ретроспективною (орієнтованою на відновлення минулого), а перспективною (орієнтованою на готовність до майбутнього, яке, ймовірно, не буде повторенням минулих станів).

Ключовим елементом цього принципу є відмова від реактивної логіки «управління кризами» на користь проактивної логіки передбачення,

попередження й підготовки. Політика стійкості має спиратися на систематичне стратегічне прогнозування, сценарне планування, регулярні навчання та стрес-тести, які моделюють як імовірні, так і малоімовірні, але високоризикові події.

Принцип динамічної адаптації прямо пов'язаний із готовністю до трансформацій, тобто з відмовою від консервації застарілих елементів системи управління заради уявної стабільності, і вимагає політичної й управлінської рішучості переглядати структури, що більше не відповідають новим умовам: змінювати моделі управління, перерозподіляти повноваження, реформувати сектори, які стали джерелом системних ризиків, відмовлятися від неефективних інституційних компромісів. Важливо, що динамічна адаптація включає також перегляд ціннісних, культурних та організаційних установок, наприклад, переосмислення ставлення до ризику, помилки й невдачі як до невід'ємної частини навчання, а не як до приводу для покарання й згортання ініціатив. В умовах цифрового суспільства проактивність і динамічна адаптація базуються на розвитку потужної аналітики даних, систем раннього виявлення ризиків, інструментів моделювання й віртуального тестування рішень. Цифрова платформа НМС у такій логіці не лише збирає інформацію про події, що вже відбулися, а й дає змогу виявляти тренди, аномалії, кореляції, які свідчать про потенційні загрози. Таким чином, цифровий вимір не лише підсилює здатність системи до адаптації, а й робить можливим перехід від реактивних дій до випереджувального планування.

Принцип динамічної адаптації та проактивності пов'язаний з інноваційним виміром стійкості [211]. Адже інвестиції в інженерні, соціальні, економічні та освітні інновації стають не другорядним напрямом, а одним із головних інструментів підготовки до майбутніх криз [212]. Інженерні інновації забезпечують модернізацію інфраструктури, що здатна витримувати нові види навантажень, включно з комбінованими фізичними й кіберзагрозами. Соціальні інновації створюють нові форми солідарності,

взаємодії, локальної самоорганізації. Економічні інновації пов'язані з розвитком гнучких, диверсифікованих моделей виробництва й постачання, які знижують залежність від критичної інфраструктури (таблиця 2.6).

Таблиця 2.6

Ключові компоненти реалізації принципу динамічної адаптації та проактивності в НМС

Аналітичний вимір принципу	Теоретичний зміст (resilience, governance, policy studies)	Операціоналізація в контексті НМС	Приклади методів та інструментів	Очікуваний ефект для стійкості
1	2	3	4	5
Розуміння стійкості (тип резильєнтності)	Перехід від «інженерної» стійкості (повернення до попереднього стану) до адаптивної і трансформаційної резильєнтності; орієнтація не на відновлення статус-кво, а на зміну конфігурації системи у нових умовах	Визнання в стратегіях НМС пріоритету адаптації й трансформації над відновленням попередньої моделі; включення цілей структурних змін (інститутів, інфраструктури, моделей управління) у політику стійкості	Рамки типу adaptive/transformational resilience; посткризові «lessons learned» з обов'язковим переглядом інституцій і політик, а не лише планів реагування	Зменшення вразливості до повторюваних і нових типів загроз; перетворення криз на драйвери модернізації НМС
Часова орієнтація (проактивність vs реактивність)	Зміщення акценту з ретроспективної логіки («усунення наслідків минулих криз») до проспективної логіки (управління майбутніми ризиками, невизначеністю та можливостями)	Інституціоналізація циклів стратегічного прогнозування й сценарного аналізу; закріплення процедур регулярного перегляду політик з урахуванням нових трендів та «слабких сигналів»	Стратегічне форсайт-прогнозування; horizon scanning; регулярні національні огляди ризиків; сценарні сесії з міжсекторальною участю	Підвищення здатності НМС «бачити наперед» та готуватися до криз, які ще не мають прецедентів у національному досвіді
Тип управління ризиками (anticipatory governance)	Перехід від reactive risk management до anticipatory governance: управління ризиками до їх матеріалізації, робота з глибинною невизначеністю, включно з low probability – high impact подіями	Створення постійно діючих міжвідомчих структур з передбачення ризиків; закріплення в законодавстві вимоги оцінки стійкості та довгострокових ризиків для політик	Регулярні stress-testing політик, інфраструктур і фінансових систем; prospective impact assessment; аналіз «чорних лебедів» і «сірих носорогів»	Зниження ймовірності системних провалів; підвищення живучості критичних функцій держави й суспільства
Механізми інституційної зміни (path-dependency vs трансформація)	Подолання path dependency (інституційної інерції, залежності від попередньої траєкторії) через керовані трансформації; стійкість як здатність до зміни, а не до консервації	Запровадження механізмів регулярної ревізії інститутів і політик (sunset-клаузули, рев'ю через визначені інтервали); створення простору для експериментів, пілотних проєктів, регуляторних «пісочниць»	Policy review cycles; institutional audits; регуляторні пісочниці в чутливих секторах (енергетика, фінанси, цифрова інфраструктура); експериментальне впровадження нових моделей управління	Здатність НМС своєчасно позбуватися застарілих, вразливих або неефективних елементів; підвищення адаптивності інституцій

Продовження таблиці 2.6

1	2	3	4	5
Роль інновацій (інженерні, соціальні, економічні, освітні)	Інновації розглядаються не як окремий сектор, а як системна умова адаптації; зміщення акценту від «латання» до створення нових соціотехнічних конфігурацій	Інтеграція виміру стійкості в інноваційну та науково-технічну політику; пріоритизація R&D, спрямованих на зниження вразливості й підвищення адаптивної спроможності	Програми підтримки deep-tech для критичної інфраструктури; соціальні інновації в громадах; економічні моделі з високою диверсифікацією; освітні програми з компетенцій резильєнтності	Формування технологічної, соціальної та когнітивної бази для швидкої перебудови систем у разі змін середовища
Цифровий вимір і дата-орієнтованість	Перехід від «цифрової архівації» (реєстрація пост-фактум) до data-driven resilience, коли дані використовуються для раннього виявлення, моделювання й адаптації	Побудова цифрової платформи НМС як інтегрованої системи даних і моделей; забезпечення інтероперабельності між секторами (безпека, економіка, енергетика, демографія тощо)	Системи раннього попередження; предиктивна аналітика; моделювання сценаріїв за допомогою ІІ; цифрові двійники (digital twins) для критичних систем і територій	Підвищення точності й швидкості прийняття рішень; можливість тестувати альтернативи до їхнього впровадження в реальності
Культура навчання з криз (learning system)	Перехід від single-loop learning («усунення окремих помилок») до double-/triple-loop learning (переосмислення цілей, припущень, інституційних рамок)	Закріплення обов'язкових post-crisis reviews; формування інституційної «пам'яті криз»; прив'язка уроків до змін у політиках, інституційному дизайні та навчальних програмах	Посткризові комісії з мандатом на рекомендації щодо реформ; репозиторії lessons learned; включення кейсів криз у підготовку держслужбовців, військових, рятувальників, управлінців	Здатність НМС еволюціонувати після кожної великої кризи, підвищуючи свою адаптивність і зменшуючи ймовірність повторення тих самих провалів

Джерело: розроблено автором

Застосований до національної моделі стійкості, цей принцип означає, що НМС будується не як раз і назавжди зафіксована конструкція, а як еволюційна система, здатна до самокорекції [213]. Структура інститутів, розподіл повноважень між рівнями управління, архітектура цифрових платформ і процедур не розглядаються як незмінні, натомість закладаються механізми їхнього регулярного перегляду й оновлення на основі зворотного зв'язку, даних моніторингу й уроків криз. У такій системі кожна велика криза – війна, пандемія, енергетичний шок, кліматичні катастрофи, масова міграція – стає не лише випробуванням, а й джерелом знань, яке інституційно перетворюється на зміни в законодавстві, інфраструктурі, освіті, управлінських практиках.

Проте реалізація принципу динамічної адаптації та проактивності стикається з потужним опором інерції інститутів, політичного процесу та суспільних очікувань. Схильність до відновлення «як було» часто сильніша за готовність визнати, що частина попередніх структур і практик була джерелом уразливості. Тому важливо інституціонально закріплювати вимогу до періодичного перегляду політик (через sunset-клаузули, ревізії, обов'язкові оцінки впливу й стійкості) [214], стимулювати культуру навчання з криз, підтримувати політичні й громадські середовища, здатні просувати непопулярні, але необхідні трансформації.

Цифрова платформа НМС у цьому контексті має працювати не лише як технологічний інструмент, а й як елемент «пам'яті системи», що акумулює дані про минулі події, зафіксовані рішення, їх наслідки й отримані власні висновки, та робить цю пам'ять доступною для прийняття нових рішень. Отже, принцип динамічної адаптації та проактивності перетворює стійкість із захисної категорії на категорію розвитку системи державного управління. Цей принцип вимагає, щоб держава, суспільство, економіка й інститути не лише витримували удари, а й системно готувалися до майбутніх змін, приймаючи невизначеність як нормальний стан і джерело можливостей. За такого підходу національна модель стійкості постає як постійно навчальна, інноваційна, цифрово підтримана система, здатна не лише адаптуватися до нових загроз, а й випереджати їх за рахунок гнучкості, передбачення та цілеспрямованих трансформацій.

5. *Принцип redundancy (системної надлишковості) та децентралізації* [215] в контексті національної моделі стійкості (НМС) відображає перехід від уявлень про «оптимізовану», мінімалістичну й жорстко централізовану систему до розуміння стійкості як властивості розподілених, мережових та модульних конфігурацій, у яких свідомо закладені резерви, дублювання та альтернативні траєкторії функціонування. На відміну від класичних підходів, орієнтованих на максимізацію ефективності (мінімізація витрат, уникнення «зайвих» потужностей), у концепті резильєнтності надлишковість

розглядається як структурний ресурс системи, що забезпечує збереження критичних функцій в умовах шоків, цілеспрямованих атак та каскадних відмов (за А.Гелмріх та інш.) [215].

У теоретичному вимірі йдеться про свідоме уникнення «точок єдиної відмови» (single points of failure) шляхом побудови архітектури системи державного управління, у якій жоден окремий вузол, канал чи інституція не є абсолютно незамінними. Ключові функції розподіляються між множиною елементів, що перебувають у відносинах часткової взаємозамінності, а потоки ресурсів, інформації та управлінських рішень можуть бути оперативно перенаправлені альтернативними маршрутами. Така архітектура наближає НМС до характеристик складних адаптивних систем, у яких стійкість досягається не через жорстку ієрархізацію, а через мережевість, поліцентричність і модульність.

Надлишковість (redundancy) у цьому контексті має щонайменше три взаємопов'язані виміри. По-перше, це інфраструктурна надлишковість: наявність дублюючих систем, резервних потужностей і паралельних ліній для виконання критичних функцій (енергопостачання, зв'язок, транспорт, водопостачання, дата-центри, об'єкти управління). Йдеться про створення додаткових генеруючих і розподільчих потужностей, альтернативних маршрутів постачання, резервних центрів обробки даних, дублюючих командно-диспетчерських пунктів, здатних перехопити навантаження у разі ушкодження або перевантаження основних елементів. По-друге, це ресурсна надлишковість, що передбачає стратегічне резервування критично важливих матеріальних, фінансових, кадрових та інформаційних ресурсів. Формування запасів палива, продовольства, медикаментів, резервних фінансових інструментів, «банків компетентностей» та корпусу резервістів створює можливість підтримувати базову життєдіяльність та керованість навіть за тривалого порушення звичних товарних і фінансових потоків. По-третє, це комунікаційна надлишковість, пов'язана з підтримкою множинності незалежних або слабо корельованих каналів зв'язку й передачі даних.

Критичні суб'єкти управління повинні мати доступ до кількох технологічно диференційованих каналів – мобільних і фіксованих мереж, супутникового зв'язку, захищених урядових мереж, автономних радіосистем, локальних офлайн- та mesh-мереж на рівні громад. Така конфігурація мінімізує ризик втрати керованості, координації та інформованості внаслідок ушкодження чи компрометації окремих сегментів комунікаційної інфраструктури.

Принцип децентралізації доповнює надлишковість, переводить її із суто техніко-інфраструктурної площини в інституційно-управлінський і територіальний виміри. У рамках теорій багаторівневого та поліцентричного врядування це означає відмову від конфігурації, де управлінські повноваження, ресурси й компетенції концентруються в єдиному «центрі», на користь розподілу цих спроможностей між кількома рівнями та типами акторів – центральними органами влади, регіональними структурами, органами місцевого самоврядування, приватними операторами, інституціями громадянського суспільства. Децентралізація в цьому розумінні не зводиться до формального перерозподілу повноважень; вона передбачає одночасне укорінення на субнаціональних рівнях реальних ресурсів, операційних спроможностей і легітимованого права на автономне (у визначених межах) ухвалення рішень.

У практичному вимірі це втілюється у локалізації систем реагування й розвитку модульних регіональних та муніципальних підсистем НМС. Регіональні хаби (логістичні, медичні, гуманітарні, інформаційні) та муніципальні центри управління кризами виконують функції проміжних вузлів, здатних як отримувати підтримку від національного рівня, так і діяти автономно у разі порушення вертикальних зв'язків. Локальні служби (комунальні підприємства, лікарні, рятувальні й добровольчі формування, мережі взаємодопомоги) формують «останню лінію» стійкості, що забезпечує базову життєдіяльність населення навіть за часткової втрати функціональності центральних інститутів. У цьому сенсі децентралізація створює інституційну надлишковість, коли певні управлінські, координаційні

та логістичні функції можуть бути дубльовані або тимчасово перебрані іншими рівнями у випадку їхнього випадіння на одному з рівнів.

Ключовим операційним виміром принципу надлишковості та децентралізації є диверсифікація джерел і постачальників як механізм зниження структурної вразливості до зовнішніх і внутрішніх впливів, про що вказує як О.Резнікова [95], так і [216]. Фактично, побудова стійкості спирається на поєднання *розподілених* та *резервних* (backup) енергетичних систем, багаторівневе планування й децентралізоване управління інфраструктурою. Адже саме надлишковість та розосередженість функцій зменшують ризик єдиної точки відмови в національних системах життєзабезпечення. Ідеться про формування портфеля енергетичних, логістичних, фінансових та інформаційних рішень, у межах якого жодне окреме джерело чи маршрут не є критично незамінним. Поєднання традиційних і відновлюваних джерел енергії, декількох маршрутів імпорту та експорту, розширеного кола постачальників критичних товарів і послуг, різних технологічних платформ для виконання схожих функцій дозволяє запроваджувати режими керованої деградації (controlled degradation). У таких режимах зниження рівня надання певних сервісів у кризових умовах відбувається не хаотично, а за заздалегідь визначеними ієрархіями критичності, коли найбільш важливі функції захищаються за рахунок надлишковості та перенаправлення ресурсів.

Нарешті, надлишковість та децентралізація мають кадрово-інституційний вимір: мова про наявність резервних управлінських команд, механізмів крос-підготовки персоналу, взаємозамінності ключових посад і «дублюючих» організаційних структур. Формування корпусу резервістів, розвиток міжінституційних мереж практиків, створення координаційних штабів і механізмів підтримки між установами дозволяє зберігати виконання критичних функцій навіть за втрати окремих органів влади чи професійних груп [216]. Функціональна системна надлишковість забезпечує гнучкий перерозподіл ролей і завдань між суб'єктами в умовах кризи (таблиця 2.7).

Таблиця 2.7

Аналітична структура принципу надлишковості та децентралізації в НМС

Аналітичний вимір принципу	Теоретичний зміст (resilience, systems, governance)	Операціоналізація в контексті НМС	Приклади методів та інструментів	Очікуваний ефект для стійкості
Архітектура без “single point of failure”	Перехід від монолітних, централізованих конфігурацій до мережових і модульних систем; відсутність вузлів, відмова яких паралізує систему	Проектування критичних функцій як мережі взаємопов’язаних вузлів із можливістю маршрутизації потоків через альтернативні шляхи	Мережева архітектура енергосистем, ІКТ і транспорту; кластеризація критичних об’єктів; дублюючі центри управління	Збереження базового функціонування навіть за масштабних ушкоджень окремих елементів
Інфраструктурна надлишковість	Системна наявність дублюючих потужностей і паралельних ліній для виконання критичних інфраструктурних функцій	Визначення “критичних функцій” та встановлення мінімально необхідного рівня дублювання для кожної з них	Резервні лінії електропередач; альтернативні траси водопостачання й транспорту; дубль-ЦОДи; резервні командні пункти	Підвищена живучість критичної інфраструктури; скорочення часу відновлення внаслідок пошкоджень
Ресурсна надлишков. і диверсифікація постачання	Підтримка системних резервів та портфеля альтернативних джерел для ключових ресурсів	Створення стратегічних запасів (паливо, продовольство, медикаменти), диверсифікація постачальників і маршрутів постачання	Державні резерви; договори з кількома постачальниками; мульти-маршрутна логістика; локальні склади і виробництва	Зменшення залежності від окремих ринків і контрагентів; стійкість до блокад, санкцій, руйнування інфраструктури
Комунікаційна надлишковість	Комунікаційна резильєнтність через множинність каналів зв’язку, частково незалежних технологічно й організаційно	Паралельний розвиток мобільних, фіксованих, супутникових, радіо- та локальних мереж	Захищені урядові мережі; супутниковий і радіозв’язок; mesh-мережі на рівні громад; локальні дата-сервери	Збереження керованості, координації та оповіщення за втрати телеком-інфраструктури
Децентралізація повноважень і спроможностей	Поліцентричне врядування: розподіл управлінських функцій і ресурсів між рівнями (нац., регіон, громада) й акторами	Інституційне закріплення компетенцій місцевого рівня у сферах безпеки, цивільного захисту, базових сервісів; фінансова децентралізація	Муніципальні й регіональні центри управління кризами; локальні плани стійкості; механізми прямого фінансування громад	Підвищення швидкості й релевантності реагування; зменшення навантаження й вразливості
Інституційна та кадрова надлишков.	Функціональна надлишковість у сфері інститутів і людського капіталу: можливість перерозподілу ролей	Підготовка резервних управлінських команд; крос-тренінг персоналу; взаємозамінність компетентностей	Резервістські програми; угоди про взаємну підтримку між установами; координаційні штаби	Здатність підтримувати безперервність управління й сервісів за втрати окремих органів
Керована деградація (controlled degradation) та пріоритизація	Концепція, за якої в кризі не всі функції зберігаються, але критичні – захищені redundancy і пріоритизацією ресурсів	Розробка матриць критичності послуг; протоколів відключення/обмеження менш критичних сервісів на користь базових	Сценарії керованого відключення; алгоритми пріоритетного забезпечення лікарень, силових структур, об’єктів КІ	Запобігання неконтрольованом у колапсу системи; концентрація ресурсів на підтримці життєво важливих функцій

Джерело: дослідження автора

Отже, принцип надлишковості та децентралізації задає для НМС специфічну архітектурну та інституційну логіку, у межах якої пріоритет надається не максимізації короткострокової ефективності, а підвищенню живучості, відновлюваності та адаптивності критичних функцій. Створення дублюючих систем, резервних потужностей, розподіленої інфраструктури, диверсифікованих джерел і локальних систем реагування в поєднанні з поліцентричним розподілом повноважень і спроможностей не лише мінімізує ризики «точок єдиної відмови», а й формує основу для збереження мінімально необхідного рівня функціонування та подальшої адаптації й трансформації системи в умовах глибоких криз.

Досліджені у дисертації принципи формування національної моделі стійкості у форматі цифрового суспільства фіксують глибинну трансформацію самої онтології державного управління. Національна стійкість більше не мислиться як властивість окремих інститутів чи секторів, а постає емерджентною характеристикою складної, мережевої, багаторівневої системи, в якій перехрещуються економічні, соціальні, політичні, екологічні, безпекові та цифрово-інформаційні виміри. У такій логіці державне управління зміщується від фрагментованих, ієрархічних та реактивних підходів до інтегрованого, поліцентричного й датаорієнтованого врядування, заснованого на цілісності, субсидіарності, динамічній адаптації, redundancy та децентралізації. Для науки державного управління це означає перехід від опису формальних інституцій до аналізу мережових конфігурацій, механізмів багаторівневої координації, цифрових платформ і режимів керованої трансформації. Відповідно, оновлюється понятійний апарат, розширюється методологія (системний аналіз, моделювання складних систем, foresight, data-driven policy), а сама резильєнтність стає центральною категорією теорії публічного управління в умовах невизначеності та гібридних загроз.

2.3. Формування методології національного розвитку на основі цифровізації в умовах правового режиму воєнного стану: актуалізація НМС

Збройна агресія РФ проти України в межах дослідницької методології національної моделі стійкості постає не лише як стрес-тест для системи державного управління, а як критичний чинник, що оголює структурні вразливості державної організації та змушує до глибокого перегляду базових засад публічноуправлінської діяльності. Правовий режим воєнного стану (ПРВС), встановлений, зокрема, 24 лютого 2022 року відповідно до Закону України «Про правовий режим воєнного стану» 2015 року, з урахуванням законів України «Про Збройні Сили України», «Про оборону України», «Про національну безпеку України», визначає особливу конфігурацію повноважень, відповідальності та взаємодії між органами влади. У координатах національної моделі стійкості це означає перехід від умовно «мирної» моделі публічного управління до режиму інтегрованого цивільно-військового управління, де кожне інституційне рішення прямо впливає на здатність держави зберігати керованість, функціональну цілісність і здатність до відновлення. За таких обставин утверджується інтегрована модель, у якій цивільне та військове управління формально поєднані, проте на практиці співіснують у напруженому полі між необхідністю максимальної централізації для ведення війни та потребою зберегти простір для демократичного самоврядування, ініціативності громад і гнучких локальних рішень.

В умовах повномасштабної війни національна стійкість виявляється не як абстрактна характеристика, а як здатність цієї складної, багаторівневої системи публічної влади витримувати удар, не руйнуючи базові інститути та одночасно перерозподіляючи функції так, щоб зберігати дієздатність як на центральному, так і на регіональному та локальному рівнях. У такій перспективі архітектура державного управління, що функціонує в умовах ПРВС, розглядається як ключовий вимір національної моделі стійкості, але

водночас і як джерело додаткових ризиків. На національному рівні вибудовується моноцентричне ядро, де концентруються політичне, воєнне й безпекове керівництво: інститут Президента України поєднує статус глави держави, Верховного Головнокомандувача Збройних Сил України, голови Ради національної безпеки і оборони, очільника Воєнного кабінету при РНБО. Така концентрація ухвалення рішень з погляду стійкості має подвійний ефект: з одного боку, посилює здатність до швидкого реагування, синхронізації дій силових структур, органів виконавчої влади та сектора оборони; з іншого – підвищує чутливість усієї системи до політичних, організаційних або комунікаційних збоїв у центрі. Поруч із цим у національному контурі залишаються Верховна Рада України, органи системи правосуддя, Кабінет Міністрів України, центральні органи виконавчої влади, органи спеціальної компетенції, Генеральний штаб Збройних Сил України, Головнокомандувач ЗСУ та самі Збройні Сили України, політичні партії й громадські об'єднання. Вони формують складну мережу розподілу повноважень, у якій будь-які розриви координації, конкуренція юрисдикцій або надмірна фрагментація рішень безпосередньо позначаються на стійкості: можуть уповільнювати реагування, посилювати правову невизначеність, знижувати рівень суспільної довіри.

Проблематика реалізації концепту національної стійкості особливо загострюється на регіональному й локальному рівнях, де інтегрована цивільно-військова модель набуває конкретних організаційних форм. Обласні військові адміністрації, районні військові адміністрації, територіальні органи центральних органів виконавчої влади, територіальні органи правоохоронних та інших державних органів спеціальної компетенції, а також органи місцевого самоврядування регіонального та субрегіонального рівня (обласні й районні ради) формально мають діяти як взаємопов'язані елементи єдиної вертикалі управління. Однак у координатах НМС актуалізується низка дилем: як поєднати єдність командування й необхідність врахування специфіки адміністрування конкретних територій;

як забезпечити субсидіарний розподіл повноважень так, щоб громади не перетворювалися на пасивних виконавців рішень «згори», але й не створювали паралельних центрів влади в умовах воєнного стану; як зберегти кадровий, експертний і фінансовий потенціал на місцях, коли частина функцій значною мірою централізується у військових адміністраціях. На локальному рівні – рівні військових адміністрацій населених пунктів і базового місцевого самоврядування – ці питання постають ще гостріше, адже саме тут стикаються вимоги безпеки, потреба в оперативних, часто жорстких управлінських рішеннях і очікування громадян щодо участі, прозорості та збереження базових соціальних стандартів. Здатність локального рівня адаптувати національні рішення до реальних умов, не руйнуючи довіру до держави, є однією з центральних передумов національної стійкості й водночас одним із найвразливіших її сегментів.

Багаторівнева функціональна моноцентрична модель публічного управління, що формується на основі наведених законів, у дослідницькій логіці національної моделі стійкості розглядається як «архітектура ризику й захисту» одночасно. Закладені у Конституції України і законах України принципи централізації, децентралізації, концентрації, деконцентрації та субсидіарності мають забезпечувати баланс між єдиним стратегічним керівництвом і розподілом відповідальності по рівнях. Однак у реальних умовах війни ці принципи проявляються нерівномірно: в окремих сферах спостерігається надмірна концентрація повноважень без достатньої компенсації механізмами підзвітності та участі; в інших – навпаки, надмірна деконцентрація без належних координаційних інструментів. Для національної стійкості це означає, що інтегрована цивільно-військова модель державного управління виступає одночасно і ресурсом, і викликом: ресурсом – оскільки забезпечує швидке прийняття й реалізацію рішень в умовах загрози, викликом – оскільки кожен дисбаланс між рівнями чи компонентами системи прямо трансформується у додаткові вразливості. Саме тому в межах дослідницької методології НМС ключовим завданням стає не лише фіксація

формальних контурів цивільної й військової влади, а й аналіз того, як ця багаторівнева, моноцентрично організована система реально працює під час війни: де посилює спроможність до опору та відновлення, а де створює загрози надмірної концентрації, інституційних розривів або втрати довіри, що безпосередньо впливає на національну стійкість як цілісну характеристику держави.

Воєнний стан є одним із найбільш критичних періодів для будь-якої держави, оскільки він супроводжується значними потрясіннями у всіх сферах суспільного життя: економіці, державному управлінні, соціальному захисті та безпеці. У таких умовах особливої важливості набуває пошук інноваційних підходів до забезпечення стійкості національного розвитку, адаптації ключових процесів до надзвичайних обставин і збереження стратегічних ресурсів. Одним із найбільш ефективних інструментів, що сприяє розв'язанню цих завдань, є цифровізація. Використання цифрових технологій дозволяє не лише оперативно реагувати на кризові виклики, але й закладати основу для подальшого відновлення та розвитку. Цифрові рішення забезпечують збереження функціонування державних інститутів, підтримку економіки, доступ громадян до соціальних послуг, а також ефективне управління ресурсами в умовах обмеженого часу та ресурсів. В умовах правового режиму воєнного стану Україна зіткнулася з унікальними викликами, які потребують інноваційних підходів до організації управління та забезпечення стабільності. Цифрові інструменти стають фундаментом для розроблення нових механізмів, які відповідають сучасним реаліям і забезпечують стійкість та відновлення.

Одним із центральних напрямів є інтеграція цифрових платформ, здатних ефективно підтримувати процеси ухвалення управлінських рішень у кризових ситуаціях [217]. Використання цифрових інструментів для оптимізації комунікації між державними органами та громадянами, на чому зосереджують увагу В. Дяченко та Н. Дяченко [219], є особливо актуальним в умовах воєнного стану. Такий підхід дозволяє не лише трансформувати

чинні адміністративні моделі, а й формувати якісно нові механізми взаємодії між державними органами та громадянами.

На думку І. Подобєд, цифровізація є важливим стимулом для розвитку інноваційного підприємництва та складником економічної безпеки держави [222]. Запозичення передового міжнародного досвіду, як зазначають Н.Демчишак, Р.Юрків та В.Демид, сприяє адаптації цифрових технологій до специфічних умов національної економіки, що забезпечує її стійкість і конкурентоспроможність [225]. Важливим також є створення сприятливих умов для розвитку бізнесу через податкові пільги та підтримку стартапів, орієнтованих на технологічний прогрес.

Значний потенціал цифрових медичних платформ для забезпечення доступності та безперервності медичних послуг під час війни підкреслює Н. Дяченко [220]. Інтеграція електронних систем дозволяє оптимізувати роботу закладів охорони здоров'я, забезпечуючи швидкий доступ до даних пацієнтів і координацію медичної допомоги.

Відомо, що цифрові технології відіграють ключову роль у збереженні соціального діалогу та захисті вразливих верств населення [221]. Тому використання цифрових платформ для моніторингу соціальних виплат та інтеграції в європейський економічний простір є важливим аспектом сучасних досліджень [223].

Особливу увагу Я.Худолей і Н.Загребельна приділяють питанням захисту персональних даних в умовах воєнного стану [224]. Забезпечення кібербезпеки та правових гарантій для користувачів цифрових послуг є нагальними завданнями, які сприяють збереженню стабільності в критичних ситуаціях. Таким чином, аналіз сучасних наукових праць з питань формування механізмів національного розвитку, заснованих на цифровізації в умовах воєнного стану, виявляє низку важливих аспектів, які раніше залишалися недостатньо дослідженими. Зокрема, основний акцент зроблено на застосуванні цифрових технологій для забезпечення ефективного управління критичними інфраструктурами та оптимізації ресурсних

механізмів у сфері цивільного захисту. Це передбачає інтеграцію сучасних цифрових платформ для координації дій у кризових ситуаціях, що дає змогу пришвидшити реагування на загрози та мінімізувати наслідки. Водночас цифровізація визнається ключовим чинником для впровадження інноваційних рішень, які сприяють не лише посиленню обороноздатності країни, а й забезпеченню економічної стабільності в умовах воєнного стану. У цьому контексті особливої уваги потребує вдосконалення нормативно-правової бази, пов'язаної із захистом персональних даних, що є вкрай актуальним через високі ризики кіберзагроз у період ескалації війни в Україні.

Цифрова економіка є рушійною силою сучасного розвитку, яка значно впливає на всі аспекти суспільного життя. Її базовими компонентами є цифрові платформи, технології автоматизації, штучний інтелект, блокчейн та інтернет речей (IoT) [220]. Цифровізація економіки також формує основу для її післявоєнного відновлення, інтеграції у світові ринки та зміцнення національної конкурентоспроможності. В останні роки було створено Електронний Уряд України – інтегровану багаторівневу інформаційну систему, що забезпечує взаємодію та інформаційний зв'язок з урядом на основі електронних форм.

Правовий режим воєнного стану вводиться для захисту національної безпеки та забезпечення ефективного функціонування державних структур в умовах надзвичайних обставин [219]. Воєнний стан може обмежувати діяльність певних секторів через пріоритетне використання інфраструктури для оборонних потреб. Уряд зобов'язаний впроваджувати обмеження на використання інформаційних технологій для уникнення витоку даних або кібератак. Система управління державою змінюється, акцентуючи увагу на оперативності рішень, що може призводити до зменшення прозорості та підзвітності процесів. Водночас введення воєнного стану стимулює інновації та цифрову трансформацію, адже змушує уряд і бізнес адаптуватися до нових умов, упроваджуючи швидкі рішення, наприклад, електронні сервіси для

мобілізації ресурсів, управління евакуацією населення та забезпечення гуманітарної допомоги.

Цифрова економіка являє собою сукупність соціально-економічних відносин, що базуються на застосуванні цифрових технологій для створення, передачі, оброблення та використання інформації. У контексті воєнного стану цифрова економіка набуває особливої важливості, забезпечуючи адаптивність державного управління, стійкість економіки та соціальної сфери до кризових викликів. Цифрові платформи виступають ключовими інструментами для підтримки адміністративних та комунікаційних процесів. Наприклад, платформи типу «Дія» дозволяють організувати дистанційний доступ до державних послуг, здійснювати виплати соціальної допомоги та координувати гуманітарні ініціативи. Вони також відіграють вирішальну роль у забезпеченні зворотного зв'язку між громадянами та державними органами в умовах обмеженої фізичної доступності.

Блокчейн-технології сприяють прозорості, безпеці та підзвітності у використанні державних і гуманітарних ресурсів. Їх застосування дозволяє створювати децентралізовані реєстри, які мінімізують корупційні ризики та підвищують довіру до рішень органів влади. У кризових умовах вони використовуються для моніторингу розподілу допомоги, управління фінансами та ведення електронного документообігу. Інтернет речей (ІоТ) забезпечує моніторинг та управління критичною інфраструктурою в реальному часі, що особливо важливо в умовах воєнних дій. Технології ІоТ використовуються для оцінювання стану транспортної, енергетичної та комунальної інфраструктури, що дозволяє оперативно реагувати на пошкодження або дефіцит ресурсів. Крім того, ІоТ сприяє підвищенню ефективності логістики та контролю за збереженням ресурсів у кризових умовах. Ці технології в комплексі створюють нові можливості для адаптації державного управління, підтримки економічної активності та підвищення стійкості національної системи під час надзвичайних ситуацій. Вони також відкривають перспективи для міжнародного співробітництва та залучення

інвестицій, спрямованих на розвиток цифрової інфраструктури України.

Для забезпечення ефективного функціонування державних і суспільних процесів в умовах воєнного стану необхідно розробити й запровадити механізми адаптації, які базуються на використанні цифрових технологій (табл. 2.8).

Таблиця 2.8

Механізми адаптації в умовах кризи

Механізм	Особливості
Цифрова трансформація державного управління	Використання електронних платформ для оперативного обміну інформацією між державними органами; Автоматизація процесів, пов'язаних із прийняттям рішень, для зменшення людського фактору та підвищення ефективності
Цифрові інструменти підтримки економіки	Впровадження онлайн-торговельних платформ для підтримки малого та середнього бізнесу; Використання електронних платежів та криптовалют для забезпечення фінансової стабільності у випадку обмеження роботи традиційних банківських систем
Забезпечення кібербезпеки	Створення систем моніторингу та реагування на кібератаки для захисту критичної інфраструктури; Навчання населення основам цифрової безпеки
Інновації в соціальній сфері	Використання онлайн-платформ для забезпечення безперервного доступу до освіти та медицини; Розвиток цифрових інструментів для координації волонтерської діяльності
Міжнародна співпраця	Залучення іноземного досвіду та інвестицій для розроблення нових цифрових рішень; Партнерство з міжнародними організаціями для створення спільних цифрових проєктів, які підтримують стійкість держави

Джерело: розроблено автором

Механізми цифровізації, як-от цифрові платформи, блокчейн та IoT, мають значний вплив на забезпечення національної стійкості, особливо в кризових умовах, спричинених воєнним станом. Вони підвищують адаптивність державного управління, забезпечують безперервність економічних процесів та знижують соціальну напругу. Зокрема, універсальна платформа «Дія» забезпечує громадянам доступ до державних послуг, включаючи видачу електронних документів, виплати компенсацій для переселенців, а також реєстрацію бізнесу та соціальних ініціатив. У воєнний

час вона стала важливим інструментом для підтримки комунікації між державою та населенням, допомагаючи зменшити бюрократичні затримки. Застосування блокчейн-рішень в Україні під час повномасштабної війни було спрямоване на прозорість гуманітарної допомоги. Наприклад, використання блокчейн-платформ для відстеження фінансових потоків допомогло забезпечити чесний розподіл міжнародної підтримки та зменшити корупційні ризики. IoT-системи були інтегровані в транспортну й енергетичну інфраструктуру, що дозволило в реальному часі контролювати стан об'єктів критичної інфраструктури. Наприклад, датчики на мостах і електростанціях дозволяють виявляти пошкодження, планувати ремонт і запобігати аваріям. Усе це значно покращило управління ресурсами в умовах війни. Наведені приклади демонструють, як впровадження цифрових технологій не тільки забезпечує національну стійкість у короткостроковій перспективі, але й створює фундамент для тривалого економічного та соціального розвитку.

У контексті правового режиму воєнного стану в Україні основною метою законодавчого регулювання є забезпечення національної безпеки, ефективного управління та підтримання соціальної стабільності. В умовах повномасштабної війни, коли країна стикається із зовнішніми та внутрішніми загрозами, законодавчі ініціативи повинні зберігати баланс між забезпеченням державної безпеки і захистом прав громадян. Ключову роль у формуванні нормативної бази відіграють кілька основних законів, які регулюють діяльність органів державної влади, державних і приватних інститутів та забезпечують правовий порядок.

Конституція України [226] визначає основні принципи правового державного управління, забезпечуючи громадянам базові права та свободи навіть у ситуаціях, коли вводиться воєнний стан. Конституція гарантує захист прав людини, що є основою для подальшої адаптації державного законодавства до нових умов. Хоча воєнний стан дає певні надзвичайні повноваження органам державної влади, Конституція зберігає принципи верховенства права, що дозволяє обмежувати права громадян лише в межах,

необхідних для забезпечення національної безпеки. Це створює основу для взаємодії між державою і громадянами, навіть під час виконання спеціальних заходів під час війни.

Закон України «Про правовий режим воєнного стану» [227] є основним нормативно-правовим актом, що регулює порядок запровадження, функціонування та скасування воєнного стану. Він визначає повноваження органів державної влади, військових адміністрацій та інших суб'єктів управління в умовах воєнного стану, що дає можливість ефективно реагувати на загрози національній безпеці. Закон передбачає особливі механізми адаптації державного управління до екстремальних умов, зокрема щодо мобілізації ресурсів, переміщення людей, використання території та управління економікою. Це дозволяє зберігати функціональність державних інститутів, навіть коли ситуація на фронті залишається нестабільною.

Закон України «Про національну безпеку» [228] включає важливі положення щодо захисту критичної інфраструктури країни, в тому числі у сфері цифрових технологій. У сучасних умовах ці технології стали основою національної безпеки, тому вказаний закон також містить положення про кібербезпеку. Кіберзагрози можуть стати не менш серйозними, ніж воєнні дії, тому питання захисту цифрових активів та інформаційних систем стають надзвичайно важливими в умовах війни. Закон про національну безпеку регулює всі аспекти, пов'язані з кіберзахистом, зокрема забезпечення стійкості критичних інформаційних інфраструктур, захисту від кібератак та розроблення національних стратегій безпеки в цифровому просторі.

Перелічені нормативні акти створюють базу для ухвалення рішень щодо впровадження цифрових інструментів у трьох основних секторах: у державному управлінні через електронне урядування та платформи для координації екстрених заходів; в економіці, де використовуються цифрові сервіси, включаючи онлайн-торгівлю, електронний документообіг та фінансові інструменти; у соціальній сфері, забезпечуючи доступ до соціальних послуг через такі цифрові канали, як дистанційна освіта,

телемедицина та онлайн-консультації. Узгодженість цих законодавчих ініціатив дозволяє Україні не лише відповідати на виклики сьогодення, але й створювати передумови для відновлення та розвитку цифрової інфраструктури в післявоєнний період.

Законодавчі заходи активно сприяють трансформації державного апарату через упровадження цифрових інструментів, одним з яких є Закон України «Про електронні довірчі послуги» [229], оскільки він регулює використання цифрових підписів, електронної ідентифікації та документообігу, що значно полегшує процеси взаємодії між громадянами, бізнесом та державою. За допомогою цього нормативного акта стало можливим здійснення електронних транзакцій і надання послуг в онлайн-форматі, що особливо актуально в умовах обмеженого фізичного доступу до державних установ під час війни.

Закон «Про стимулювання розвитку цифрової економіки в Україні» [230] вводить механізми підтримки ІТ-сектору, стартапів і технологічних компаній, що сприяє розвитку інновацій на підприємствах, їх виходу на міжнародний ринок і створенню нових робочих місць у країні. Податкові стимули для ІТ-сфери, зокрема пільгове оподаткування для компаній, що займаються розробками програмного забезпечення і технологічними інноваціями, надають значний імпульс для розвитку цифрових технологій в Україні. Це дозволяє залучати інвестиції в галузь, що є однією з найдинамічніших в економіці.

Закон «Про віртуальні активи» [231] визначає правовий статус криптовалют та інших цифрових активів, що сприяє розвитку фінансових технологій і забезпечує стабільність у криптовалютному секторі. Це важливий крок для регулювання сфери віртуальних фінансів, забезпечення безпеки транзакцій і підвищення довіри до цифрових валют.

Крім того, цифровізація активно впливає на розвиток торгівлі та бізнесу в Україні. Законодавчі ініціативи, спрямовані на стимулювання онлайн-торгівлі, включають спрощення процедур реєстрації суб'єктів

господарювання, а також упровадження електронних касових апаратів, що дозволяє підприємцям швидко та ефективно вести свою діяльність [225]. Це набуває особливого значення в умовах воєнного стану, коли доступ до фізичних торгових точок обмежений, а онлайн-продажі дозволяють бізнесу функціонувати в умовах постійних змін і непередбачуваності. Отже, завдяки впровадженню таких цифрових інструментів, як електронне урядування, онлайн-торгівля, дистанційна освіта та телемедицина, в Україні забезпечується безперебійне функціонування важливих секторів у кризових умовах, а також створено основи для подальшого відновлення та модернізації держави і підвищення її конкурентоспроможності на міжнародній арені.

Воєнний стан суттєво вплинув на правове регулювання цифрових трансформацій в Україні, змусивши державу адаптувати законодавство до нових викликів та загроз. Потреба в забезпеченні національної безпеки, стабільності державного управління, економіки та соціальної сфери призвела до прискорення впровадження цифрових інструментів і технологій. У цих умовах законодавство було спрямоване на підтримку стійкості критичної інфраструктури, розвиток електронного урядування, посилення кібербезпеки та стимулювання цифрової економіки [217]. Водночас регуляторна база мала враховувати обмеження та специфіку кризового періоду, створюючи гнучкі та оперативні механізми для ефективного управління та підтримки громадян. Такий підхід закладає основу для довгострокових трансформацій, сприяючи відновленню країни та її інтеграції в сучасний цифровий простір.

Практичні аспекти цифровізації в умовах воєнного стану охоплюють кілька важливих сфер, кожна з яких має значний вплив на забезпечення стабільності країни та ефективне управління. У державному управлінні цифрові платформи стали незамінним інструментом для оперативного прийняття рішень. Наприклад, електронне урядування та платформи для комунікації між органами влади і громадянами дозволяють швидко реагувати на змінювану ситуацію та забезпечувати доступ до державних послуг навіть у кризових умовах. Як уже було зазначено вище, платформа «Дія», яка

активно використовується для надання електронних документів та послуг, дає можливість громадянам отримувати важливі документи без необхідності відвідувати державні установи, що є важливим під час воєнного стану.

В економічній сфері цифровізація сприяє підтримці бізнесу через різноманітні механізми національного розвитку, спрямовані на оптимізацію управлінських процесів, ефективне використання ресурсів та підтримку економічної стійкості держави в періоди криз. Одним із важливих інноваційних інструментів є розроблення платформ для збору та аналізу даних у реальному часі. Така система дозволяє оперативно відслідковувати зміни в економічній та соціальній ситуації, а також приймати обґрунтовані рішення для оптимізації ресурсів і забезпечення необхідних заходів безпеки. Завдяки використанню таких платформ можна швидко адаптувати державні та бізнес-процеси до нових умов, підвищити ефективність управління та прогнозувати потенційні загрози.

Іншим важливим інструментом є використання штучного інтелекту для управління критичними процесами. Штучний інтелект дозволяє значно покращити оброблення великих обсягів даних, автоматизувати ухвалення рішень у сферах, що потребують швидкої реакції, як-от безпека, економіка, логістика та управління енергетичними ресурсами. Використання алгоритмів для виявлення аномалій, прогнозування кризових ситуацій та оптимізації виробничих і постачальницьких ланцюгів є важливим кроком до цифровізації економіки та управлінських структур, що дозволяє країні ефективніше реагувати на зовнішні та внутрішні виклики.

Стратегічним напрямом розвитку через цифровізацію є створення національної програми цифрової стійкості. Така програма передбачає інтеграцію цифрових технологій у всі сфери суспільного життя: від державного управління до освіти і охорони здоров'я. Вона включає розроблення національної інфраструктури для забезпечення безпечного та ефективного використання цифрових технологій, захисту даних та розвитку цифрових навичок населення. Це не лише підвищить

конкурентоспроможність країни на міжнародній арені, але й сприятиме її соціально-економічному зростанню в умовах глобальних змін.

Міжнародна співпраця та інвестиції теж сприяють розвитку цифрових технологій в Україні, зокрема в умовах війни та економічної кризи. Залучення міжнародних партнерів надає можливість як фінансової підтримки, так і впровадження передових технологій, що допомагає країні адаптуватися до нових викликів [223]. Одним з яскравих прикладів є програма підтримки від Європейського Союзу для розширення доступу до широкосмугового інтернету в сільських та віддалених регіонах України. Це співробітництво не лише сприяє розвитку цифрової інфраструктури, але й допомагає зменшити цифрову нерівність у країні. Також фінансування від USAID допомогло впровадити цифрові платформи для полегшення доступу до державних послуг в умовах воєнного стану. Партнерство з такими міжнародними організаціями, як World Bank та UNDP, дозволило реалізувати проєкти, спрямовані на вдосконалення електронних послуг в Україні, зокрема через платформу «Дія». Ця ініціатива покращила доступ до соціальних виплат та інших державних послуг, що особливо важливо в умовах кризи. В Україні активно розвивається співпраця з міжнародними технологічними компаніями IBM та Microsoft для впровадження блокчейн-технологій у сферу державного управління. Зокрема, блокчейн використовується для забезпечення прозорості та безпеки державних реєстрів, як-от реєстр нерухомості, що дозволяє зменшити ризики корупції та підвищити ефективність управління в умовах кризових ситуацій. Співпраця з міжнародними партнерами також включає ініціативи у сфері інтернету речей (IoT), які сприяють розвитку смарт-міст і покращенню управління енергетичними, транспортними та комунікаційними ресурсами. Ініціативи на кшталт Smart City в Україні реалізуються за участі міжнародних компаній, що дозволяє розвивати інфраструктуру, яка адаптована до сучасних вимог безпеки та ефективного використання ресурсів. Такі проєкти й ініціативи мають важливе значення для розвитку цифрових технологій в Україні та є

основою для побудови більш стійкої та адаптивної економіки під час війни.

Інтеграція інноваційних інструментів і стратегічних напрямів у процеси національного розвитку через цифровізацію забезпечить ефективне функціонування країни навіть в умовах криз та обмежених ресурсів, забезпечуючи стабільність, розвиток економіки, покращення управлінських механізмів та створення конкурентних переваг для України в глобальному контексті. Наприклад, упровадження електронних рішень для управління ланцюгами постачання дозволяє підприємствам швидше адаптуватися до змін у логістиці та попиті. Ці платформи автоматизують процеси, зменшують час на пошук постачальників та дозволяють ефективно керувати запасами та замовленнями. Окрім того, використання цифрових інструментів для моніторингу та аналізу фінансових потоків допомагає бізнесу зберігати стійкість в умовах нестабільності. У соціальній сфері цифровізація також відіграє важливу роль. Розвиток онлайн-освіти дозволяє забезпечити доступ до навчальних матеріалів та занять навіть у віддалених чи небезпечних регіонах, що дає можливість продовжувати навчання дітей та дорослих у період, коли фізична присутність у закладах освіти неможлива. Крім того, використання цифрових інструментів для забезпечення соціального захисту дає змогу оперативно надавати соціальні виплати, пенсії та іншу допомогу через онлайн-сервіси, що важливо для забезпечення підтримки вразливих груп населення в умовах війни [6].

Таким чином, цифровізація стала важливим елементом національної стратегії, забезпечуючи безперервність функціонування ключових державних, економічних та соціальних інститутів навіть у складних умовах воєнного стану. Однак процес цифровізації також пов'язаний з низкою викликів та ризиків, які можуть обмежити ефективність впровадження новітніх технологій. Технологічні та соціальні проблеми, пов'язані з цифровізацією, вимагають комплексного підходу для їх розв'язання. Від успішного подолання цих викликів залежить не тільки розвиток держави в умовах воєнного стану, але й можливості для її подальшого відновлення та

сталого розвитку в післявоєнний період (табл. 2.9).

Таблиця 2.9

Виклики та ризики цифровізації

Виклики	Приклади їх подолання
Кіберзагрози	Зростання кібератак на критичну інфраструктуру є одним із ключових ризиків цифровізації. Для боротьби із цим в Україні створено державний орган – Національний координаційний центр кібербезпеки, діяльність якого включає моніторинг, прогнозування кіберзагроз та реагування на атаки. Наприклад, відбиття масованих кібератак на українські енергетичні об’єкти продемонструвало ефективність цих заходів
Цифрова нерівність	Не всі громадяни України мають рівний доступ до цифрових технологій. Для подолання такої проблеми уряд разом із міжнародними партнерами реалізує проєкт «Інтернет-субвенція», який забезпечує доступ до швидкісного інтернету в сільських і віддалених районах. Це допомагає зменшити розрив між містами та селами, сприяючи соціальній згуртованості населення
Захист конфіденційності	Зростання обсягу цифрових даних, які обробляються державними установами, підвищує ризик їх витоку. У відповідь в Україні впроваджуються блокчейн-технології для захисту реєстрів, зокрема реєстру нерухомості. Це гарантує, що дані залишатимуться незмінними та захищеними від стороннього втручання
Інфраструктурні виклики	Масштабні руйнування фізичної інфраструктури ускладнюють цифровізацію, особливо в зоні бойових дій. Однак упровадження мобільних дата-центрів і відновлення комунікаційних ліній за підтримки міжнародних партнерів, як-от Starlink, дозволяє зберігати функціональність цифрових платформ навіть у складних умовах
Навчання цифрових навичок	Відсутність цифрової грамотності серед частини населення гальмує повноцінне впровадження технологій, тому було започатковано національну програму «Дія. Цифрова освіта», яка надає громадянам можливість безкоштовно навчатися основам роботи з цифровими інструментами

Джерело: розроблено автором

Виклики та ризики цифровізації в умовах воєнного стану вимагають від держави не тільки технічних рішень, але й соціальної та правової уваги. Кібербезпека та захист даних стають критично важливими, оскільки під час війни зростає ймовірність кібератак та спроб втручання в державні інформаційні системи. Обмеження інфраструктури, що виникають унаслідок руйнувань та дестабілізації через бойові дії, ускладнюють впровадження і підтримку цифрових технологій. У соціальному контексті важливими є питання нерівного доступу до цифрових ресурсів, що може поглиблювати соціальну нерівність, а також захист прав людини і конфіденційності особистої інформації в умовах надзвичайних ситуацій. Системний підхід до розв'язання цих проблем допоможе мінімізувати ризики та забезпечити ефективне впровадження цифрових технологій в умовах кризи.

Захист інформації в умовах війни не обмежується лише технічними аспектами. Серед важливих складників є також правове забезпечення захисту даних, включаючи розроблення нормативно-правових актів, що встановлюють стандарти захисту інформації, особливо конфіденційної, в умовах кризових ситуацій [223]. У цьому контексті уряд України має створити юридичні механізми, які дозволяють державним та приватним структурам працювати з інформацією в умовах обмежень воєнного стану, зокрема забезпечення прозорості та довіри до електронних систем державного управління [221]. Цифровізація також вимагає розгляду питань захисту прав людини в умовах війни, адже створюються нові ризики для особистої свободи, права на приватність та доступу до інформації. У цифровому середовищі зростає ризик порушення конфіденційності особистих даних, що може бути використано як інструмент політичного або військового тиску. Отже, важливим є створення таких правових механізмів, які б захищали громадян від несанкціонованого збору та використання їхніх особистих даних, особливо за обмеженого доступу до правосуддя та контролю за діями держави в умовах воєнного стану.

Сучасна геополітична турбулентність та безпрецедентний характер

повномасштабної агресії РФ проти України вивели на передній план не стільки питання нарощування окремих елементів обороноздатності, скільки потребу у цілісній НМС як новій організуючій рамці державної політики. Традиційні підходи, зосереджені переважно на військовій силі та фізичному захисті кордонів, виявилися концептуально обмеженими в умовах гібридної війни, де бої точаться одночасно в кіберпросторі, інформаційному полі, економіці, на рівні суспільної довіри та здатності інфраструктурних систем зберігати працездатність. Формалізація національної стійкості Указом Президента України у 2021 році шляхом затвердження «Концепції забезпечення національної системи стійкості» закріпила перехід від фрагментарного бачення безпеки до інтегративної моделі, у якій якість взаємозв'язків між підсистемами не менш важлива, ніж їхня індивідуальна потужність [232].

У цьому контексті варто виокремити три базових напрями аналізу НМС:

Напрямок І: Забезпечення безперервності урядування та цифрова інфраструктура держави. В умовах війни здатність уряду продовжувати виконання своїх функцій є критичним показником стійкості. Український досвід продемонстрував, що цифрова інфраструктура може бути більш живучою, ніж фізична, за умови правильної архітектури та правового забезпечення.

До початку повномасштабного вторгнення українське законодавство жорстко регламентувало зберігання державних даних виключно на серверах, фізично розташованих в Україні. Це створювало критичну вразливість: фізичне знищення дата-центрів ракетними ударами могло призвести до паралічу державного апарату. Проте, за тиждень до 24 лютого 2022 року, Верховна Рада прийняла революційні зміни до законодавства, дозволивши міграцію державних реєстрів у хмарні середовища за кордоном. Цей крок дозволив оперативно перенести критичні дані на сервери таких техногігантів, як Amazon Web Services (AWS) та Microsoft Azure. AWS, використовуючи

свій досвід реагування на катастрофи, допоміг українським відомствам побудувати захищені канали передачі даних та забезпечити їх резервне копіювання. Це створило ефект «розподіленої держави, дані стали екстериторіальними, що гарантувало збереження інформації про права власності, громадянський стан та соціальні виплати навіть у випадку окупації територій.

Платформа «Дія», запущена у 2020 році як інструмент зручних державних послуг, під час війни трансформувалася у мультифункціональну платформу національної стійкості [233]. Архітектура «Дії», побудована на системі інтероперабельності «Трембіта» (аналог естонської X-Road [234]), дозволила забезпечити обмін даними між реєстрами без створення єдиної вразливої бази даних. В умовах масового переміщення населення (ВПО та біженці), цифрові документи в «Дії» отримали юридичну силу повних аналогів паперових документів, що стало унікальним прецедентом у світовій практиці. Україна стала першою країною з повністю цифровим паспортом, дійсним усюди. Це дозволило мільйонам громадян, які втратили документи під час евакуації, підтвердити свою особу, отримати доступ до банківських послуг та перетнути кордон (за домовленостями з країнами-сусідами).

Функціонал платформи був оперативно розширений для вирішення завдань ПРВС: по-перше, *соціальна підтримка* – автоматизація виплат для ВПО (190 тис. користувачів на початковому етапі) та послуга «Відновлення» для компенсації за зруйноване житло дозволили уникнути колапсу системи соціального захисту [235]. По-друге, *інформаційний опір* – запуск «Дія.ТБ» та «Дія.Радіо» забезпечив доступ до офіційних джерел інформації в умовах блекаутів та знищення телевеж. По-третє, *громадянська розвідка* – чат-бот «ЄВорог» дозволив громадянам безпечно передавати координати ворожої техніки, перетворивши смартфони українців на елементи системи ситуаційної обізнаності армії. Авторизація через «Дію» мінімізувала ризик спаму та дезінформації.

В умовах ПРВС стійкість цифрової інфраструктури забезпечується не

лише технологіями, але й інституційною спроможністю. Міністерство цифрової трансформації спільно з Держспецзв'язку сформували ефективну вертикаль кіберзахисту. Важливим досягненням стало підтвердження відповідності платформи «Дія» вимогам регламенту e-IDAS [337] у 2023 році та отримання сертифікації ISO/IEC 27001 [238] оператором вузла e-IDAS в Україні у червні 2025 року. Це не лише свідчить про високий рівень безпеки, але й відкриває шлях до повної інтеграції в Єдиний цифровий ринок ЄС, дозволяючи взаємне визнання цифрових підписів та ідентифікаторів.

Напрямок 2: Ситуаційна обізнаність та аналіз ризиків національної безпеки.

У сучасній війні перемагає той, хто швидше збирає, обробляє та використовує інформацію. Саме тому Україна імплементувала передові інструменти Data-Driven Decision Making на найвищому державному рівні. Зокрема, державне управління проходить етап цифровізації, що передбачає системне збирання, накопичення та аналіз інформації для обґрунтованого прийняття рішень. Великі компанії, як-от ДТЕК, також інтегрують DDDM-стратегії в рамках своїх програм цифрової трансформації. Це дозволяє оптимізувати процеси, підвищити ефективність та реагувати на зміни ринку більш гнучко. Подальша успішна імплементация залежить від комплексної реалізації цифрових стратегій без фрагментації.

Так, система «СОТА» (Інформаційно-аналітична система «СОТА»), розроблена та впроваджена Апаратом Ради національної безпеки і оборони (РНБО), стала головним інструментом стратегічного моніторингу. «СОТА» є складною багатошаровою інформаційно-аналітичною системою найвищого рівня захисту інформації, має гнучку, відкриту архітектуру, що дозволяє створювати нові функціональні модулі відповідно до завдань, які виникають при реалізації державної політики в сфері національної безпеки. Вона агрегує дані з усіх доступних державних реєстрів та закритих джерел, візуалізуючи їх у режимі реального часу [239].

Ключові функціональні модулі «СОТА»: 1) *військовий моніторинг* –

відстеження ракетних обстрілів, переміщення військ, аналіз оперативної обстановки на фронті та контроль постачання західного озброєння, що дозволило військово-політичному керівництву мати цілісну картину бойових дій; 2) *економічна безпека* – система моніторингу сплати податків, використання надр, стану енергетики та продовольчої безпеки. Це дозволило виявляти кризові явища (наприклад, дефіцит палива чи продовольства) на ранніх стадіях; 3) санкційний контроль як окремий модуль, що відстежує ефективність застосування санкцій проти фізичних та юридичних осіб, виявляючи спроби їх обходу [239].

Напрямок 3. Військово-технічна трансформація та екосистема Defense Tech [240]. Війна в Україні стала каталізатором безпрецедентного розвитку оборонних технологій, де приватний сектор та стартапи відіграють провідну роль. Кластер Brave1: Акселератор інновацій для фронту. Створений у квітні 2023 року кластер Brave1 став єдиним вікном для співпраці між державою, військовими та розробниками (G2B та B2G). Він виконує функції акселератора, надаючи гранти, експертизу та доступ до випробувань. Brave1 допоміг українським defense-tech компаніям залучити \$90 млн зовнішніх інвестицій з 2024 року. Середній чек інвестицій зріс з \$300 тис. до \$1 млн, що свідчить про зростання довіри інвесторів та зрілості проектів. Окрім безпілотних літальних апаратів (БПЛА), яких у 2024 році було поставлено понад 1,3 млн одиниць, кластер активно розвиває напрями наземних роботизованих комплексів (UGV), систем радіоелектронної боротьби (РЕБ), ІШІ для аналізу відеопотоків та технологій розмінування [240].

Важливо вказати на цифровізацію Збройних Сил України. Запуск застосунку «Армія+» у серпні 2024 року став символом переходу від радянської паперової бюрократії до цифрових стандартів управління персоналом у Збройних Силах. Платформа «Армія+» є комплексною державною цифровою ініціативою, спрямованою на модернізацію військової сфери України. Вона поєднує в собі освітній компонент для підвищення військової майстерності військовослужбовців через онлайн-навчання, а

також надає функціонал для спрощення та вирішення бюрократичних питань, що є особливо важливим в умовах сучасної війни. Платформа дозволяє військовим зручно взаємодіяти з документами та сервісами, використовуючи сучасні технології, зокрема авторизацію через BankID. Також існує освітньо-інформаційний портал, спеціально розроблений для потреб військових закупівельників.

Функціональні можливості «Армія+»: 1) запровадження Army ID та цифрових рапортів (на відпустку, лікування, матеріальну допомогу); 2) зворотний зв'язок – модуль опитувань дозволяє Генеральному штабу та Міністерству оборони України отримувати верифіковану інформацію про потреби бійців (харчування, екіпірування, моральний стан) безпосередньо, минаючи проміжні ланки командування, що зменшує викривлення інформації; 3) гнучкість служби – новий функціонал, анонсований у 2025 році, дозволяє спрощену процедуру переведення між військовими частинами та навіть між різними видами сил (ЗСУ та НГУ), що підвищує ефективність використання кадрового потенціалу [241].

Отже, національна стійкість (resilience) постає не поєднанням ізольованих секторних спроможностей, а властивістю цілісної конфігурації держави і суспільства, що визначається тим, наскільки узгоджено працюють інституції, інфраструктури, ринки, спільноти та цифрові платформи. Йдеться про здатність системи не лише протидіяти загрозам різної природи, а й підтримувати життєво важливі функції в умовах шоків, швидко змінювати режими роботи під впливом нових викликів та відновлювати збалансований стан на вищому рівні організації. Ключовим у цьому є чутливість до змін і здатність до своєчасного коригування: НМС орієнтується на постійне збирання сигналів із різних середовищ, їхню аналітичну обробку та оперативне перетворення на управлінські рішення, що дозволяє уникати запізнілих реакцій і накопичення критичних вразливостей.

У такій архітектурі цифровізація перетворюється з допоміжного інструмента модернізації на структурну «цифрову платформу» держави, від

стану якої прямо залежить ефективність усієї НМС. Саме цифрові платформи інтегрують розрізнені потоки даних, з'єднують між собою органи влади, бізнес, громадянське суспільство та локальні спільноти, забезпечують безперервність управління і публічних сервісів, навіть коли фізична інфраструктура зазнає ударів. Від того, наскільки глибоко безпекова політика, економічне регулювання, соціальна підтримка та територіальне управління враховані такою цифровою платформою, залежить реальна здатність НМС підтримувати керованість, економічну активність і соціальну згуртованість у режимі постійної загрози. Таким чином, якість національної стійкості визначається не лише наявністю окремих цифрових сервісів чи оборонних спроможностей, а цілісністю та узгодженістю конфігурації, в якій вони функціонують і спільно генерують новий рівень адаптивності держави.

Отже, методологія виокремлення ключових напрямів цифровізації як структурного елемента НМС ґрунтується на поетапній аналітичній процедурі, яка дозволяє перейти від розрізнених нормативних положень та управлінських практик до цілісної типології. Вихідною передумовою є розуміння цифровізації не як сукупності окремих ІТ-проектів, а як одного з базових вимірів національної стійкості, що пронизує безпекову політику, публічне управління, економічне регулювання, соціальну сферу та комунікацію держави з громадянами. У цьому контексті аналітичний фокус спрямовується не на опис окремих технологічних рішень, а на реконструкцію конфігурації політик, у межах якої цифрові інструменти набувають інституційного та безпекового значення.

На *першому етапі* формується сукупність джерел, яка слугує емпіричним підґрунтям дослідження. До неї включаються ключові нормативно-правові акти у сферах цифрової трансформації, національної безпеки, кібербезпеки, публічного управління, регулювання та захисту критичної інфраструктури, а також стратегічні документи – концепції, стратегії, державні програми, дорожні карти цифровізації й стійкості, затверджені або актуалізовані в досліджуваний період. Окремий блок

становлять офіційні аналітичні звіти профільних міністерств і урядових офісів, презентаційні матеріали, в яких узагальнюються цілі, інструменти та проміжні результати цифрових ініціатив, а також публічні комунікації органів державної влади, що відображають еволюцію підходів до цифровізації в умовах воєнної та безпекової кризи. Відбір документів здійснюється за наперед визначеними критеріями часової актуальності (відповідність досліджуваному проміжку), тематичної релевантності (змістовний зв'язок із цифровими інструментами управління, безпеки чи стійкості), офіційного статусу (ухвалення або схвалення уповноваженими органами) та впливовості (роль документа у формуванні рамкових політик для інших актів і програм).

На *другому етапі* вибудовується аналітична рамка та формується категоріальна сітка для якісного контент-аналізу. Виходиться з того, що описи цифрових ініціатив у нормативних і стратегічних текстах розгортаються одночасно в кількох вимірах, тому для подальшого кодування задаються щонайменше п'ять основних вимірів. По-перше, функціональний вимір, у межах якого фіксуються управлінські завдання, покладені на цифрові інструменти: моніторинг, координація, надання публічних послуг, управління ризиками, кризове реагування, комунікація, аналітична обробка даних, підтримка прийняття рішень, забезпечення безперервності функціонування критичних систем тощо. По-друге, інституційний вимір, орієнтований на ідентифікацію акторів, що залучаються до розроблення та реалізації цифрових політик: центральні органи виконавчої влади, органи сектору безпеки й оборони, органи місцевого самоврядування, суб'єкти приватного сектору, громадські організації, експертні спільноти. По-третє, технологічний вимір, який охоплює типи цифрових рішень (державні та відомчі платформи, реєстри, мобільні застосунки, хмарні та гібридні інфраструктури, системи аналітики й обробки великих даних, засоби кіберзахисту). По-четверте, просторовий вимір, де фіксується рівень розгортання ініціатив – національний, регіональний, локальний,

міждержавний. По-п'яте, безпековий вимір, у межах якого відстежуються категорії загроз і вразливостей, на які спрямовані цифрові рішення: військові, інформаційні, кібернетичні, енергетичні, економічні, соціальні, гуманітарні, демографічні тощо. Категоріальна сітка конструюється як відкрита до уточнень система, що допускає розширення й конкретизацію набору кодів у процесі роботи з емпіричним матеріалом.

На *третьому етапі* зазначена сітка застосовується до відібраного переліку джерел, і здійснюється покрокове кодування змісту. Кожен текстовий фрагмент, у якому описуються цифрові інструменти, ініціативи чи політики, позначається відповідними кодами за всіма релевантними вимірами. У поле уваги потрапляють не лише прямі згадки цифровізації, а й опосередковані контексти, де використання цифрових технологій пов'язується із завданнями стійкості, наприклад: підтримкою функціонування критичної інфраструктури під час атак, забезпеченням безперервності соціальних виплат і базових державних послуг у кризових умовах, дистанційною організацією роботи освітніх та медичних систем, координацією дій між органами влади, приватним сектором і громадянським суспільством. Результатом цього етапу стає карта розподілу цифрових ініціатив за секторами політики, типами технологічних рішень, колом залучених акторів і категоріями загроз, на які вони спрямовані. Така карта дозволяє виявити як очевидні, так і латентні зони концентрації цифрових перетворень у структурі НМС.

Четвертий етап пов'язаний із переходом від рівня окремих закодованих фрагментів до рівня узагальнених смислових кластерів. На основі отриманих даних здійснюється групування цифрових практик і політик, у яких повторюються подібні конфігурації управлінських функцій, технологічних рішень та інституційних акторів. Формуються, зокрема, кластери, що відображають внутрішню трансформацію державного управління (автоматизація документообігу, інтеграція відомчих інформаційних систем, створення міжвідомчих шлюзів, розвиток внутрішніх

цифрових сервісів органів влади); кластери, пов'язані з електронним урядуванням та мобільними сервісами для громадян і бізнесу (електронні документи, онлайн-реєстрація статусів, дистанційне отримання соціальних та адміністративних послуг, цифрові інструменти підтримки підприємництва); кластери, що описують побудову систем ситуаційної обізнаності, управління загрозами та ризиками (інтегровані платформи, реєстри, аналітичні панелі, системи раннього попередження); а також кластери, які відображають інституціоналізоване публічно-приватне партнерство у сфері цифрових рішень. При цьому дотримуються критерії внутрішньої однорідності (наявність спільної управлінської логіки та близького кола акторів усередині кластера) та зовнішньої відмінності (розмежування кластерів за їхньою основною функціональною роллю в архітектурі НМС).

На *п'ятому етапі* здійснюється перехід від смислових кластерів до узагальнених напрямів цифровізації та їх інституційно-політична верифікація. Попередньо виокремлені кластери інтерпретуються як потенційні напрями й перевіряються на предмет їхньої стійкості у часовому вимірі та закріпленості в інституційній структурі. Для кожного напрямку аналізується наявність відповідних організаційних утворень (профільних органів, підрозділів, центрів компетенцій, міжвідомчих координаційних механізмів), наявність чи відсутність спеціалізованих стратегій, програм, концепцій, дорожніх карт, а також наявність пріоритетних державних або державно-приватних проєктів, які втілюють відповідну логіку цифровізації на практиці. Такий підхід дозволяє відокремити стійкі, структурно значущі напрями від випадкових, короткотривалих чи суто декларативних ініціатив, що не отримали інституційного продовження.

Шостий етап передбачає порівняльне зіставлення отриманої типології напрямів з міжнародними аналітичними рамками у сфері цифрового врядування, національної безпеки та резильєнтності. У цьому контексті аналізується, наскільки виокремлені напрями відповідають усталеним у науковому дискурсі категоріям (цифрове врядування, управління ризиками,

кібербезпека, управління даними, локальна стійкість, роль приватного сектора, адаптивне стратегічне планування) і разом із тим відображають специфіку конкретного національного контексту, зокрема воєнних і поствоєнних викликів. За потреби здійснюється уточнення назв і меж напрямів, аргументується збереження тих елементів, які не мають прямих аналогів у міжнародних схемах, але концептуально важливі для опису вітчизняної моделі стійкості. Метою цього етапу є інтеграція національно специфічної типології в ширший науковий і політичний контекст без втрати її аналітичної чіткості.

На *сьомому, верифікаційному етапі*, до аналізу залучаються емпіричні кейси реалізації цифрових рішень у кризових і воєнних умовах, а за можливості – й експертні оцінки. Розглядаються конкретні приклади міграції державних сервісів у хмарні середовища, організації цифрової підтримки оборони, забезпечення безперервності соціальних виплат та надання базових послуг через мобільні застосунки, відновлення роботи освітніх, медичних та інших критичних систем за рахунок цифрових платформ. Кожен із таких кейсів співвідноситься з виокремленими напрямками цифровізації, що дає змогу уточнити їхні межі, виявити гібридні або проміжні конфігурації, а також перевірити, чи відповідає побудована типологія фактичним практикам функціонування держави в умовах високої турбулентності. У разі виявлення систематичних розбіжностей здійснюється коригування структури напрямів, зберігаючи загальну логіку типології.

Узагальнено, описана методологія передбачає послідовність кроків від формування корпусу джерел, розроблення категоріальної сітки та проведення якісного контент-аналізу – до кластеризації цифрових практик, інституційно-політичної верифікації, порівняння з міжнародними підходами та емпіричної перевірки. Така логіка дозволяє сформулювати не довільний перелік цифрових ініціатив, а науково обґрунтовану типологію напрямів цифровізації як взаємопов'язаних, але аналітично розрізнених компонентів НМС, що відображає структурну роль цифрових інструментів у забезпеченні

життєздатності держави в умовах тривалих і багатовимірних криз.

Квінтесенцією такої логіки управлінської діяльності у 2016-2024 рр. виступило нормативне переосмислення системи державного управління у сфері безпеки, що відбувалося в умовах формальної стабільності конституційного ладу, коли масштабний конституційний процес 2016–2020 рр. [242-248] з акцентом на децентралізацію влади не завершився внесенням змін до Основного Закону не завершився внесенням змін до Конституції України, зокрема, щодо територіальної організації влади, але створив стійку політико-правову рамку для подальших реформ у безпековому секторі. За таких умов поступове оновлення законодавства та стратегічних документів узяло на себе функцію «м'якої конституціоналізації» нової моделі публічного управління безпеки: через закріплення принципів субсидіарності, збалансованої централізації й децентралізації, верховенства права, демократичної підзвітності, ризикоорієнтованого підходу та національної стійкості як базової цінності.

Прийняття Закону України «Про національну безпеку України» надало цьому процесу системного характеру, визначивши секторальні складові безпеки, механізми цивільного демократичного контролю, засади інтеграції до ЄС і НАТО, а також поклавши на Стратегію національної безпеки статус «матриці» для підпорядкованих стратегій воєнної, інформаційної, економічної, кібербезпеки та національної стійкості [228]. У межах цієї рамки воєнне управління та інші безпекові підсистеми отримали чіткі контури раціоналізації: було запроваджено логіку всеохоплюючої оборони, розбудови спроможностей, орієнтації на безпеку людини та її прав, розвитку партнерств, посилення інституційної й організаційної стійкості держави й суспільства.

Поступова поява в 2017–2024 рр. комплексу стратегій і концепцій – у сфері національної, воєнної, економічної, інформаційної та кібербезпеки, а також Концепції забезпечення національної системи стійкості [249-254] закріпила нормативну модель безпеки, у якій інтегруються принципи

превенції, готовності, всеохоплюючої оборони, захисту критичної інфраструктури, багаторівневого управління ризиками та широкої взаємодії держави, громад і бізнесу. Водночас така еволюція стратегічних документів позначила перехід від фрагментарних підходів до цілісної архітектури національної стійкості, де безпекові й розвиткові цілі розглядаються у взаємозв'язку, а не як конкуруючі пріоритети. У практичному вимірі це створює підґрунтя для формування узгоджених міжвідомчих механізмів планування, фінансування та оцінювання ризиків, що дозволяють поєднати оборонний, цивільний, економічний і муніципальний виміри політики стійкості (таблиця 2.10)

Таблиця 2.10

Ключові стратегії і концепції у сфері безпеки, ухвалені у 2017–2024 рр.

(подаються основні рамкові документи загальнодержавного рівня)

Рік	Документ (офіційна назва, стисло)	Тип	Ключовий фокус / зміст	Базові принципи та акценти (у контексті НС)
2017	Доктрина інформаційної безпеки України (Указ Президента від 25.02.2017)	Доктрина	Визначення засад державної політики у сфері інформаційної безпеки, ідентифікація інформаційних загроз, насамперед з боку РФ; окреслення пріоритетів розвитку нац. інформаційного простору, протидії пропаганді та дезінформації	Суверенітет в інформаційному просторі, захист конституційного ладу, поєднання свободи вираження поглядів і безпеки, розвиток власних медіа-спроможностей, взаємодія держави й суспільства в протидії інформаційним впливам
2020	Стратегія національної безпеки України «Безпека людини – безпека країни» (Указ Президента №392/2020 від 14.09.2020)	Стратегія	Базовий документ, що визначає нац. інтереси, загрози, стратегічні цілі та засади політики безпеки; встановлює три ключові «стовпи»: стримування, стійкість, взаємодія	Людиноцентричність (безпека людини як ядро), демократична підзвітність сектору безпеки, інтеграція до ЄС і НАТО, всеохоплюючий підхід до загроз, розвиток спроможностей, національна стійкість і управління ризиками як системний принцип
2021	Стратегія воєнної безпеки України «Воєнна безпека – всеохоплююча оборона» (Указ Президента №121/2021 від 25.03.2021)	Стратегія	Конкретизація воєнного виміру НБ: модель всеохоплюючої оборони, підготовка держави, сил оборони та суспільства до тривалої збройної боротьби; інтеграція військової та цивільної компонент	Всеохоплююча оборона, інтеграція цивільно-військового управління, готовність і мобілізація, розвиток сил оборони й територіальної оборони, партнерство з НАТО, стійкість тилу, захист критичної інфраструктури в умовах війни

Продовження таблиці 2.10

1	2	3	4	5
2021	Стратегія економічної безпеки України на період до 2025 року (Указ Президента №347/2021 від 11.08.2021)	Стратегія	Визначення загроз економічній безпеці (зовнішніх і внутрішніх), пріоритетів структурних реформ, зменшення критичних залежностей, посилення фінансової стійкості, розвитку промислового та інноваційного потенціалу	Економічна стійкість як основа НБ, диверсифікація ринків і постачань, енергетична безпека, зменшення тіньової економіки, підтримка критичних галузей, інтеграція в європейський економічний простір
2021	Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» (Указ Президента №447/2021 від 26.08.2021)	Стратегія	Формування цілісної системи кібербезпеки, визначення ролі держави, приватного сектору та суспільства у захисті кіберпростору, протидії кібератакам та гібридним загрозам	Безпечний і стійкий кіберпростір, державно-приватне партнерство, розвиток нац. кіберспроможностей, захист критичної інформаційної інфраструктури, кіберстійкість органів влади, ризикоорієнтований підхід, інтеграція з кіберпростором НАТО та ЄС
2021	Стратегія інформаційної безпеки (Указ Президента №685/2021 від 28.12.2021)	Стратегія	Оновлення підходів до інформаційної безпеки з урахуванням досвіду гібридної війни; визначення актуальних загроз, пріоритетів формування стійкого інформаційного середовища, підтримки медіаграмотності та стратегічних комунікацій	Стійкість суспільства до дезінформації, розвиток стратегічних комунікацій, підтримка незалежних медіа, захист від інформаційних операцій РФ, поєднання безпеки та прав людини, партнерство з громадянським суспільством
2021	Концепція забезпечення національної системи стійкості (Указ Президента №479/2021 від 27.09.2021)	Концепція	Визначає мету, принципи, напрями, механізми та строки формування нац. системи стійкості; окреслює багаторівневу архітектуру (державний, регіональний, місцевий рівні), базові елементи (інституції, критична інфраструктура, суспільство, економіка) та цикл управління ризиками	Комплексність, широка взаємодія, передбачуваність, надійність, обізнаність, готовність, мобільність, адаптивність, наявність резервів, безперервність, субсидіарність; стійкість як здатність системи «витримувати, адаптуватися і відновлюватися»
2017–2024	Стратегічні та програмні документи, розроблені на виконання Стратегії нац. безпеки (секторальні стратегії, плани реалізації, документи оборонного планування)	Стратегії, плани	Імплементація базової Стратегії нац. безпеки в окремих секторах: оборона, правоохоронна діяльність, цивільний захист, енергетична безпека, розвиток сил оборони, взаємосумісність з НАТО	Узгодженість з тріадою «стримування – стійкість – взаємодія», розвиток спроможностей, всеохоплюючий підхід до оборони, поетапність реформ, цивільний демократичний контроль, посилення інституційної та організаційної стійкості

Джерело: [249-254]; узагальнення автора

Узагальнено, комплекс цих документів формує позитивно

регламентуючу нормативну рамку, у межах якої відбувається раціоналізація сектору безпеки та публічного управління: від зміцнення воєнної й економічної складових до побудови стійкого інформаційного й кіберпростору, а також запровадження власне національної системи стійкості як інтегруючої надсистеми державного управління. Усі стратегії та концепції послідовно відтворюють спільні принципи – людиноцентричність, пріоритет верховенства права, демократичну підзвітність, багаторівневе управління, партнерство з ЄС і НАТО, ризикоорієнтованість та стійкість, які й задають орієнтири для подальшого розвитку Національної моделі стійкості в умовах тривалої безпекової кризи.

2.4. Особливості застосування функціонального підходу у дослідженні механізмів національної стійкості в умовах цифрового суспільства

У сучасних умовах, коли Україна розбудовує власну систему безпеки й публічного управління під тиском тривалої війни та глибоких трансформацій, поняття стійкості виходить далеко за межі суто технічної або вузькосекторальної категорії. На основі чинних законодавчих і стратегічних документів, а також з урахуванням реалій цифрового суспільства, доцільно запропонувати авторське, узагальнене бачення чотирьох пов'язаних між собою понять: «стійкість», «національна стійкість», «національна система стійкості» та «національна модель стійкості».

Отже, під стійкістю доцільно розуміти інтегральну властивість будь-якої системи – державного органу, інституту, громади, підприємства, критичного об'єкта інфраструктури, навіть спільноти людей – зберігати керованість і ключові функції в умовах дії загроз і криз, адаптуватися до змін середовища та своєчасно відновлюватися після стресових подій, мінімізуючи довгострокові негативні наслідки. У класичному розумінні це включає здатність витримувати негативні (і позитивні, в окремих випадках) впливи, підтримувати безперервність необхідних процесів, змінювати процедури,

структури й розподіл ресурсів, а також повертатися до прийнятного або оновленого, вищого рівня функціонування. У цифровому суспільстві цей зміст неминуче доповнюється виміром цифрової спроможності. Сьогодні практично будь-яка організація є цифрово опосередкованою: управління, облік, комунікації, фінансові операції, логістика, надання послуг відбуваються через ІТ-системи, платформи та мережі. Відповідно, стійкість означає не лише наявність підготовленого персоналу, налагоджених процедур і матеріальних резервів, а й здатність підтримувати та відновлювати ключові цифрові сервіси – резервне копіювання, дублювання даних, альтернативні канали зв'язку, базовий рівень кіберзахисту, достатній рівень цифрових навичок працівників, готовність до роботи в умовах часткового або тимчасового руйнування цифрової інфраструктури. Класична вимога «зберігати керованість» тут означає також збереження цифрової керованості: можливості ухвалювати рішення й реалізовувати їх попри збої у зв'язку, кібератаки чи відмову ІТ-сервісів.

Національна стійкість є похідною від цього загального поняття, але стосується вже не окремих організацій, а цілісної конфігурації «держава – суспільство – економіка – критична інфраструктура – територіальні громади». Національну стійкість варто визначити як здатність держави й суспільства в цілому – політичних інститутів, сектора безпеки й оборони, економічної системи, критичної (включно з цифровою) інфраструктури, інститутів громадянського суспільства, приватного сектору та громадян – спільно протистояти комплексним загрозам, зберігати керованість країни, забезпечувати базову безпеку людей і доступ до життєво важливих послуг, адаптуватися до тривалих криз і відновлюватися на вищому або принаймні прийнятному рівні функціонування. Вона охоплює військові, безпекові, політичні, економічні, соціальні, інформаційні, кібернетичні та інші виміри, спирається на багаторівневе управління (національний, регіональний, місцевий рівні) та передбачає активну взаємодію держави, органів місцевого самоврядування, бізнесу, громадянського суспільства й окремих громадян. У

стратегічних документах це узагальнюється тріадою «стримування – стійкість – взаємодія», де стійкість стає не просто наслідком оборонних зусиль, а окремою стратегічною засадою політики безпеки.

У цифрову епоху національна стійкість дедалі більше залежить від функціонування розгалуженої цифрової екосистеми. Загрози стають мережевими, транскордонними, часто невидимими. Це кібератаки, інформаційно-психологічні операції, маніпулювання алгоритмами соціальних мереж, залежність від зовнішніх хмарних сервісів, глобальних технологічних платформ і платіжних інфраструктур. До кола фактичних носіїв національної стійкості входять не лише органи державної влади чи військові структури, а й великі ІТ-компанії, оператори мобільного зв'язку, інтернет-провайдери, банки, платіжні системи, логістичні та комунікаційні платформи, які іноді перебувають поза юрисдикцією однієї держави. Рівень національної стійкості визначається також цифровими компетентностями населення – вмінням розпізнавати дезінформацію, користуватися електронними послугами в умовах кризи, мінімізувати власні цифрові уразливості. Тому національна стійкість у цифровому макросередовищі – це здатність широкої, багаторівневої, людиноцентричної й мережевої системи протистояти постійним цифровим впливам, зберігати цілісність і керованість країни, не втрачаючи при цьому свобод і прав людини. Якщо національна стійкість описує властивість системи в цілому, то національна система стійкості (НСС) – це її інституціонально й нормативно оформлена «архітектура».

Концепція забезпечення національної системи стійкості [232] визначає національну систему стійкості як комплекс цілеспрямованих дій, методів та механізмів взаємодії органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, інститутів громадянського суспільства, які гарантують збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після настання кризової ситуації.

Національна стійкість – здатність держави і суспільства ефективно протистояти загрозам будь-якого походження і характеру, адаптуватися до змін безпекового середовища, підтримувати стає функціонування, швидко відновлюватися до бажаної рівноваги після кризових ситуацій [232].

Разом з тим, вважаємо, що доцільно розглядати національну систему стійкості (НСС) з позицій суб'єктного підходу, й визначити як *комплекс суб'єктів, механізмів, процедур і ресурсів, за допомогою яких держава, органи місцевого самоврядування, сектор безпеки й оборони, бізнес, громадянське суспільство та громадяни координовано здійснюють виявлення загроз і вразливостей, оцінювання ризиків, планування, підготовку, реагування й відновлення, забезпечуючи реалізацію національної стійкості на державному, регіональному та локальному рівнях*. Це вже не абстракція, а сукупність функціонування конкретних інститутів і процесів – органи координації на національному рівні (РНБО, КМУ, спеціалізовані міжвідомчі структури), уповноважені органи на регіональному й місцевому рівнях, нормативно-правова база (закони, стратегії, концепції, плани), процедури кризового менеджменту, системи моніторингу загроз та оцінювання спроможностей, канали обміну інформацією, механізми взаємодії з приватним сектором і громадськістю.

У цифровому суспільстві НСС неминуче набуває вигляду не лише організаційної мережі, а й цифрової інфраструктури управління ризиками та стійкістю. Реалізація базових функцій системи – ідентифікації загроз, оцінки ризиків, планування превентивних заходів, координації під час криз і відновлення – передбачає наявність інтегрованих інформаційних платформ: національних і регіональних реєстрів загроз та ризиків, систем ситуаційної обізнаності, аналітичних панелей для ухвалення рішень, захищених комунікаційних каналів для суб'єктів стійкості. НСС повинна спиратися на аналітику великих даних, інструменти кіберрозвідки та реагування на інциденти, механізми управління цифровими ланцюгами постачання, а також на правила взаємодії з глобальними технологічними гравцями. Це, у свою

чергу, вимагає доповнення класичних принципів стійкості (комплексність, передбачуваність, готовність, адаптивність, субсидіарність, безперервність, широка взаємодія) цифровими принципами – інтероперабельності даних, побудови безпеки й захисту приватності «за замовчуванням» і «за дизайном», розумного поєднання відкритості даних з вимогами безпеки.

Національна модель стійкості (НМС) – це концептуальне й аналітичне відображення того, як саме в конкретній державі, у реальних історичних і політичних умовах взаємодіють інституції, норми, процеси, ресурси та практики забезпечення стійкості на всіх рівнях управління. Якщо НСС – це нормативно задумана архітектура (схема того, як система має бути влаштована), то НМС – це рамка, яка одночасно описує бажаний стан (як «має бути») і фактичне функціонування (як «є насправді»), фіксує логіку розподілу повноважень, баланс централізації й децентралізації, формати взаємодії цивільного та військового компонентів, особливості управління ризиками, канали відновлення й розвитку.

У цифровому макросередовищі НМС повинна враховувати, що вузлами влади та вразливості стають не лише класичні державні інституції (парламент, уряд, суди, силові відомства, місцеве самоврядування), а й цифрові мережі та платформи: соціальні мережі, месенджери, платіжні й логістичні сервіси, глобальні та національні хмарні платформи, електронні сервіси держави, комерційні інформаційні ресурси. Вона має описувати, яким чином рішення, ухвалені політичними та адміністративними центрами, реалізуються й модифікуються в цифровому просторі; як алгоритми рекомендацій, модераційні практики приватних платформ, міжнародні стандарти кібербезпеки впливають на національну безпеку та суспільну стійкість; яким є реальний баланс між централізованими державними цифровими сервісами та децентралізованими ініціативами громад, бізнесу, волонтерських і експертних спільнот.

НМС є комплексним, багатовимірним концептом, який відображає здатність держави, суспільства та економіки адаптуватися до динамічних

змін і протистояти різнотипним викликам – від військових і гібридних до екологічних, технологічних та гуманітарних. Основними складниками цієї моделі визначено: інституційну спроможність, що детермінує ефективність державних структур у прогнозуванні, запобіганні, реагуванні та відновленні після криз; соціальну згуртованість, яка забезпечує довіру, солідарність і готовність громадян брати участь у спільних діях, підтримувати державні інститути й протидіяти дезінформації; економічну стабільність, що передбачає диверсифікацію економіки, раціональне використання ресурсів, стійкість до шоків і підтримку сталого розвитку; технологічну адаптивність, яка включає сприйнятливості до інновацій, цифрову трансформацію управлінських процесів, розвиток цифрових компетентностей та захищену цифрову інфраструктуру; національно-культурну стійкість і ментальну резильєнтність, які охоплюють систему цінностей, ідентичність, історичну пам'ять і здатність суспільства зберігати єдність та суб'єктність в умовах зовнішнього тиску й інформаційно-психологічних операцій.

НМС, з одного боку, спирається на комплекс стратегічних і концептуальних документів (Стратегію національної безпеки, стратегії воєнної, економічної, кібер- та інформаційної безпеки, Концепцію забезпечення національної системи стійкості), а з іншого – наповнюється змістом через практики управління в умовах війни й криз. У цифровому суспільстві вона стає, по суті, моделлю цифрово-інституційної стійкості: описує, як інститути, норми й процедури взаємодіють із цифровими мережами й платформами, як змінюється конфігурація влади, де виникають нові вразливості й нові джерела стійкості, якою є роль глобальних технологічних гравців у національній безпеці, як громадяни та громади використовують цифрові інструменти для самоорганізації, опору, відновлення й розвитку.

Таким чином, уявлення про стійкість, національну стійкість, національну систему стійкості та національну модель стійкості в сучасних українських умовах невіддільні від контексту цифрового суспільства.

Цифрове середовище перестає бути «однією з галузей» і перетворюється на середовище, в якому розгортаються всі без винятку процеси – від ухвалення державних рішень до повсякденної поведінки громадян, від роботи критичної інфраструктури до інформаційних кампаній. Саме в цьому середовищі й має реалізовуватися національна стійкість: як здатність не лише витримувати удари та відновлюватися, а й навчатися, накопичувати досвід, підвищувати якість управління й рівень свободи людини попри тривалі й багатовимірні загрози.

Концепція забезпечення національної системи стійкості [232], яка розглядається як один із базових нормативних документів у нашому дослідженні, фіксує не стільки вже сформовану систему, скільки цільовий, проєктний образ Національної моделі стійкості. Вона задає рамкові уявлення про те, що в українських умовах означає «стійка держава», на яких принципах має базуватися її функціонування в умовах багатовимірних загроз, якими є ключові суб'єкти та які сфери життєдіяльності мають бути охоплені, аби можна було говорити не про випадкове виживання, а про свідомо вибудовану здатність протистояти ударам, адаптуватися до нових умов і відновлюватися [232]. У нашій аналітичній аналітичній концепції НМС затверджена Концепція постає як вихідна нормативна матриця, крізь яку інтерпретується подальший розвиток практик публічного управління в умовах російської агресії та режиму воєнного стану, й водночас як «лакмусовий папірець» тих структурних розривів, суперечностей і прогалин, які у воєнних реаліях виявилися особливо загостреними.

У змістовній частині Концепція пропонує чітке розрізнення між трьома рівнями, які в сукупності утворюють зміст національної стійкості: системним, інституційним та організаційним. На найвищому рівні стійкість трактується як здатність держави і суспільства в цілому протистояти загрозам різного походження, підтримувати критично важливі функції навіть за умов кризових ситуацій, адаптуватися до мінливої безпекової реальності й повертатися до бажаного стану рівноваги або трансформувати його з

урахуванням нових викликів. Це визначення важливе тим, що виходить далеко за межі вузько безпекового, військового або секторального бачення: стійкість постає як інтегральна характеристика конфігурації «держава – суспільство – економіка – критична інфраструктура – локальні громади» [232]. На наступному, системному рівні вводиться поняття національної системи стійкості як комплексу дій, інструментів, процедур і механізмів взаємодії, за допомогою яких різні суб'єкти – органи державної влади, органи місцевого самоврядування, бізнес, громадські об'єднання, окремі громадяни – спільно забезпечують безпеку та безперервність функціонування базових сфер життєдіяльності до кризи, у ході її розгортання та після виходу з неї. Ідеться не про формальну сукупність інституцій, а про певну узгоджену конфігурацію процесів: ідентифікації загроз і вразливостей, оцінки ризиків, планування превентивних заходів, готовності до реагування, організації відновлення, повернення до нормального стану або переходу до нового рівня функціонування. Нарешті, на організаційному рівні стійкість пов'язується зі спроможністю конкретних інституцій – міністерств, інших державних органів, підприємств, організацій, установ – готуватися до криз, підтримувати працездатність у стресових умовах, адаптувати процедури, структури, кадровий склад і технологічні рішення для того, щоб не допустити управлінського паралічу чи неконтрольованого колапсу ключових функцій.

У межах нашої дослідницької методології така трирівнева конструкція дозволяє одночасно працювати з різними масштабами аналізу: від макрорівня архітектури публічного управління та взаємодії держави із суспільством до мезорівня секторальних систем (безпека, енергетика, транспорт, соціальна сфера) й мікрорівня окремих організацій, їхніх процедур, цифрових рішень та управлінських практик. Саме через таке поєднання стає можливим побачити, як абстрактні норми та принципи, зафіксовані в Концепції, втілюються або, навпаки, розходяться з реальними управлінськими конфігураціями періоду повномасштабної війни.

Однією з центральних аналітичних цінностей Концепції національної системи стійкості (НСС) є те, що вона детально фіксує вихідні умови, в яких відбувається становлення національної системи стійкості: системна, цілісна архітектура НСС де-факто відсутня, натомість наявні фрагментовані, часто неузгоджені між собою механізми кризового реагування, цивільного захисту, секторальної безпеки, міжнародного співробітництва. В інституційному вимірі підкреслюється: не існує органу, що мав би чітко визначений мандат щодо координації політики стійкості, управління ризиками та узгодження дій державних і недержавних акторів; відсутні національний реєстр ризиків і єдина методика їх оцінювання; кризовий менеджмент не має чітко формалізованої, апробованої структури; резервні пункти управління морально та технологічно застарілі; більшість органів влади обмежено готові підтримувати функціонування базових елементів стійкості в умовах довготривалих і комплексних криз. Інакше кажучи, ще до повномасштабної агресії система перебувала у стані становлення, коли окремі «острівці» спроможностей не були інтегровані в єдине поле управління ризиками та стійкістю. На методологічному рівні додатково підкреслюється відсутність загальних стандартів оцінки загроз та вразливостей, єдиного підходу до вимірювання спроможностей, фрагментованість підходів до кібербезпеки та інформаційної безпеки, що в сукупності підриває передбачуваність і керованість системи в умовах інформаційно-кібернетичних атак. Комунікаційний вимір проблеми проявляється в низькому рівні довіри до органів влади, слабкій залученості громадян до підготовки до криз, недостатньому розвитку горизонтальних зв'язків між державою, бізнесом та громадянським суспільством, а також у недостатньому рівні міжнародної кооперації саме в площині стійкості. Для нашого дослідження цей опис вихідного стану є принциповим, адже НМС формується не як еволюція зрілої, відпрацьованої структури, а як спроба створити цілісну систему в умовах уже наявної багатовимірної агресії й довготривалої реформної турбулентності і турборежимів, які самі по собі є викликами для

національної стійкості. Це означає, що багато практик публічного управління, які ми аналізуємо, виникають як відповіді на структурні прогалини, а не як реалізація заздалегідь продуманого плану розвитку країни.

Окрема змістовна лінія Концепції пов'язана з поняттям «базових елементів» національної системи стійкості. Вони описуються як ключові блоки, без підтримки яких будь-які декларації щодо стійкості залишаються порожніми. Йдеться про інституційну спроможність і стійкість органів державної влади, захищеність критичної інфраструктури (енергетичної, транспортної, водної, продовольчої, інформаційно-комунікаційної, медичної тощо), функціональність єдиної державної системи цивільного захисту, здатність держави реагувати на масові переміщення людей, суспільну стійкість до інформаційних впливів, фінансово-економічну стійкість та безперервність бізнес-процесів. Для нашого дослідження цей перелік є важливим, по-перше, як нормативно зафіксований «мінімальний набір» напрямів, за якими має здійснюватися аналіз стійкості; по-друге, як відкрита конструкція, яка за задумом Концепції може розширюватися й уточнюватися в міру зміни безпекового середовища. Саме з цієї точки зору ми розглядаємо, як в умовах воєнного стану у цей перелік фактично інтегруються нові виміри – зокрема, цифрова інфраструктура, взаємодія оборонно-безпекового сектору з приватними технологічними компаніями, транснаціональні канали матеріальної й інформаційної підтримки. Базові елементи, окреслені Концепцією, стають у нашій моделі своєрідною «рамкою спостереження», всередині якої виявляються як сторони, де система продемонструвала вражаючу адаптивність, так і ті поля, де інституційні слабкості створили додаткові загрози для виживання та відновлення.

У розділі, присвяченому принципам національної системи стійкості, Концепція пропонує перелік нормативних орієнтирів, які в нашому дослідженні ми переосмислюємо як операційні критерії оцінки фактичних практик. Принцип комплексності вимагає розглядати загрози не ізольовано, а в їхньому взаємозв'язку й кумулятивному ефекті, тобто визнавати, що

одночасне поєднання військових, енергетичних, кібернетичних, інформаційних і соціально-економічних ударів створює якісно нову конфігурацію ризиків, до якої традиційні, секторальні системи безпеки не були готові. Принцип широкої взаємодії підкреслює, що держава сама по собі не здатна забезпечити стійкість: потрібна включеність органів місцевого самоврядування, бізнесу, громадянського суспільства, експертних спільнот і міжнародних партнерів. Він прямо співвідноситься з нашими спостереженнями щодо ролі волонтерського руху, IT-спільноти, місцевих бізнес-мереж, які виявилися критично важливими для підтримання функціональності системи під час перших місяців повномасштабного вторгнення.

Принцип передбачуваності орієнтує на системне виявлення й оцінку ризиків; на практиці ми бачимо, що саме нестача належної аналітичної інфраструктури та єдиних методик до 2022 року обмежувала спроможність держави завчасно моделювати сценарії комбінованих загроз. Принципи надійності, обізнаності, готовності й мобільності у нашій оптиці постають як взаємопов'язані компоненти інституційної та організаційної стійкості: вони включають кадрову підготовку, наявність процедур, здатність швидко розгортати резервні потужності, а також культуру кризового управління, що значною мірою формується через навчання, симуляції, міжвідомчі тренування. Особливої ваги у воєнний період набувають принципи адаптивності й безперервності: саме здатність швидко змінювати формальні структури, перерозподіляти повноваження, переосмислювати стандарти надання послуг, переходити на дистанційні чи цифрові формати взаємодії дозволила уникнути системного колапсу у сферах фінансів, соціальних виплат, освіти, охорони здоров'я в умовах масованих атак. Нарешті, принцип субсидіарності, тобто ухвалення рішень на найнижчому можливому рівні за умови належної координації з вищими рівнями, прямо резонує з аналізованою нами інтегрованою цивільно-військовою моделлю управління під час воєнного стану: там, де цей принцип працював, громади отримували

простір для власних рішень без руйнування загальнонаціональної логіки оборони; там, де він порушувався, виникали конфлікти юрисдикцій, затримки в реагуванні або відчуження населення від рішень центральної влади.

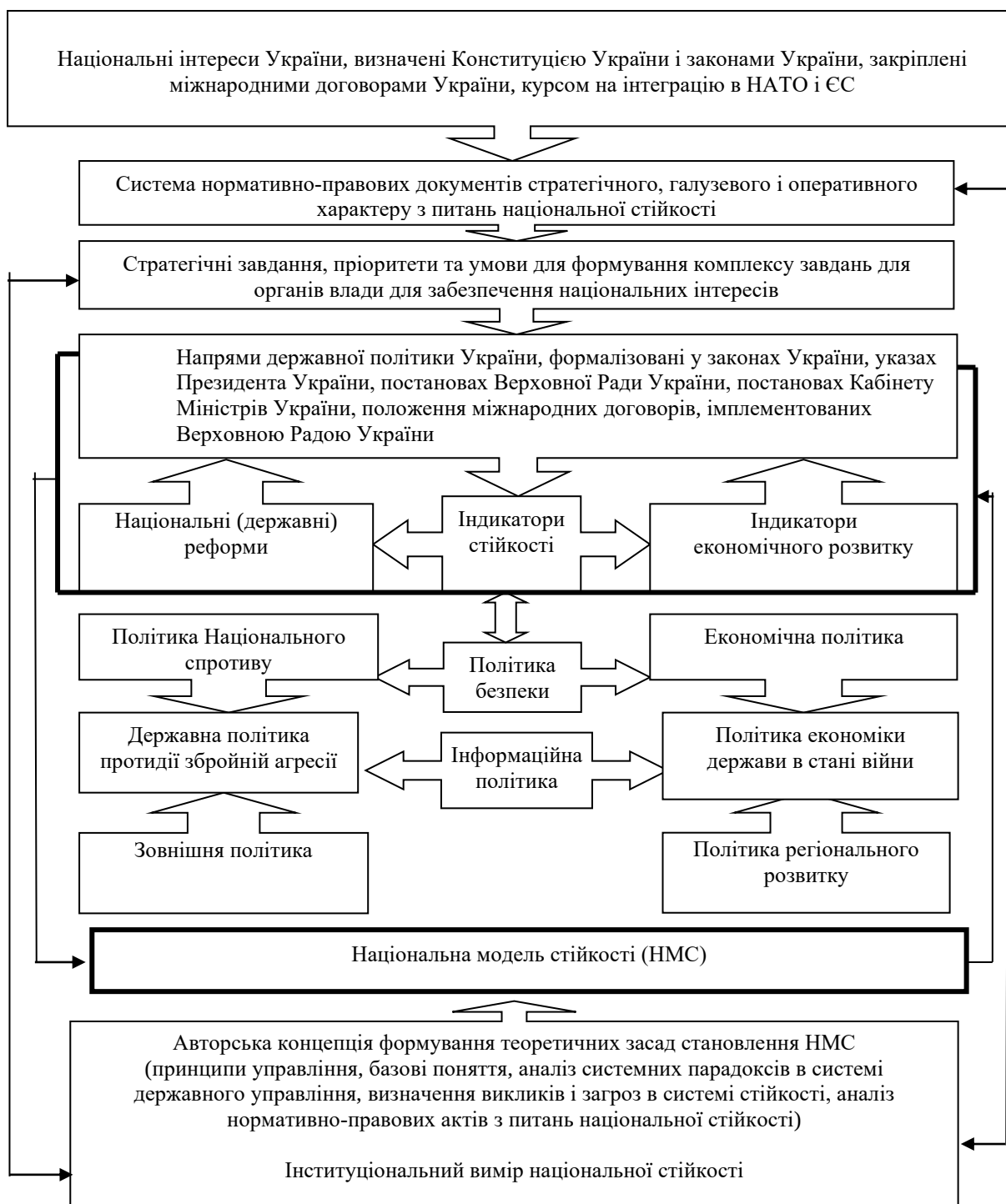


Рис. 2.4. Методологічна рамка формування НМС

Джерело: дослідження автора

Концепція містить також контур інституційної архітектури НСС, яку в межах нашого дослідження варто трактувати як спробу визначити «ядро» національної моделі стійкості та його зв'язок із периферійними, але необхідними елементами. На національному рівні таке ядро утворюють РНБО як центр координації в питаннях безпеки і стійкості, спеціальні урядові координаційні органи, національний координатор співробітництва з НАТО у сфері стійкості, міжвідомчі координаційні структури та аналітично-експертні мережі. На регіональному та місцевому рівнях передбачається створення міжвідомчих структур безпеки та стійкості при місцевих державах адміністраціях, розгортання регіональних аналітичних центрів, активне залучення органів місцевого самоврядування, підприємств, громадських організацій.

Для нас важливо, що ця схема (рис.2.4), хоч і є дескриптивною, задає ідею мережевого, багатосуб'єктного управління стійкістю, де вертикальні владні відносини мають поєднуватися з горизонтальними зв'язками, а експертне середовище – відігравати роль каналу, через який до політичних рішень потрапляє складна, багатовимірна інформація про ризики та спроможності. У реальності воєнного періоду частина цих задумів реалізується через воєнні та військові адміністрації, частина – через посилену роль РНБО України, частина – через ad hoc створені координаційні механізми. Наше дослідження дозволяє оцінити, де ця інституційна проєкція справді набула рис функціональної системи, а де залишилася радше декларативним наміром.

Нарешті, ключовим для методологічного виміру нашого дослідження є те, що Концепція пропонує не лише перелік принципів та інститутів, а й чітко окреслює цикл управління ризиками та кризами як каркас майбутньої НМС. Йдеться про послідовність взаємопов'язаних кроків: виявлення загроз, ідентифікація вразливостей, побудова національних та регіональних реєстрів ризиків, регулярне оцінювання поточних і прогнозованих ризиків, періодичне оцінювання спроможностей, планування заходів запобігання,

готовності, реагування та відновлення, розроблення уніфікованих алгоритмів дій на різних рівнях влади, інституціоналізація кризового менеджменту.

У нашій дослідницькій методології ці елементи трансформуються в послідовність аналітичних процедур: від формування корпусу документів і реконструкції нормативної рамки – до виявлення реальних конфігурацій ризиків, вимірювання інституційних спроможностей, опису практик взаємодії між акторами, оцінки здатності системи до адаптації та відновлення. Реальність правового режиму воєнного стану, непередбачувані удари по критичній інфраструктурі, масові переміщення населення, кібератаки, інформаційні кампанії стали своєрідною «дослідницькою лабораторією», де можна перевірити, наскільки концептуально задуманий цикл управління ризиками втілюється в управлінській практиці.

Узагальнюючи, слід визначити, що Національна система стійкості в редакції Концепції є нормативною проєкцією тієї Національної моделі стійкості, яку наше дослідження намагається реконструювати в її реальному, емпіричному вимірі. З одного боку, Концепція задає понятійний ряд, через який можна описувати та порівнювати різні управлінські конфігурації – вводить поняття стійкості, спроможностей, ризиків, багаторівневої архітектури, базових елементів, принципів. З іншого боку, вона фіксує структурні обмеження стартового періоду: розмитість інституційної відповідальності, відсутність координаційних центрів, методологічні прогалини, слабкість каналів взаємодії з суспільством. Для аналізу трансформацій публічного управління в умовах воєнного стану цей подвійний статус Концепції – ідеальної моделі та реєстру проблем – є фундаментальним, адже він дозволяє не обмежуватися описом того, що робиться «де-факто», а постійно співвідносити наявні практики з тим, «як мало б бути» за власною ж логікою української держави. Саме в цьому напруженні між нормативним образом і фактичним станом і розкривається глибинна динаміка національної стійкості: десь система виявляється здатною діяти значно більш гнучко й ефективно, ніж це передбачалося

документацією, де, навпаки, залишається полоненою інерцією, централізму, недовіри й не здатна повною мірою реалізувати власний потенціал.

Саме тому важливо сформулювати основні напрями розвитку НМС у площині цифрової трансформації як розвиток авторської методології НМС:

- 1) цифровізація державного управління на основі розвитку електронного урядування;
- 2) створення Національного реєстру загроз як інтегрованої цифрової платформи для систематизації ризиків, агрегування даних з усіх секторів безпеки та оперативного прийняття рішень щодо реагування, що посилює превентивний потенціал НМС;
- 3) інтеграція публічно-приватного партнерства в процеси цифровізації державного управління, що забезпечує залучення інвестицій, технологічних інновацій і управлінських практик бізнесу для розроблення та впровадження рішень, орієнтованих на результат і ефективність;
- 4) розвиток електронного урядування та мобільних платформ як інструментів спрощення доступу до державних послуг, підвищення їх якості, прозорості й клієнтоорієнтованості органів публічної влади;
- 5) адаптація цифрових технологій до локальних умов, що передбачає урахування територіальних відмінностей у рівні інфраструктурного розвитку, цифрових компетентностей населення, безпекових ризиків і соціальної структури, що є критично важливим для успішної імплементації інновацій у державному секторі;
- 6) впровадження механізмів управління даними в державному секторі (data governance) з урахуванням вимог захисту персональних даних, кібербезпеки та етичного використання інформації, що забезпечує баланс між прозорістю, відкритістю даних і захистом приватності та підвищує довіру громадян до інституцій влади;
- 7) формування інтегрованої системи стійкості на основі сучасних підходів до управління загрозами (risk management, resilience management, системи раннього попередження), що дає змогу державі переходити від

реактивних практик до проактивного й превентивного управління кризами;

8) постійне коригування національних стратегій у сфері цифровізації, резильєнтності, кібербезпеки та секторальних політик із урахуванням динаміки безпекового середовища, технологічних трендів і досвіду реалізації попередніх програм.

При цьому важливо вказати на визначальну роль правового компонента у формуванні та розвитку Національної моделі стійкості (НМС), адже саме право задає «правила гри» для всіх учасників системи – держави, органів місцевого самоврядування, сектора безпеки й оборони, бізнесу, громадянського суспільства та громадян. Ми вказали у межах розділів 1 та 2 на особливості парадигмального підходу до нормативного змісту НМС.

Право в цьому контексті доцільно розглядати не як один із багатьох елементів, а як платформу моделі стійкості, яка встановлює рамки допустимих дій, закріплює механізми розподілу повноважень, відповідальності й контролю та формує передбачуване середовище для управління ризиками й подолання криз. Без чітко окресленого, внутрішньо узгодженого правового поля НМС неминуче перетворюється або на сукупність ситуативних управлінських рішень, або на нерівномірний набір відомих практик, що суперечать одна одній.

По-перше, право виконує функцію конституційно-правового ствердження НМС. Йдеться про те, що саме конституційні норми та базове галузеве законодавство визначають суб'єктний склад системи стійкості, їхні компетенції, форми взаємодії й обмеження влади. У межах сталого конституційного режиму фіксується розподіл влад, засади місцевого самоврядування, механізми демократичного контролю та гарантії прав і свобод людини – усе це задає каркас, усередині якого можлива побудова стійкої моделі публічного управління. Національна модель стійкості, що претендує на довгостроковість та легітимність, не може спиратися лише на підзаконні акти чи відомчі інструкції; вона має бути «вписана» в систему верховенства права, де будь-яке розширення повноважень чи запровадження

надзвичайних процедур супроводжується чіткими матеріальними й процесуальними запобіжниками.

По-друге, право в НМС задає рамки допустимих дій держави та інших суб'єктів у кризових ситуаціях. Мова не лише про регулювання стану війни чи надзвичайного стану, а й про ширший спектр спеціальних правових режимів – у сфері цивільного захисту, протидії тероризму, кібербезпеки, захисту критичної інфраструктури, інформаційної безпеки, публічного здоров'я тощо. Саме правові норми визначають, які повноваження можуть бути тимчасово розширені, які права – обмежені, за яких умов, на який строк і якими органами, а також які механізми контролю та відповідальності супроводжують такі рішення. Від того, наскільки детально й збалансовано виписані ці рамки, залежить, чи перетворюватиметься стійкість на виправдання свавільного втручання в права людини, чи навпаки – стане засобом їх ефективного захисту в умовах загрози.

По-третє, право визначає архітектуру розподілу повноважень, відповідальності та контролю всередині НМС. Стратегічні документи у сфері національної, воєнної, економічної, інформаційної й кібербезпеки, а також Концепція забезпечення національної системи стійкості закріплюють логіку багаторівневого управління: держава формує загальнонаціональні стандарти й методики, регіони та громади адаптують їх до своїх особливостей, а спеціалізовані органи координують зусилля та здійснюють моніторинг реалізації. Однак така модель стає реально дієвою лише тоді, коли правові норми чітко визначають, хто саме за що відповідає: який орган веде національний реєстр загроз і ризиків, хто формує регіональні реєстри, які процедури подання та оновлення інформації, які інструменти впливу має центр у випадку невиконання вимог на місцях, які права наділяються органам місцевого самоврядування для самостійного реагування на загрози. Розмитість або дублювання повноважень у цій царині безпосередньо підривають стійкість, оскільки в момент кризи породжують управлінський параліч, конфлікти юрисдикцій і втрату часу.

По-четверте, правовий компонент забезпечує інституціоналізацію ризикоорієнтованого підходу як ключового принципу НМС. Стратегічні акти, що розвивають положення Закону про національну безпеку, фіксують необхідність систематичного виявлення загроз, оцінювання вразливостей, формування національного та регіональних реєстрів ризиків, регулярної оцінки спроможності протидії. Проте сам факт фіксації цих завдань у стратегіях ще не гарантує їх виконання. Потрібні конкретні нормативні приписи, які зобов'язують органи влади здійснювати певні дії у визначені строки, застосовувати уніфіковані методики оцінювання, готувати звіти з чітко окресленим змістом та процедурою погодження, а також передбачають відповідальність за невиконання цих зобов'язань. Лише за таких умов ризикоорієнтованість перестає бути політичною декларацією й стає юридичним обов'язком, інтегрованим у повсякденну управлінську практику.

По-п'яте, право виконує захисну функцію в НМС, забезпечуючи баланс між вимогами безпеки й гарантіями прав людини, між потребою оперативних рішень і приписами демократичної підзвітності. У НМС, що розгортається в умовах воєнного стану й тривалої безпекової кризи (мілітарі-НМС), особливо актуальним є питання меж розширення повноважень виконавчої влади, застосування військових інструментів у цивільному житті, обмеження свободи слова та інформації, втручання в приватне життя й економічну діяльність. Правові норми мають не лише дозволяти вживати жорсткі заходи за певних обставин, а й містити процедури їх перегляду, скасування, оскарження, а також механізми парламентського, судового та громадського контролю. Це критично важливо для того, щоб НМС не перетворилася на модель «фортеці в облозі», де стійкість до зовнішніх загроз досягається ціною руйнування внутрішньої легітимності та довіри суспільства до держави.

По-шосте, правовий компонент стає каналом інтеграції міжнародних стандартів і зобов'язань у національну модель стійкості. Орієнтація на членство в ЄС і НАТО означає не лише політичний вибір, а й необхідність

приведення національного законодавства у відповідність до *acquis* ЄС, стандартів НАТО у сфері планування на випадок надзвичайних ситуацій, захисту критичної інфраструктури, кібербезпеки, цивільної готовності та взаємодії цивільних і військових структур. Право в цьому сенсі виступає механізмом «вшивання» міжнародних зобов'язань у тканину національної НМС: через адаптацію законів, імплементацію директив і регламентів, укладення міжнародних договорів, інституціоналізацію спільних механізмів планування та реагування.

По-сьоме, важливо підкреслити роль права у формуванні передбачуваного середовища для цифрового простору, який став не лише сферою комунікації, а й критичною інфраструктурою функціонування НМС. Нормативне регулювання кібербезпеки, захисту інформаційних систем, персональних даних, електронного урядування, цифрових публічних послуг, діяльності платформ та провайдерів має визначальне значення для того, чи буде цифровий простір посилювати національну стійкість, чи, навпаки, створюватиме нові уразливості. Правові норми тут повинні враховувати специфіку транскордонності цифрових загроз, асиметрію між державою та глобальними технологічними компаніями, необхідність поєднання інноваційності з безпекою, а також залучення приватного сектору як повноцінного суб'єкта НМС. Відсутність або фрагментарність таких норм призводить до правової невизначеності, де ключові рішення ухвалюються поза прозорими процедурами, а отже, поза полем демократичної підзвітності.

По-восьме, правовий компонент НМС визначає участь громад та громадян у забезпеченні стійкості. Йдеться не лише про формальну можливість залучення громадськості до обговорення стратегічних документів чи планів, а й про закріплені в праві механізми участі в кризових ситуаціях: волонтерська діяльність, місцеві ініціативи з підвищення готовності, громадський контроль за використанням ресурсів, подання інформації про загрози, участь у навчаннях і тренуваннях. Правові норми можуть або обмежувати цю участь до декларативних форм (консультації без

реального впливу), або, навпаки, інституційно вписувати її в НМС через дорадчі органи, публічні звіти, інструменти електронної демократії, відкриті дані, механізми співпраці з волонтерськими й експертними спільнотами. В умовах війни саме громадянська активність часто стає головним ресурсом стійкості; завдання права – не придушувати її, а спрямовувати й інтегрувати в загальнонаціональну архітектуру.

І, нарешті, право задає адаптивний вимір НМС, оскільки воно не є раз і назавжди сталою конструкцією. Нормативна основа національної стійкості має розвиватися в результаті аналізу реального досвіду криз, помилок і успіхів. Кожна велика криза – від пандемії до повномасштабної війни – виявляє прогалини в законодавстві, колізії між різними правовими режимами, неузгодженість повноважень. Спроможна НМС передбачає наявність процедур «зворотного зв'язку», коли за результатами кризових ситуацій проводяться не лише організаційні, а й нормативні ревізії: вносяться зміни до законів, підзаконних актів, стратегій, концепцій. Цей адаптивний вимір особливо важливий у сучасному динамічному середовищі, де загрози швидко змінюють форму – від традиційної військової агресії до складних комбінацій кібероперацій, інформаційних впливів, економічного тиску та технологічних обмежень. Таким чином, правовий компонент у Національній моделі стійкості України виступає не лише як сукупність норм, а як базова платформа, яка: конституює суб'єктів і структури НМС; встановлює рамки допустимих дій і надзвичайних повноважень; закріплює розподіл компетенцій, відповідальності й контролю; інституціоналізує ризикоорієнтований підхід; забезпечує баланс між безпекою та правами людини; інтегрує міжнародні стандарти; формує передбачуване середовище для функціонування цифрового простору; відкриває можливості для участі громад і громадян; створює умови для адаптивного оновлення моделі на основі практичного досвіду.

Важливим напрямом формування засад НМС є інтерпретація її змісту у розрізі Стратегії реформування державного управління на 2022-2025 (далі –

Стратегії). Текст Стратегії не містить понять «стійкість» («сталість», «резильєнтність»), хоча, на нашу думку, сама парадигма реформування має виходити з концептуального змісту стійкості. Така ж особливість притаманна і попередній редакції стратегії [255-256].

Це свідчить про певний концептуальний розрив між безпеково-резильєнтнісним дискурсом, закріпленим у стратегічних документах сектору безпеки й оборони, та баченням трансформації системи публічного управління, яке й далі фокусується переважно на ефективності, результативності й підзвітності у вузько адміністративному вимірі. У такій конфігурації державне управління розглядається радше як «машина з надання послуг» та адміністрування політик, а не як ключовий інституційний каркас національної стійкості, покликаний забезпечувати здатність суспільства витримувати шоки, адаптуватися й трансформуватися. Відсутність чітко артикульованого резильєнтнісного виміру у Стратегії ускладнює інтеграцію її цілей і інструментів з Концепцією забезпечення національної системи стійкості, відсуваючи питання готовності, адаптивності, надлишковості й багаторівневої координації на другий план. У результаті існує ризик, що реформа державного управління відтворюватиме лінійну логіку «оптимізації» та скорочення, замість формування інституцій, здатних діяти в умовах тривалих криз і багатовимірних загроз.

Аналіз окремих нормативних актів з питань оборони, сталого розвитку, безпеки – законів України «Про оборону України», «Про Збройні Сили України, Стратегії сталого розвитку «Україна-2020» [257-259] свідчить, що імператив стійкості не включено до важливих нормативно-правових актів. Але на нашу думку, визначення основних складників НМС як структурного елементу Стратегії реформування державного управління відкриває можливість по-новому осмислити саму логіку модернізації публічної влади в Україні. Адже НМС у цьому контексті перестає бути виключно безпековою чи суто «кризовою» категорією, і постає як інтегральний концепт, що має пронизати всю архітектуру державного управління – від конституційних

засад і організації центральних органів виконавчої влади до роботи конкретних служб на місцевому рівні. Тому включення НМС до нової Стратегії реформування державного управління до 2030 р. вимагає системного підходу, який синхронізує три ключові вектори: критерії вступу до ЄС, вимоги цифрової трансформації та завдання відновлення територіальної цілісності й післявоєнної реконструкції.

Як структурний елемент Стратегії до 2025 р., НМС може бути описана через кілька взаємопов'язаних складників. По-перше, інституційний складник, який визначає, які саме органи й інституції відповідають за формування, реалізацію й координацію політики стійкості – від урядового рівня до територіальних громад. По-друге, нормативно-правовий складник, що фіксує принципи, процедури, механізми розподілу відповідальності та інструменти демократичного контролю. По-третє, функціональний складник, який описує конкретні процеси – прогнозування загроз, управління ризиками, планування готовності, реагування, відновлення та навчання на основі досвіду криз. По-четверте, ресурсний складник, що включає кадрові, фінансові, інформаційні, інфраструктурні та аналітичні ресурси, без яких стійкість залишається декларацією. Нарешті, цифровий та територіальний складники, які відображають, з одного боку, залежність НМС від сучасних технологій та електронного урядування, а з іншого – її вкоріненість у багаторівневій системі управління й нерівномірність спроможностей регіонів та громад.

Інтеграція цих складників у нову Стратегію реформування державного управління до 2030 р. має відбуватися з урахуванням критеріїв вступу до ЄС, які задають «рамку якості» для публічної влади. Європейські принципи публічного управління – професійна, політично нейтральна та стабільна державна служба; верховенство права; підзвітність і прозорість; орієнтація на громадянина та якість публічних послуг; ефективне багаторівневе управління – в українських умовах повинні бути переосмислені крізь призму стійкості. Це означає, що кожен із реформаторських напрямів (реорганізація ЦОВВ,

посилення спроможності урядового центру, зміцнення місцевого самоврядування, реформування державної служби, удосконалення інструментів стратегічного планування й політик) має розглядатися не лише з погляду відповідності європейським стандартам, а й з погляду їхнього внеску в здатність держави й суспільства витримувати кризи, адаптуватися до них і відновлюватися на якісно вищому рівні.

У цьому контексті формування цілісного концепту НМС стає першим і базовим завданням. Йдеться не просто про опис загальної ідеї стійкості, а про створення концептуальної рамки, яка чітко відповідає на кілька ключових питань: що саме вважається об'єктом національної стійкості (інституції, інфраструктури, території, спільноти, окремі особи); хто є суб'єктами забезпечення стійкості; які між ними існують вертикальні й горизонтальні зв'язки; які принципи лежать в основі функціонування цієї системи; як вимірюється стійкість і як оцінюється прогрес у її зміцненні. Така рамка має бути узгоджена з концепцією європейської держави й водночас враховувати специфіку України як країни, що переживає повномасштабну війну, має тимчасово окуповані території й готується до комплексної післявоєнної реконструкції.

Ключовим викликом при формуванні цього концепту є адаптація європейських принципів публічного управління до української системи влади. З одного боку, наявні стандарти (у тому числі розроблені в межах ініціативи SIGMA) пропонують усталену модель «добре керованої держави», де поєднуються верховенство права, ефективні інституції, стабільна професійна бюрократія, участь громадян, прозорість і підзвітність. З іншого – українська система влади має свою історичну спадковість, глибоко вкорінені практики патримоніалізму, політичної фрагментації, неформальних центрів впливу, слабкість середнього управлінського рівня, нерівномірну спроможність органів влади на місцях. Отже, адаптація не може бути просто механічним перенесенням «моделі ЄС»; вона потребує аналізу можливостей, обмежень і ризиків: що реально може бути впроваджено у середньо- й

довгостроковій перспективі; які елементи вимагають поетапної імплементації; де необхідні проміжні, «гібридні» рішення.

Особливо важливим у цьому процесі є усвідомлення того, що НМС повинна не лише відповідати європейським вимогам, а й зміцнювати здатність України діяти в умовах постійної загрози. Наприклад, принцип субсидіарності та багаторівневого управління в ЄС передбачає значне перенесення повноважень і відповідальності на регіональний та місцевий рівні. В українських умовах це поєднується з необхідністю враховувати нерівномірність спроможностей громад, руйнування інфраструктури, різний ступінь безпекових ризиків у прифронтових, деокупованих і відносно безпечніших регіонах. Відповідно, НМС як елемент нової Стратегії до 2030 р. має передбачати диференційовані підходи, які дозволяють, з одного боку, не відмовлятися від принципів децентралізації й наближення послуг до громадян, а з іншого – не перекладати на слабкі місцеві інституції завдання, які вони об'єктивно не здатні виконати без цілеспрямованої підтримки й координації з боку центру.

Другим великим завданням є розроблення методологічної моделі реалізації НМС у контексті концепції «Україна – європейська держава» на основі наявних досліджень у цьому напрямі [260-262]. Така модель повинна описувати, яким чином принципи та цілі НМС інтегруються в цикл публічної політики – від стратегічного планування до оцінки результатів. Методологічна модель передбачає визначення критеріїв і індикаторів стійкості, процедур регулярного моніторингу, механізмів корекції політики на основі отриманих даних. Вона також має враховувати стандарти верховенства права, прав людини, відкритого врядування, прозорості, участі громадян, які є основою європейської концепції держави. Стійкість у такій моделі не може досягатися за рахунок згортання демократичних процесів; навпаки, саме відкритість, підзвітність і залучення суспільства створюють «мережу довіри», без якої неможливо забезпечити цілісну та дієву НМС.

Не менш важливим компонентом методологічної моделі є врахування

вимог цифрової трансформації. Сучасна європейська держава мислиться як держава, що активно використовує цифрові технології для надання послуг, прийняття рішень, взаємодії з громадянами, управління даними. Для НМС це означає, що стійкість стає немислимою без надійних цифрових інфраструктур, інтероперабельних реєстрів, автоматизованих систем моніторингу, кіберзахисту, здатності органів влади працювати в режимі «цифрової безперервності» навіть у кризових умовах. Водночас цифрова трансформація створює нові вразливості – від кібератак на критичні системи до маніпуляцій в інформаційному просторі. Методологічна модель реалізації НМС у новій Стратегії реформування державного управління має одночасно використовувати потенціал цифрових технологій та враховувати пов'язані з ними ризики, інтегруючи до інструментарію управління ризиками окремий блок цифрових загроз.

Третім стратегічним завданням стає теоретичне обґрунтування сучасного дослідницького тренду формування НМС на основі компаративно-адаптаційної парадигми. Ця парадигма виходить з того, що зовнішні (глобальні та європейські) стандарти не можуть бути ані відкинуті, ані просто скопійовані. Вони мають бути сприйняті, критично переосмислені й адаптовані з урахуванням національних особливостей, історичних традицій, політичної культури та реального стану інституцій. У випадку України це означає необхідність порівняння різних європейських моделей побудови стійкості – скандинавської, центральноєвропейської, балтійської, південноєвропейської – з українськими реаліями, виявлення елементів, які можуть бути «перенесені» майже без змін, і тих, які вимагають глибокої модифікації.

Компаративно-адаптаційний підхід дозволяє розглядати НМС не як «копію» західних зразків, а як результат діалогу між глобальними стандартами й національним досвідом [263-267]. Даний підхід підкреслює, що збереження національних особливостей і управлінської культури не є перешкодою для європейської інтеграції, але за умови, що ці особливості проходять через фільтр критичної рефлексії та узгоджуються з ключовими

принципами європейського публічного управління. Такий підхід також відкриває простір для інновацій: Україна, яка вимушена будувати свою модель стійкості в умовах повномасштабної війни та масштабної руйнації, може внести до європейського дискурсу нові рішення – зокрема в сферах цивільно-військової взаємодії, волонтерської мобілізації, цифрового врядування в кризових умовах, відновлення деокупованих територій.

Важливим елементом цієї парадигми є також врахування завдань відновлення територіальної цілісності та післявоєнної реконструкції. НМС, інтегрована в Стратегію реформування державного управління до 2030 р., має містити не лише механізми реагування на поточні виклики, а й інструменти, спрямовані на довгострокове «відбудовування стійкості» [269-273]. Це означає, що процес реконструкції інфраструктури, відновлення економіки, реінтеграції населення деокупованих територій повинен будуватися на принципах «краще, ніж було» (build back better), де нові або відновлені інституції та об'єкти проєктуються з урахуванням майбутніх ризиків, стійкості до можливих атак, здатності продовжувати функціонування в умовах нестабільності. Таким чином, НМС стає не тільки інструментом виживання в кризі, а й рамкою планування розвитку після кризи.

У підсумку, Національна модель стійкості, розглянута як структурний елемент Стратегії реформування державного управління до 2025 р. і водночас як один із центральних модулів нової Стратегії до 2030 р., постає багатовимірною конструкцією. Вона інтегрує європейські критерії якості публічного управління, вимоги цифрової трансформації, завдання відновлення територіальної цілісності й післявоєнної реконструкції, спираючись на компаративно-адаптаційний підхід до використання зовнішніх стандартів. Реалізація окреслених завдань – формування цілісного концепту НМС, розроблення методологічної моделі її впровадження та теоретичне обґрунтування адаптивної парадигми реформ – є необхідною передумовою того, щоб реформа державного управління перестала бути

лише «технічним» процесом інституційних змін і перетворилася на стратегію побудови здатної до стійкого розвитку, демократичної, проєвропейської та, водночас, глибоко вкоріненої в українському суспільстві держави.

Разом з тим, визначальним складником для успішного впровадження НМС є усвідомлення потреби в інтеграції знань, практик і досвіду з різних наук: політології, соціології, економіки, права, психології, культурології та безпеки. Цей підхід дозволяє формувати цілісну картину викликів, з якими стикається країна, і готовність системи управління адекватно на них реагувати. Зокрема, такий підхід демонструє, що управлінські рішення повинні базуватися на різнобічних даних, отриманих з різних джерел і сфери знань, що підвищує ймовірність їхнього успіху. Дослідження в рамках НМС мають зосереджуватися на аналізі легітимності, ефективності та справедливості інституцій, що реалізують державну політику. Таке дослідження сприяє розпізнаванню факторів, що підривають національну стійкість, та ідентифікації механізмів, які можуть підвищити рівень довіри до державних інституцій. Крім того, інтегративний підхід розглядає стійкість не як статичне чи одномірне явище, а як динамічний процес, у якому формуються нові елементи та механізми залежно від змін середовища.

Створення ефективного механізму реалізації НМС не лише модернізує державне управління, але й стає умовою виживання українського суспільства. У рамках цього процесу ключовим є усвідомлення того, що агресія та гібридна війна вимагають адаптації інститутів та процедур, які виправдовують свою ефективність й відповідність постійно змінюваним умовам. Еволюція НМС передбачає формування нових підходів до організації державного управління, які мають включати не лише чинні потреби, а й передбачати потенційні загрози. Важливою метою державної політики стає не тільки реагування на агресію, а й створення інститутів, які здатні спрогнозувати та потенційно запобігти виникненню загроз. Це передбачає гнучкість управлінських структур, ефективне використання сучасних технологій, принципів прозорості та відкритості у веденні

державних справ.

Концептуалізація стійкості в умовах протидії збройній агресії потребує системного аналізу та класифікації існуючих теоретичних підходів до НМС. Для цього необхідно важливим є глибокий моніторинг існуючих моделей стійкості, які вже реалізовані в інших країнах, що опинились у схожих умовах. Очевидно, що визначення інституційних, соціальних, економічних, культурних і безпекових змінних параметрів стане основою для перенесення та адаптації цих досліджень на український контекст. Системний підхід дозволить виявити сильні та слабкі сторони кожного з підходів, а також їхню відповідність реаліям українського суспільства, що суттєво ускладнені війною. Концепція стійкості охоплює ризики, пов'язані з гібридною війною, та соціально-економічними наслідками агресії, що потребують ідентифікації та аналізу.

Алгоритм інтеграції підходів до НМС передбачає кілька ключових етапів: 1) систематизація ключових концепцій, визначення основних концепцій, що розкривають різні виміри стійкості, включаючи юридичну, соціальну, економічну та технологічну складові. При цьому слід звернути увагу на міжнародні практики стійкості, які можуть бути корисними для модифікації національних підходів; 2) порівняльний аналіз переваг і обмежень різних концепцій стійкості, що дозволить окреслити можливості адаптації та модифікації підходів відповідно до специфіки українського контексту, що вимагатиме врахування історичних, культурних та соціальних факторів; 3) оцінка функціональної придатності, як оцінку можливостей кожного з підходів у контексті збройної агресії та гібридної війни. Важливо усвідомлювати, які саме елементи стійкості можуть бути застосованими з досвіду інших країн; 4) виокремлення інваріантних аспектів через детермінацію принципів, механізмів та індикаторів, які можуть стати основою для формування цілісної стратегії, що відповідає специфіці українського контексту. Це може включати принципи субсидіарності, прозорості, відкритості у документуванні та звітності, які є ключовими для

формування позитивної довіри до державних інституцій.

Запропонований алгоритм інституціоналізації та реалізації НМС сприятиме логічній завершеності, теоретичній аргументованості та практичній релевантності концепції у контексті сучасних викликів. НМС не може бути окремим елементом – вона повинна стати основою для планування та реалізації всіх аспектів державного управління. Важливість цієї концепції підкреслюється необхідністю не лише ефективного реагування на агресію, а й побудови спроможної системи, яка зможе підтримувати розвиток, відновлення і демократичний контроль у післявоєнний період. Таким чином, формування НМС у форматі цифрової правової держави стає глобальним завданням, яке потребує комплексного підходу, що об'єднує зусилля всіх учасників суспільного процесу. Інтегративні міждисциплінарні дослідження стають фундаментом для реалізації цієї концепції, що поглиблює розуміння стійкості та дозволяє Україні ефективно інтегруватися в європейське суспільство, відновити свою територіальну цілісність і забезпечити добробут населення в умовах стабільного розвитку.

Таким чином, для України, поряд із впровадженням цифрових технологій, важливо вбудувати принципи стійкості в саму методологічну основу стратегій розвитку, сформувати структуру управління, у межах якої цифровізація стане інструментом для досягнення більшого рівня стійкості та адаптивності до сучасних викликів.

Висновки до розділу 2

1. У розділі обґрунтовано концепцію національної моделі стійкості (НМС) як багатофункціональної та інтегративної системи, що включає економічні, соціальні, політичні та екологічні компоненти. Підкреслено, що для формування ефективної НМС необхідно забезпечити злагоджене взаємодію між цими елементами, що дозволяє максимізувати використання наявних ресурсів і потенціалу України. Дослідження виявило важливість стратегічного планування, яке має бути спрямоване не лише на миттєве реагування на кризи, але й на довгострокову стійкість розвитку в умовах

глобалізації. У рамках НМС акцентовано значення адаптації управлінських практик до змінних умов, зокрема, у контексті цифровізації, розроблено механізми інтеграції політик та ресурсів, здатних швидко реагувати на виклики, такі як екологічні катастрофи, економічні кризи або соціальні конфлікти. Ця інновація в моделі управління підкреслює необхідність формування National E-Resilience – національної моделі інтегрованого управління, зокрема через впровадження централізованої цифрової платформи, що забезпечує цілісність відносин між різними рівнями влади та суспільством.

Інституціональна основа НМС має системно-структурний характер, що виражається через розроблену автором інституціональну формулу стійкості (institutional formula of resilience), яка об'єднує ключові компоненти: інституціональне середовище, формат державотворення, функціональний стан інститутів, систему їх взаємовпливу, механізми інституційних змін та витрат. Така комплексна структура забезпечує не просто ситуативну реакцію на кризи, а системну здатність держави підтримувати функціонування в умовах множинних загроз.

2. Дослідження питання адаптивності організаційних структур держави виявило, що для успішного впровадження НМС необхідно зосередитися на регіональних особливостях та специфіці управлінських практик. У розділі запропоновано нову методологічну концепцію, що передбачає запровадження механізмів динамічного управління, які базуються на принципах автономії локальних органів влади в поєднанні з централізованим контролем. Ця концепція є інноваційною у вітчизняному контексті, оскільки пропонує нові підходи до здійснення державного управління в умовах цифровізації. Наголошено на важливості формування гнучких управлінських систем, які здатні оперативно адаптуватися до нових викликів та загроз, включаючи заходи з локалізації цифрових рішень. Було виконано аналіз практичних прикладів, що демонструє, як адаптивні стратегії можуть бути реалізовані в різних регіонах країни, одночасно підтримуючи

баланс між єдністю політики на національному рівні та локальними потребами. Розроблена концепція управлінської адаптації дозволяє інтегрувати цифрові рішення, які відповідають специфіці кожного регіону, завдяки чому забезпечується ефективність у реагуванні на сучасні виклики.

Сформульовано чітку багаторівневу модель НМС – від макроінституційного середовища до операційних механізмів політик. Виділено: 1) інституційне середовище й формат державотворення (макрорівень); 2) суспільні інститути, їхня функціональна автономність, баланс і система взаємовпливу (мезорівень); 3) інституційні витрати, виклики, механізми змін; 4) механізми реалізації та стійкості політик (мікрорівень). Така декомпозиція дозволяє пов'язати абстрактні категорії (довіра, верховенство права, баланс влади) із конкретними управлінськими інструментами (організації, процедури, «запобіжники» для політик).

3. Обґрунтовано принципи системної залежності та цілісності як ядро теоретичних засад НМС. Доведено, що національна стійкість є відображенням стану й взаємодії базових підсистем – економічної, соціальної, екологічної, політичної, безпекової – і не може перевищувати стійкість їхніх «найслабших ланок». Запропоновано систему індикаторів та узагальнених вимірів (інституційно-управлінський, соціально-демографічний, економіко-інфраструктурний, безпеково-оборонний, еколого-кліматичний, цифрово-інформаційний), що дає можливість інтегрованого моніторингу й форсайт-управління, а не суто реактивного «гасіння пожеж».

4. Суттєво розширено розуміння стійкості за рахунок введення екзистенційного виміру й цифрової стійкості. Поряд із «функціональною» стійкістю (працездатність інститутів) обґрунтовано «екзистенційну» – здатність держави й суспільства зберігати сенс, гідність, суб'єктність у ситуаціях війни, травми, масових втрат, а також підтримувати колективні наративи, пам'ять і горизонтальні зв'язки громад. Одночасно показано, що правові й інституційні кроки у сфері цифровізації (кібербезпека, захист

даних, електронні довірчі послуги, інтероперабельність, проєкти на кшталт EU4DigitalUA, система «Трембіта», «Дія») уже формують каркас національної цифрової стійкості, інтегрований у європейські та глобальні стандарти.

5. Методологія національного розвитку в умовах правового режиму воєнного стану актуалізує НМС через механізми адаптації державного управління, зокрема: інтеграцію цифрових платформ для підтримки прийняття рішень, забезпечення безперервності критичних функцій держави, формування багаторівневої системи управління ризиками та кризами, а також розвиток гібридних моделей координації між державою, бізнесом та громадянським суспільством, що дозволяє зберегти керованість системи в умовах високої турбулентності.

Основні результати дисертаційного дослідження, що надані у цьому розділі, були опубліковані у фахових наукових виданнях зі спеціальності «Публічне управління і адміністрування» і включені до списку публікацій автора [22-25].

РОЗДІЛ 3

ЦИФРОВІ УПРАВЛІНСЬКІ ПЛАТФОРМИ ТА РОЗВИТОК ДЕРЖАВНИХ І
СУСПІЛЬНИХ ІНІЦІАТИВ В УКРАЇНІ: ВПЛИВ НА СОЦІАЛЬНУ
СТАБІЛЬНІСТЬ І БЕЗПЕКУ УПРАВЛІНСЬКИХ СИСТЕМ3.1. Цифрові управлінські платформи у форматі НМС: теоретичний
аналіз

Сучасний етап розвитку глобальної економіки та суспільних відносин характеризується безпрецедентним зростанням складності об'єктів управління. Традиційні ієрархічні моделі, розроблені в епоху індустріалізації, демонструють свою неспроможність в умовах високої ентропії, невизначеності та експоненційного зростання обсягів даних [272]. Відповіддю на ці виклики стала цифрова трансформація, ядром якої є перехід до платформної моделі управління. Цифрова управлінська платформа не просто сукупність програмно-апаратних засобів, а складна соціотехнічна система, що забезпечує оптимізацію ресурсів, процесів та взаємодій у реальному часі [273].

Досить часто цифрові управлінські платформи у технічному аспекті досліджують крізь призму теорії систем, кібернетики та сучасної архітектури бізнес-адміністрування [274]. Це зумовлено необхідністю створення адаптивних, резистентних до зовнішніх шоків організаційних структур, здатних до саморегуляції та еволюційного розвитку. У звіті детально розкриваються онтологічні властивості платформ, інваріантні принципи їх побудови, структурна анатомія та методологія створення, що базується на кращих світових практиках. Адже цифрові управлінські платформи (далі вживаємо – eGovPro) є невід'ємною складовою національної моделі стійкості, яка формується в умовах цифровізації.

Обґрунтування eGovPro доповнює концептуалізацію НМС як інтегративної системи, що передбачає синергію між різними елементами,

такими як державні органи, приватний сектор і громадянське суспільство. Це вимагає чіткої координації дій та обміну інформацією в реальному часі, для чого цифрові платформи забезпечують необхідні технологічні та інформаційні ресурси. eGovPro функціонують як механізми, що підтримують стійкість системи управління, завдяки можливостям збору, аналізу і обробки даних. Вони дозволяють забезпечити своєчасне реагування на кризові ситуації, адекватність управлінських рішень, а також швидкість адаптації до нових умов. Обґрунтування ролі eGovPro полягає в здатності таких платформ агрегувати інформацію з різних джерел, що дозволяє державним органам приймати більш обґрунтовані рішення.

У науковому дискурсі eGovPro стають дедалі важливішими для трансформації публічного управління. Такі платформи не лише збирають та обробляють дані, але й виступають каталізатором для нових форм взаємодії між різними учасниками процесу – державними установами, приватними організаціями та громадянами. Перехід від традиційних інформаційних систем до eGovPro відкриває нові можливості для удосконалення управлінських практик. Основним аспектом роботи eGovPro є агрегація даних, що включає збір інформацію з різноманітних джерел, що дозволяє створювати комплексну базу даних для аналізу і ухвалення рішень. Система eGovPro дає змогу збирати дані з всіх державних реєстрів, фінансових систем, а також інформації, що надходить від широкої громадськості. Це дозволяє державним органам швидко реагувати на зміни в суспільстві та адаптувати свої політики, спираючись на фактичні дані, а не лише на статистику. Когнітивна обробка даних у контексті eGovPro передбачає трансформацію сирих даних на управлінські інсайти. Це дозволяє державним органам не лише аналізувати минулі дані, а й робити прогнози на основі отриманих результатів. Завдяки застосуванню аналітичних методів керівники можуть виявляти патерни, тренди та потенційні ризики. Це забезпечує більш точне і своєчасне ухвалення рішень, які відповідають потребам суспільства.

У контексті формування екосистеми НМС саме eGovPro забезпечує

безбар'єрну комунікацію між усіма учасниками процесу. Це включає в себе: по-перше, інтегративну взаємодію, коли суб'єкти і об'єкти державноуправлінської діяльності можуть легко обмінюватись інформацією, комунікувати та співпрацювати в реальному часі, що сприяє органічному розвитку управлінських рішень. Також, eGovPro дозволяє державним і приватним організаціям інтегрувати свої інформаційні системи, що стимулює крос-секторальну співпрацю.

Натомість, eGovPro має фундаментальні відмінності від традиційних інформаційних систем (IC), що можна охарактеризувати через зміни вектору цінності. Так, традиційні IC зосереджені на оптимізації внутрішніх процесів і контролі за ними, слідуючи лінійній логіці управління, й при цьому основною метою є зменшення витрат і підвищення ефективності роботи окремих структур. eGovPro-платформи створюють цінність через мережеві ефекти та фасилітацію зовнішніх взаємодій, що концептуалізує перехід від традиційних урядових інформаційних систем, заснованих на внутрішній оптимізації та лінійному управлінні, до платформної моделі, що створює цінність через мережеві ефекти та фасилітацію екосистемних взаємодій. Трансформація парадигми управління від IT-систем як «центрів витрат» до платформ означає, що їх цінність зростає залежно від кількості учасників, які взаємодіють у системі, і від якості цих взаємодій. Це, в свою чергу, веде до створення нових можливостей, таких як залучення громади до формування публічних політик, що підвищує легітимність державних рішень [275]..

У цьому аспекті варто навести досвід Естонії, яка є однією з провідних країн у світі за рівнем цифровізації державного управління. Стратегія естонського уряду з цифровізації розпочалася на початку 2000-х років і виявилася надзвичайно успішною, зробивши країну піонером в електронному врядуванні у світі. Одним з ключових аспектів цієї трансформації є система e-Estonia, яка надає можливість громадянам отримувати доступ до різноманітних державних послуг онлайн. Згідно з дослідженням, проведеним у 2020 році, впровадження електронних послуг в Естонії призвело до 50%-го

скорочення часу, необхідного для отримання адміністративних послуг. Це значно підвищує зручність для громадян, оскільки вони можуть отримувати послуги без необхідності фізично відвідувати державні установи, що особливо важливо в умовах пандемії COVID-19. Дослідження показує, що в результаті цього впровадження, приблизно 80% естонців задоволені якістю електронних державних послуг, що свідчить про їхню ефективність у покращенні взаємодії між урядом і громадянами [276].

Досвід естонського електронного врядування чітко демонструє, як eGovPro може істотно змінити підходи до управління. Основними перевагами є: 1) підвищення операційної ефективності: Скорочення часу та витрат на отримання адміністративних послуг робить державне управління більш ефективним, що важливо для забезпечення стійкості держави в умовах криз; 2) задоволеність населення, коли високий рівень задоволеності населення електронними послугами свідчить про довіру громадян до державних інститутів, що зміцнює соціальну стабільність і сприяє активній участі громадян у формуванні політик; 3) адаптивність системи управління: eGovPro дозволяє швидко реагувати на зміни в середовищі, включаючи екологічні, економічні та соціальні виклики, що відповідає концепції національної стійкості. Важливо зазначити, що впровадження eGovPro в Естонії й інших країнах відкрило нові можливості для розвитку публічного управління. Це не лише покращило доступ до державних послуг, але й сприяло формуванню міцних відносин між державою та громадянами, створюючи основу для більш відкритого, прозорого та відповідального урядування.

Досвід естонського електронного врядування чітко демонструє, як eGovPro може істотно змінити підходи до управління. Основними перевагами є: 1) підвищення операційної ефективності, коли скорочення часу та витрат на отримання адміністративних послуг робить державне управління більш ефективним, що важливо для забезпечення стійкості держави в умовах криз; 2) задоволеність населення, коли високий рівень задоволеності

населення електронними послугами свідчить про довіру громадян до державних інститутів, що зміцнює соціальну стабільність і сприяє активній участі громадян у формуванні політик; 3) адаптивність системи управління: eGovPro дозволяє швидко реагувати на зміни в середовищі, включаючи екологічні, економічні та соціальні виклики, що відповідає концепції національної стійкості. Важливо зазначити, що впровадження eGovPro в Естонії й інших країнах відкрило нові можливості для розвитку державного управління. На прикладі Естонії доцільно формалізувати переваги електронного врядування через ряд ключових аспектів і механізмів, які підкріплюють його ефективність та вплив на публічне управління.

Таблиця 3.1

Традиційні інформаційні системи (ІС) та eGovPro (цифрові управлінські платформи)

Аспект	Традиційні інформаційні системи (ІС)	eGovPro	Докладний опис	Вплив на державне управління
Основна мета	Оптимізація внутрішніх процесів	Створення сусп. цінностей через мережеві ефекти	Традиційні ІС спрямовані на поліпшення внутрішніх бізнес-процесів. eGovPro засновані на інтеграції і залученні зовнішніх учасників	Зміна підходів до управління, враховуючи потреби суспільства
Структура взаємодії	Лінійна логіка управління	Нелінійна логіка через зовнішні взаємодії	Традиційні ІС - через фіксовані послідовності дій, eGovPro забезпечують гнучкість і можливість паралельних зв'язків між учасниками	Підвищує масштаби й рівень співпраці між різними відомствами
Агрегація даних	Зосереджена на внутрішніх джерелах даних	Збір даних з гетерогенних джерел	Традиційні ІС не інтегрують дані з зовнішніх джерел, eGovPro використовують дані від громадян, IoT-пристроїв, соціальних мереж	Створює більш точну картину реалізації політик і потреб населення
Когнітивна обробка даних	Обмеження до підготовки звітності	Аналіз даних і видобуток інсайтів	ІС використовують базові методи звітності, eGovPro застосовують аналітику та штучний інтелект для прогнозування і керування ризиками	Підвищує якість ухвалених рішень, опираючись на глибокий аналіз

Продовження таблиці 3.1

Аспект	Традиційні інформаційні системи (ІС)	eGovPro	Докладний опис	Вплив на державне управління
Залучення громадян	Обмежена участь громадян	Активне залучення громадян до процесів ухвалення рішень	Традиційні системи часто не надають можливостей для зворотного зв'язку, eGovPro створюють механізми для активної участі людей у прийнятті рішень	Сприяє розвитку довіри і партнерства між державою і суспільством
Прозорість	Залежить від внутрішніх процедур	Підвищена прозорість через відкриті платформи	Традиційні ІС можуть мати обмежений доступ до даних, eGovPro пропонують широкому загалу можливість перегляду і оцінки державних дій	Укріплює легітимність держави, зміцнюючи довіру населення
Адаптивність	Складно адаптуватися до нових умов	Швидка адаптація до змін у середовищі	Традиційні ІС часто потребують тривалого часу на модернізацію, eGovPro здатні оперативно реагувати на нові виклики і зміни	Полегшує ухвалення рішень в умовах кризи і невизначеності
Культурні зміни	Мінімальний вплив на культуру управління	Перетворення культури управління через інтегровану співпрацю	Традиційні ІС можуть підтримувати традиційний підхід до управління, eGovPro впроваджують нові моделі співпраці та комунікації	Поширення нових цінностей у держуправлінні: прозорість, відкритість, залучення
Вартість впровадження	Висока вартість підтримки та оновлення	Зниження витрат через централізовану інфраструктуру	Традиційні ІС може вимагати значних ресурсів для утримання, у eGovPro хмарні технології зменшують витрати	Ефективніше використання державних бюджетів і ресурсів
Моніторинг та звітність	Обмежені можливості для інтерактивного моніторингу	Динамічний моніторинг та зворотний зв'язок	Традиційні ІС можуть продукувати статичні звіти, тоді як eGovPro забезпечують динамічні аналітичні звіти, що базуються на реальних даних	Підвищує обізнаність суспільства про політики та дії уряду

Джерело: розроблено автором.

Як видно з таблиці 3.1, eGovPro, як інтегроване цифрове середовище управління, стане важливим елементом для вдосконалення державного управління й забезпечення національної стійкості. У порівнянні з

традиційними інформаційними системами, eGovPro демонструють значно більшу гнучкість, адаптивність і активну участь громадян. Впровадження таких платформ забезпечує більш якісний зворотний зв'язок, підвищує прозорість та ефективність ухвалення рішень, а також зміцнює довіру до держави, формуючи таким чином більш стійку та адаптовану до змін систему управління.

Отже, eGovPro (цифрові управлінські платформи) – це інтегроване цифрове середовище, що базується на сучасних технологіях, яке забезпечує агрегацію даних з різноманітних джерел, когнітивну обробку інформації та безшовну екосистемну взаємодію серед усіх учасників управлінських процесів, виступає ключовим інструментом національної стійкості (НМС), надає можливість оперативно й ефективно реагувати на виклики сучасності, збільшуючи прозорість, адаптивність і залученість громадян у процеси ухвалення рішень. При цьому цифровізація інтерпретується не лише як технологічний процес, а як значний чинник трансформації логіки державного управління. Вона є комплексним явищем, яке впливає на організаційні моделі державного управління, змінюючи традиційні підходи до взаємодії між урядовими структурами і громадянами. Цифровізація дозволяє створити нові можливості для участі громадян у процесах ухвалення рішень, що є критично важливим для розвитку демократичних суспільств. Наприклад, через електронні платформи громадяни можуть активно долучатися до обговорення політик, висловлювати свої думки через опитування та петиції, а також контролювати виконання державних обов'язків. Це не лише підвищує їхню відповідальність і активність, але й формує баланс між державою і суспільством, сприяючи більшій легітимності прийнятих рішень.

Крім того, цифровізація зміцнює соціальну стабільність та безпеку функціонування управлінських систем, адже дає змогу урядам швидше реагувати на виклики, зокрема на кризові ситуації, через використання даних у реальному часі. Унікальність цього процесу полягає в можливості інтеграції даних з різних джерел, що формує цілісну картину дійсності і

дозволяє ухвалювати зважені рішення. Наприклад, під час епідемій або природних катастроф швидка обробка і аналіз інформації з різних джерел допомагають органам влади оперативно вжити заходів, що знижує ризики для населення. Цифровізація також стимулює зміни в культурі управління, переходячи від традиційних, закритих моделей до більш відкритих і прозорих форм взаємодії. Такий підхід дозволяє створювати середовище довіри між громадянами та державою, зміцнюючи соціальний капітал. Громадяни, коли спостерігають, як їхні голоси мають значення, активніше долучаються до управлінських процесів, що підвищує їхню довіру до інституцій. Одночасно з цим, цифровізація вимагає нових навичок від державних службовців, що сприяє розвитку професійного потенціалу управлінців і їхньої адаптивності у швидко змінюваному середовищі.

Отже, цифровізація є не просто модернізацією інструментів управління, а глибоким культурним і структурним зрушенням, яке підвищує здатність управлінських систем адаптуватися до нових викликів і потреб суспільства [277]. У результаті, ефективна реалізація цифровізації в державному управлінні може привести до стабільнішої, прозорішої і більш залученої у взаємодію з громадянами системи, що, в свою чергу, підвищує загальну стійкість національної моделі управління. Ці зусилля не лише сприяють короткостроковим досягненням, але й закладають основи для довготривалого розвитку країни у швидко змінюваному світі.

При цьому розуміння властивостей eGovPro вимагає виходу за межі суто технічних характеристик., адже такі платформи мають розглядатися як самостійний механізм, що володіє набором атрибутів якості (Quality Attributes), які визначають його життєздатність та ефективність.

1. *Емерджентність та системна складність.* Головною властивістю eGovPro є емерджентність – поява у системи нових властивостей, які не притаманні її окремим елементам. Ефективність eGovPro не може бути зведена до простого підрахунку результативності модулів (як у бізнес-адмініструванні), таких як ERP (Enterprise Resource Planning, планування

ресурсів), CRM (Customer Relationship Management, управління взаємовідносинами з клієнтами) та BI (Business Intelligence, управлінська аналітика). Кожен з подібних компонентів у державному управлінні виконує свої специфічні функції, але їх загальна ефективність значно перевищує просту різницю в даних, отриманих від кожного модуля. Щоб зрозуміти це, важливо провести детальний аналіз кожного з аспектів, що визначають комплексну ефективність управлінської платформи [278;279].

Ефективність управлінської платформи виникає з інтеграції модулів, що забезпечує синергію в управлінських процесах. Кожен модуль виконує свою роль і спеціалізується на певному аспекті управління: ERP відповідає за управління внутрішніми операціями, такими як фінанси, закупівлі та управління запасами і дозволяє оптимізувати внутрішні процеси. Модулі CRM орієнтовані на управління взаємовідносинами з клієнтами, забезпечують глибше розуміння потреб і уподобань клієнтів, допомагаючи налаштувати стратегії обслуговування та маркетингу на базі зібраних даних. Модулі BI займаються збором, обробкою та аналізом даних, перетворюючи дані в аналітичні звіти та інсайти, що допомагають у прийнятті рішень. Коли ці модулі правильно інтегровані, вони створюють міцну платформу, що дозволяє організації діяти швидше та ефективніше, адаптуючись до змін у навколишньому середовищі. Наприклад, завдяки даним з ERP, CRM може пропонувати персоналізовані рішення, а BI може виявити нові можливості на основі аналізу даних.

Ефективність eGovPro визначається також рівнем комунікації і взаємодії між модулями. Якщо модулі працюють автономно, без належної інтеграції, виникає ризик дублювання зусиль і неузгодженості даних, що безпосередньо вплине на якість прийнятих рішень. Комплексна ефективність eGovPro також визначається здатністю організації використовувати інтуїтивну аналітику для прийняття обґрунтованих рішень. Таким чином, ефективність управлінської платформи формується не просто як результат функціонування її окремих модулів, а як результат цілісної інтеграції,

ефективної комунікації між компонентами та їх здатності працювати в синергії. Спільна робота модулів ERP, CRM і BI дозволяє не лише досягти високих результатів у виконанні конкретних завдань, а й забезпечує стійкий розвиток організації, покращує управлінські рішення, знижує ризики та підвищує рівень обслуговування клієнтів. Це робить управлінську платформу eGovPro потужним інструментом для досягнення стратегічних цілей публічного управління.

Таблиця 3.2

Порівняльні характеристики систем державного управління

Аспект	Традиційне ДУ	Цифровізація в ДУ	Докладний опис
Основна мета	Упорядкування внутрішніх процесів управління	Підвищення участі громадян, покращення якості держ. послуг	Традиційне управління зосереджене на внутрішніх процедурах, тоді як цифровізація прагне до створення відкритих і прозорих механізмів обслуговування та взаємодії з населенням
Доступ до даних	Обмежений доступ до інформації про діяльність урядів	Відкритість та доступність інформації для всіх громадян	У традиційних системах важко отримати інформацію про роботу держави. Цифровізація дозволяє громадянам отримувати дані в реальному часі, що покращує прозорість процесів ухвалення рішень
Тип взаємодії з громадянами	Одностороння комунікація від уряду до населення	Двостороння комунікація з активним залученням громадян	У традиційних системах уряд повідомляє про свої рішення, тоді як цифровізація забезпечує конструктивний діалог, що дозволяє громадянам брати активну участь у формуванні політики
Адаптивність до змін	Низька швидкість реагування на нові потреби суспільства	Швидка адаптація до вимог суспільства і зовнішніх змін	Традиційні системи зазвичай потребують часу для зміни політики, в той час як цифровізація забезпечує гнучкість, яка дозволяє швидко реагувати на нові виклики і ситуації
Контроль і моніторинг	Обмежені можливості для громадського контролю	Ефективний контроль за діяльністю уряду в реальному часі	У традиційних системах контроль за виконанням рішень часто залишається на папері, тоді як цифрові технології надають доступ до даних і можливість моніторингу результатів діяльності
Соціальний капітал	Низький рівень довіри до державних інститутів	Підвищення довіри завдяки прозорості і відкритості	У традиційних системах часто спостерігається недовіра до держави, цифровізація через активну участь громадян та доступ до інформації може зміцнити ці відносини

Продовження таблиці 3.2

Аспект	Традиційне ДУ	Цифровізація в ДУ	Докладний опис
Співпраця між урядом і суспільством	Окремі ініціативи без активної взаємодії	Системна співпраця між урядом і громадськими організаціями	У традиційних системах відсутня координація, тоді як цифровізація сприяє розвитку партнерства, що дозволяє спільно формувати політики та рішення, важливі для суспільств
Механізми зворотного зв'язку	Відсутність структурованих каналів для зворотного зв'язку	Створення платформ для збору громадської думки і пропозицій	Традиційні системи часто не мають можливостей для активного зворотного зв'язку, тоді як цифрові платформи активно залучають громадян до обговорення і формулювання рекомендацій для політики

Джерело: узагальнено автором.

2. *Масштабованість (scalability)*. Хоча ці терміни часто вживаються як синоніми, в контексті фундаментальної архітектури вони мають різне фізичне змістовне навантаження. У нашому випадку, масштабованість передбачає здатність платформи обробляти зростаюче навантаження шляхом нарощування ресурсів, може бути вертикальною (scale up) та горизонтальною (scale out). Загалом, теоретична межа масштабованості описується законом Амдала, який стверджує, що прискорення виконання програми на паралельних системах обмежене часом, необхідним для виконання її послідовної частини [280]. Закон Амдала є концепцією, що описує теоретичні межі прискорення виконання програм на паралельних обчислювальних системах. Цей закон, сформульований Д.Амдалем у 1967 році, виявляє просте, але суттєве обмеження на зростання продуктивності при розподілі обчислень. Закон Амдала, що при розподілі завдання на кілька частин, загальний час виконання на паралельній системі не може бути меншим за час виконання найдовшого фрагменту завдання. Це означає, що прискорення виконання програми за рахунок паралелізації її інструкцій на багатьох обчислювальних одиницях обмежене часом, необхідним для виконання її послідовних інструкцій. Коли частина програми має виконуватися послідовно, вона стає «гальмом» для загальної продуктивності системи, незалежно від того, скільки ресурсів виділено для паралельних

обчислень [281].

Закон Амдала, хоча і стосується технічних аспектів паралельного обчислення, може бути адаптований до сфери державного управління, особливо в контексті сучасних технологічних ініціатив, таких як eGovPro. Основна ідея, що лежить в основі цього закону, полягає в розумінні того, що не всі частини процесів управління можуть бути паралелізовані. Це спостереження стає особливо важливим у контексті формування нами концепту національної моделі стійкості (НМС) та впровадження електронних послуг. По-перше, у межах eGovPro при розподілі завдань між державними структурами слід врахувати, що у державному управлінні існують процеси, які можуть бути реалізовані паралельно (наприклад, автоматизація надання адміністративних послуг) та ті, що потребують послідовності (наприклад, ухвалення законодавчих актів або стратегічне планування). Знання про це дає змогу на основі eGovPro ефективно розподіляти ресурси і оптимізувати процеси, запобігаючи затримкам, викликаним непродуманою організацією.

По-друге, у рамках концепції НМС та конкретно eGovPro, важливо розуміти, що навіть з наявністю сучасних технологій не всі аспекти управління можуть бути прискорені до однакової міри. Наприклад, впровадження цифрових рішень може значно скоротити час на обробку заяв громадян, але етапи узгодження та перевірки все ще вимагатимуть значних часових ресурсів. Це обмеження визначає, як швидко можуть бути реалізовані нові ініціативи.

По-третє, у рамках НМС, затримки в послідовних частинах управлінських процесів можуть впливати на загальну ефективність реалізації електронних послуг. Наприклад, якщо затвердження нових стандартів для електронних систем займає тривалий час, це може гальмувати запуск нових послуг, навіть якщо вся технічна інфраструктура готова. Розуміння цього аспекту дозволяє структурувати план реалізації НМС так, щоб мінімізувати затримки в процесах, які не можуть бути автоматизовані.

Закон Амдала ілюструє суттєві обмеження, з якими стикаються

державні управлінці при впровадженні нових технологічних рішень у рамках публічного управління. При застосуванні цього закону у контексті національної моделі стійкості (НМС) та eGovPro важливо усвідомити, що зростання ефективності управлінських процесів залежить не лише від доступності ресурсів, але й від здатності мінімізувати вплив послідовних етапів, які не можуть бути автоматизовані. Це дозволить створити більш відкриту, прозору і швидку систему публічного управління, що є ключовим для стійкості та адаптивності держави в умовах сучасних викликів.

3. *Інтероперабельність (Interoperability)* – як здатність платформи eGovPro безперешкодно обмінюватися інформацією з іншими системами є критичною умовою існування в сучасному цифровому ландшафті. Інтероперабельність реалізується на трьох рівнях: технічному – як сумісність протоколів передачі даних, синтаксичному – як сумісність форматів даних, та семантичному – єдиному розумінні змісту даних різними системами. Значення інтероперабельності для НМС полягає у тому, що, по-перше, забезпечується поліпшення адміністративних процесів, й інтероперабельність дозволяє державним органам оперативно обмінюватися інформацією, що значно скорочує час обробки запитів громадян. Це підвищує ефективність адміністративних послуг і зменшує бюрократію, що в свою чергу, зміцнює довіру до державних інститутів. По-друге, гарантується адаптивність до змін, й інтероперабельні системи можуть швидко адаптуватися до нових викликів та змін у законодавстві, програмних забезпеченнях або суспільних умовах. Це важливо для забезпечення стійкості в умовах змінюваного середовища (економічних криз, соціальних трансформацій тощо). По-третє, забезпечується участь громадян і прозорість, відкриті та інтероперабельні платформи заохочують активну участь громадян у процесах управління, громадяни мають доступ до відомостей про адміністративні послуги, що підвищує прозорість діяльності держави та сприяє залученню населення до формування політик. По-четверте, формується узгодженість між урядовими установами, адже

інтероперабельність дозволяє забезпечити більш надійний зв'язок між різними державними структурами, що зменшує ризик дублювання зусиль та конфліктів у даних. Це покращує координацію дій між органами влади та відповідальність у виконанні завдань.

4. Резильєнтність (resilience) – концептуальна і засаднича характеристика НМС та eGovPro, її внутрішній зміст. Будь-яка управлінська платформа є критично важливою інфраструктурою, тому вона повинна продовжувати функціонувати навіть при виході з ладу окремих компонентів. Резильєнтність – це здатність системи адаптуватися, відновлюватися та покращуватися після стресових ситуацій. Для досягнення цієї резильєнтності в державному управлінні можуть бути використані архітектурні принципи, які знайшли своє застосування в інформаційних технологіях.

«Resilient» походить від латинського дієслова «resilire», що означає «повернутися» або «відскочити назад». Слово «resilience» вперше з'явилося в англійській мові на початку 17 століття, зокрема в контексті емоційного або фізичного відновлення. Спочатку воно вживається в наукових або технічних текстах, пов'язаних з матеріями, але згодом його значення розширилося і почало використовуватися в контексті психології, соціології та інших наук [283]. У сучасному світі, сповненому невизначеності і різноманітних викликів, цифрові управлінські платформи позначилися як критично важливий елемент інфраструктури, що забезпечує координацію між державними, приватними та громадськими ініціативами. Особливо це стало очевидним в умовах воєнної агресії з боку РФ проти України та гібридних загроз, які вимагають швидких, адаптивних і прозорих рішень. Як логічне формування нового напрямку в державному управлінні, що концептуалізує НМС та eGovPro, ми визначаємо феномен Integrated Open Government (IOG). Концепція IOG є важливим інструментом для вирішення наукової проблеми формування та реалізації державних реформ, а також складає основу для розробки складників парадигми цифрової держави як самостійного напрямку в науці державного управління.

Integrated Open Government (IOG) – управлінська концепція, яка поєднує елементи відкритого урядування з інтеграцією технологій для забезпечення більшої прозорості, підзвітності та участі громадян у публічному управлінні (рис.3.1).

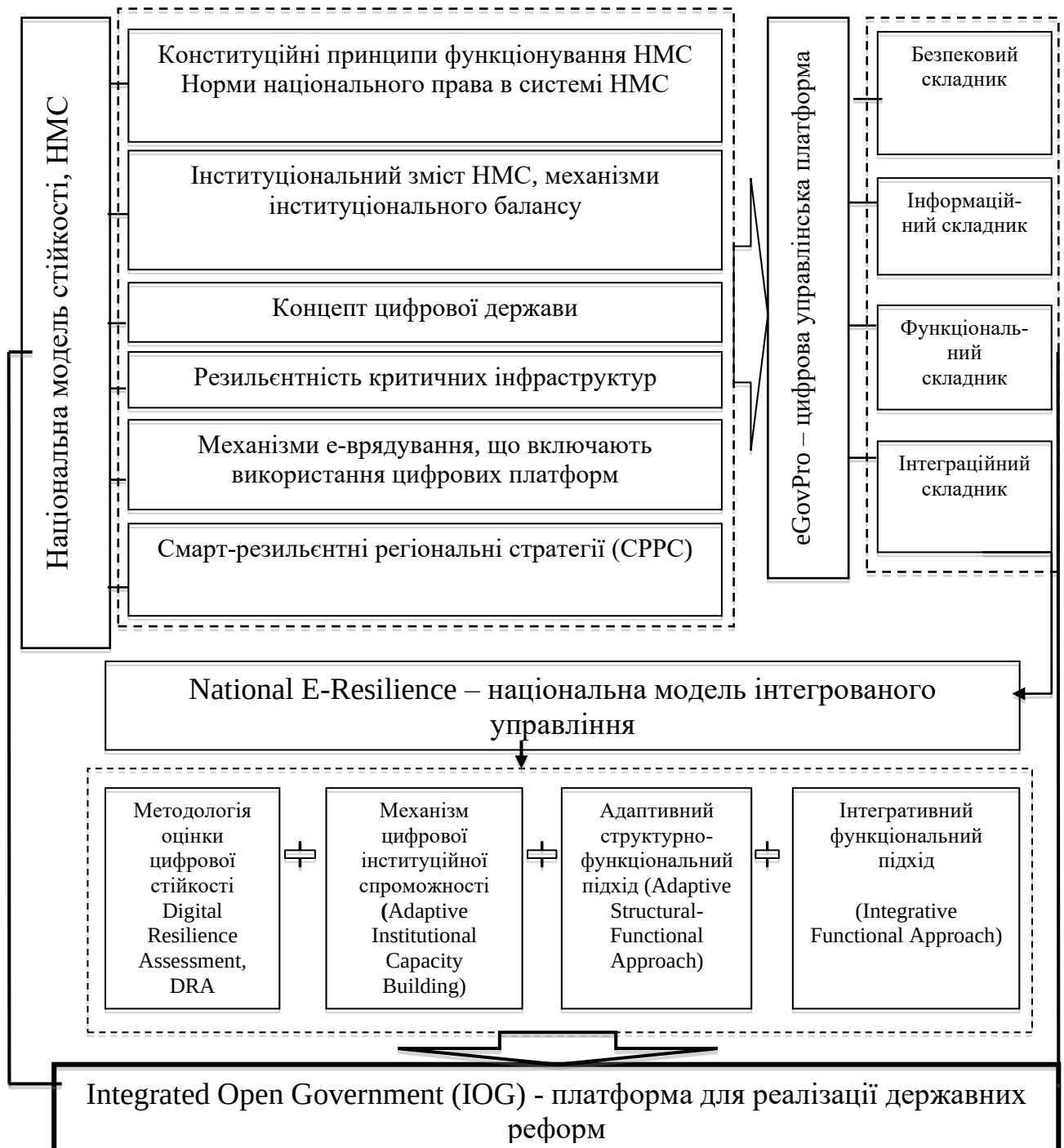


Рис.3.1. Формалізація авторського концепту Integrated Open Government (IOG) як практичного інструменту для реалізації державних реформ

Джерело: [283]; дослідження автора

Основна ідея IOG полягає в тому, що відкритість державних процесів має відбуватися не лише на рівні доступу до інформації, але й у формі інтеграції даних і технологій, що створює платформу для активної участі всіх учасників – від державних органів до приватного сектора і громадян [284]. Для досягнення цілісності в дослідженні концепції IOG важливо таку інтеграцію на концептуальному рівні. Це передбачає поєднання відкритого державного управління і цифрових технологій, що вимагає синергетичного підходу. Дослідження має обґрунтувати, яким чином технологічна інфраструктура може підтримувати відкритість і підзвітність управлінських платформ, забезпечуючи одночасно інтеграцію даних і механізмів зворотного зв'язку. На практичному рівні концепція IOG потребує інтеграції державних і недержавних ініціатив, розробку практичного механізму для інтеграції зусиль держави, приватного бізнесу та громадських організацій, що дозволяє реалізувати принципи IOG. Це вимагатиме співпраці на всіх рівнях управління та формування необхідної інфраструктури.

Важливим при цьому є завдання об'єднання класичних та новітніх теорій управління, перш за все, аналізу традиційних теорій публічного управління з сучасними концепціями, такими як «Управління через мережі» (Network Governance) та «Управління через результати» (Outcome-Based Governance), для створення цілісної моделі, що сприймає концепцію IOG [285]. Таким чином забезпечується формування нових теоретичних основ для IOG через дослідження аспектів відкритості, підзвітності, та громадської участі в управлінні. Це у дослідженні концепції Integrated Open Government (IOG) дозволяє інтегрувати численні аспекти публічного управління, технологій, соціальних наук та практичних рішень, забезпечує нові перспективи для досягнення стійкості, прозорості та ефективності в управлінні, що є критично важливим у контексті сучасних викликів. Дослідження інтеграції має на меті створити не лише теоретичну основу, але й практичні рекомендації для впровадження IOG у державне управління, що може сприяти покращенню благополуччя громадян і загальному розвитку

суспільства.

3.2. Integrated Open Governance як нова концепція публічного управління в цифрову епоху

Важливим завданням сучасної науки державного управління є визначення основних принципів і підходів до інтегрованого відкритого управління та розроблення методологій, які дають можливість забезпечити цифрову інтеграцію державних структур, прозорість та інклюзивність прийняття рішень. Практичний аспект полягає у створенні умов для доступності цифрових інструментів та подолання цифрового розриву серед різних соціальних груп [286].

Застосування концепції інтегрованого відкритого управління сприяє підвищенню довіри громадян до державних інституцій, що особливо актуально в умовах глобальних викликів, пов'язаних зі швидкими змінами суспільно-політичних та економічних реалій [287]. Водночас це потребує розв'язання низки проблем, зокрема захисту кібербезпеки й персональних даних та створення нормативно-правової бази для регулювання цифрових взаємодій між державою, бізнесом і громадянами. Таким чином, дослідження інтегрованого відкритого управління є важливим кроком у розвитку сучасних систем публічного управління, що відповідають вимогам цифрової доби та забезпечують гнучкість, прозорість і ефективність у реалізації державних функцій.

Інтегроване відкрите управління (IOG) залишається важливим об'єктом дослідження у сфері державного управління, адже воно забезпечує прозорість, підзвітність та залучення громадян до прийняття рішень через використання цифрових платформ і відкритих даних. Значна увага приділяється аналізу міжнародного досвіду, інноваційних практик та проблемних аспектів реалізації цієї концепції в різних країнах. Дослідження відкритості управлінських процесів показує, що залучення громадськості до

обговорення та моніторингу політики суттєво підвищує рівень довіри до державних інституцій. Зокрема, це підтверджено в роботі О. Доброгорського, де акцентовано на важливості ефективної комунікації між владою та громадянами для забезпечення прозорості [288]. Аналіз цифровізації публічного управління в США, проведений О. Савченком, свідчить про важливість інтеграції інноваційних платформ для моніторингу та громадських обговорень, що підвищує результативність політичних рішень [289]. Також Г. Бондар дослідив практику впровадження відкритих даних та електронних послуг в Україні, підкресливши проблему цифрової нерівності та потребу в оновленні нормативно-правового забезпечення [290].

А. Сіленко та Н. Крук звертають увагу на те, що впровадження концепції «відкритого уряду» потребує адаптації міжнародних практик відповідно до національних реалій. Їхній аналіз підкреслює важливість розробки локальних механізмів реалізації цифрового врядування [291]. Взаємодію органів влади з громадянським суспільством також розглянуто в дослідженні О. Каретної, І. Милосердної та І. Ігнат'євої, де наголошено на тому, що інформаційно-комунікаційні технології можуть сприяти підвищенню підзвітності, але лише за умови розвитку цифрових навичок населення [292]. Проблему безпеки інформаційних систем порушено в роботі Д. Луніна, де обґрунтовано необхідність запровадження єдиних стандартів безпеки та регулярного аудиту цифрових платформ [293]. Водночас J. Gil-Garcia та його колеги досліджують міждисциплінарний підхід до управління відкритими даними та зазначають, що ефективність систем залежить від узгодженості правових та технічних механізмів [294].

Питання інтеграції цифрових технологій у надання державних послуг порушено в роботі V. Lapuente та S. Van de Walle, де проаналізовано вплив публічних управлінських реформ на якість послуг. Автори роблять висновок, що недостатнє правове регулювання може спричинити фрагментацію процесів [295]. Колаборативні платформи, як зазначено в дослідженні С. Ansell та А. Gash, можуть підвищити якість прийняття рішень завдяки

спільному використанню ресурсів і відкритості процедур [296]. Проте J. Millard звертає увагу на необхідність правового регулювання розширення обсягів цифрових послуг, аби уникнути ризиків зловживань та зниження безпеки [297].

Вплив цифрових рішень на взаємодію між громадянами та адміністрацією висвітлено в роботі T. Janowski та його колег, де зроблено висновок про необхідність адаптації цифрових інструментів до соціальних потреб для забезпечення сталого розвитку [298]. Крім того, в огляді дослідження J. Twizeyimana та A. Andersson наголошено, що суспільна цінність електронного урядування залежить від забезпечення рівного доступу до послуг і підтримки цифрової інклюзії [299]. Таким чином, проаналізовані дослідження демонструють важливість комплексного підходу до інтегрованого відкритого управління, що охоплює вдосконалення правових механізмів, розвиток цифрових навичок громадян та підвищення кібербезпеки.

Попри значні досягнення у вивченні концепції інтегрованого відкритого управління (IOG), існує безліч важливих питань, що залишаються нерозв'язаними. Основною проблемою є оцінка ефективності функціональних складників цієї концепції та проникнення в складну природу впливу цифрових платформ на рівень громадянської участі в процесах управління. Безпідставно уходять з поля зору науковців специфіка та методологія використання електронних консультацій, а також адаптація міжнародних практик до специфічного українського контексту. Це підкреслює вкрай необхідність здійснення критичного аналізу існуючих механізмів залучення громадян у формування політик, що, на жаль, досі не має системного обґрунтування.

Крім того, проблема цифрової нерівності розглядається переважно через призму доступу до інтернету, що є занадто вузьким підходом. Непоміченими залишаються такі важливі фактори, як рівень цифрової грамотності населення та доступність електронних сервісів, особливо для

вразливих груп. Включення останніх до процесів управління, безумовно, є запорукою створення справедливого суспільства. Ситуація ускладнюється зростанням міжрегіональних диспропорцій у забезпеченні доступності цифрових послуг, що підвищує ризик соціальної ізоляції певних груп населення, які не мають змоги інтегруватися у цифровий світ.

Другим важливим аспектом є захист персональних даних громадян, а також правове регулювання механізмів громадського контролю. В умовах зростання кіберзагроз питання безпеки стає особливо важливим, адже недотримання вимог про конфіденційність може призвести до серйозних негативних наслідків для всієї системи відкритого управління. Таким чином, необхідність глибокого аналізу цих питань стає очевидною, що передбачає комплексне дослідження на основі методу головних компонент, який дозволить виділити найбільш критичні фактори, що впливають на ефективність IOG.

У зв'язку з вищезазначеним, дослідження покликане заповнити вказані прогалини шляхом всебічної оцінки функціональних складників системи відкритого управління. Особлива увага буде приділена виявленню причинно-наслідкових зв'язків, які лежать в основі низької участі громадян у публічному управлінні. Це дозволить розробити практичні рекомендації для вдосконалення нормативної бази, що, у свою чергу, сприятиме підвищенню прозорості, підзвітності та довіри до державних інституцій. Концепція інтегрованого відкритого управління, визначена як сучасний підхід до урядування, передбачає синергію принципів прозорості, відкритості та інклюзивності з ефективним використанням цифрових технологій для оптимізації управлінських процесів. Ця модель орієнтована на інтеграцію інформаційних потоків, активну взаємодію між різними державними установами та залучення громадян до прийняття рішень. Вона включає у себе реалізацію принципів відкритих даних, підзвітності органів влади та доступу громадян до цифрових сервісів, що безпосередньо сприяє зміцненню довіри до державних інституцій та створенню належних передумов для більш

ефективної політики. Концептуальні засади інтегрованого відкритого управління охоплюють такі основні принципи, як прозорість, підзвітність, цифрова інклюзія та взаємодія на основі відкритих платформ. (табл. 3.3).

Таблиця 3.3

Концептуальні основи інтегрованого відкритого управління: принципи, функціональні складники та їхня практична імплементація

Принципи	Функціональні складники	Практичне застосування	Проблеми та виклики
Прозорість та відкритість даних	Публікація відкритих даних на державних порталах	Доступ громадян до актуальної інформації про діяльність органів влади	Нехтування приватністю даних, недостатня якість даних, обмежений доступ до інформації в регіонах
Підзвітність та контроль	Автоматизовані звіти та моніторинг результатів	Громадські організації здійснюють незалежний моніторинг ефективності політики	Відсутність стандартів і критеріїв оцінки, неможливість реального контролю за виконанням
Інклюзивність та участь	Цифрові платформи для публічних консультацій	Проведення електронних обговорень та збору пропозицій громадян	Низький рівень залучення громадян, цифрова нерівність, відсутність урахування думки всіх верств населення
Інновації та цифрова інтеграція	Використання аналітичних інструментів та ІТ-рішень	Автоматизація процесів і прогнозування наслідків управлінських рішень	Невідповідність технологій до потреб користувачів, ризики кібербезпеки, недостатня підготовка персоналу
Відкритість рішень та механізмів	Публічні слухання візуалізації рішень	Громадяни можуть слідкувати за процесом ухвалення рішень	Непрозорість прийняття рішень, недостатня інформаційна підтримка
Взаємодія між секторами	Партнерства між державними та недержавними організаціями	Спільні проекти та ініціативи з активним залученням бізнесу	Відсутність чітких механізмів взаємодії, конкуренція між секторами, потреба у фінансуванні
Адаптивність до змін	Гнучкі адміністративні структури	Швидка реакція на виклики та зміни у суспільстві	Опір змінам з боку державних службовців, ускладненість реорганізації
Висока якість послуг	Стандартизація процесів і послуг	Покращення якості електронних сервісів для громадян	Невідповідність стандартів реальним потребам населення, технічні недоліки у системах управління
Комплексний підхід до реалізації	Взаємодія між усіма учасниками процесу	Залучення всіх зацікавлених сторін у процеси управління	Складність в організації комунікації, небажання деяких сторін співпрацювати

Джерело: сформовано автором на підставі [288; 293]

На практиці інтегроване відкрите управління демонструє ефективність у створенні єдиного інформаційного простору для взаємодії між органами державної влади та громадянами. Державні портали з відкритими даними дають можливість користувачам не лише отримувати інформацію, але й проводити власний аналіз та пропонувати альтернативні рішення. Це створює умови для прозорості прийняття рішень і зменшує ризик корупційних дій. Використання цифрових платформ для публічних обговорень та електронних консультацій сприяє забезпеченню реального зворотного зв'язку з громадянами, що робить управлінські процеси більш інклюзивними. Водночас автоматизовані аналітичні системи сприяють оперативному моніторингу результатів упровадженої політики та забезпечують підвищення ефективності управління завдяки прогнозуванню можливих соціальних та економічних наслідків. Такий підхід дає змогу не лише оперативно реагувати на виклики, але й створювати стратегії розвитку, які відповідають потребам суспільства в умовах цифрової епохи.

Цифрові управлінські платформи (та відкриті дані є важливими елементами сучасного публічного управління, які забезпечують прозорість управлінських процесів та сприяють активному залученню громадян до прийняття рішень. Відкритий доступ до інформації про діяльність державних органів дає можливість громадянам контролювати прийняття політичних і фінансових рішень, брати участь у суспільно важливих ініціативах та взаємодіяти з владою у форматі електронних консультацій. Це підвищує підзвітність органів державної влади та формує нові стандарти двосторонньої взаємодії між владою та громадянами. Відкриті дані забезпечують можливість доступу до фінансових звітів, нормативно-правових актів та показників соціально-економічного розвитку, що сприяють проведенню незалежного моніторингу та оцінюванню ефективності реалізації державних програм. Цифрові управлінські платформи підтримують інтерактивність процесів управління та полегшують комунікацію між громадськістю та державними установами, створюючи передумови для громадського

контролю та впливу на прийняття рішень (таблиця 3.4)

Таблиця 3.4

Компоненти цифрових управлінських платформ та відкритих даних у
забезпеченні прозорості управління та громадської участі

Компоненти eGovPro	Функціональне значення	Вплив на прозорість та громадську участь	Проблеми та виклики
Публічні бази даних	Надання відкритого доступу до інформації про діяльність державних установ, що сприяє прозорості	Збільшення кількості ініціатив із громадського моніторингу	Неправильність або застарілість даних, обмежений доступ до інструментів аналізу даних
	Підтримка аналізу державних витрат і ефективності служб	Дослідження зацікавлених сторін щодо виконання бюджету	Ускладненість у верифікації інформації, відсутність інтеграції з іншими системами
Платформа електронної демократії	Служить інструментом для електронного залучення громадян до формування порядку денного	Підвищення рівня громадянської активності в прийнятті рішень	Низький рівень обізнаності з платформою, технічні проблеми з доступом до електронних ресурсів
	Сприяння відкритій комунікації між громадянами та державними органами	Сформування діалогу між владою і суспільством	Технічні складнощі, що можуть перешкоджати участі, недостатня підтримка з боку держави
Інтерактивні бюджетні панелі	Сприяння контролю за використанням бюджетних коштів і фінансових потоків	Зростання прозорості та підвищення звітності органів влади	Складність в розумінні даних бюджету, можливість маніпуляції інформацією
	Надає користувачам можливість брати участь у фінансових рішеннях і оцінювати їх перед ухваленням	Активізація участі громадян у бюджетному процесі	Відсутність належної освіти і підготовки населення для ефективного використання панелей
Консультації з громадськістю	Організація онлайн-обговорень і збору думок щодо нормативних актів	Формування прозорого механізму ухвалення рішень з урахуванням громадської думки	Низький рівень зворотного зв'язку, відсутність адресних запитів, неузгодженість у каналах комунікації
	Розвиток механізмів для зворотного зв'язку між громадянами та органами влади	Підвищення довіри до держави через активну участь у прийнятті рішень	Висока частка «шуму» у відгуках, нерівність доступу до платформи
	Вдосконалення процедур прослуховування думок та ініціатив громадян	Створює передумови для ефективної участі громади в ухваленні рішень	Ускладненість у контролі за якістю отриманих відгуків, обмежений доступ для вразливих груп

Продовження таблиці 3.4

Компоненти eGovPro	Функціональне значення	Вплив на прозорість та громадську участь	Проблеми та виклики
Аналітичні інструменти для управління даними	Використання новітніх аналітичних технологій для обробки та візуалізації даних	Підвищення ефективності прийняття рішень завдяки даним і їхній інтерпретації	Ризики кібербезпеки, постійні апдейти технологій, потреба в освіченому персоналі
	Спрощення доступу до аналітики для користувачів	Сприяння глибшому аналізу й прийняттю рішень на основі даних	Обмежений доступ до аналітичних платформ для менш забезпечених верств населення
Системи управління зворотним зв'язком	Використання платформ для збору відгуків і пропозицій від громадян	Посилення зворотного зв'язку між населенням та державою	Непродумані механізми збору відгуків, можлива маніпуляція на користь окремих груп
	Автоматизація збору даних про громадську думку	Підвищення точності виявлення трендів і настроїв громад	Низький рівень учасників опитувань, відсутність критичних даних для аналізу

Джерело: сформовано автором на підставі [300-303]

На практиці eGovPro в Україні відіграють важливу роль у забезпеченні прозорого управління. Наприклад, платформа «Єдиний вебпортал використання публічних коштів» [300] дає змогу громадянам отримувати інформацію про бюджетні витрати та проводити власний аналіз фінансових операцій у режимі реального часу, що сприяє виявленню неефективного використання ресурсів. Платформа електронної демократії «e-dem.ua» [301] забезпечує можливість безпосередньої участі громадян у суспільно важливих процесах шляхом розробки ініціатив, які можуть бути розглянуті органами місцевого самоврядування. У багатьох випадках це створює умови для врахування громадської думки під час формування місцевої політики та ухвалення управлінських рішень.

Інтерактивні бюджетні панелі дають змогу громадянам стежити за розподілом бюджетних коштів, що особливо важливо в періоди масштабних державних проєктів чи соціальних ініціатив. Платформа «Консультації з громадськістю» [302] надає можливість організовувати онлайн-дискусії, що

заохочує враховувати пропозиції та зауваження громадян під час розробки нормативно-правових актів. Це формує основу для побудови системи управління, заснованої на принципах відкритості, прозорості та співпраці.

Одним із прикладів розширення цифрових можливостей взаємодії між державою та громадянами є застосунок «Дія» [303], який став основним інструментом цифрової трансформації публічного управління в Україні, що дає можливість громадянам отримувати доступ до державних послуг безпосередньо зі смартфона, а це значно спрощує адміністративні процеси та мінімізує бюрократичні перепони.

«Дія» інтегрує цифрові документи, такі як паспорт, ідентифікаційний номер та водійське посвідчення, що сприяє зручності в повсякденному житті та взаємодії з державними установами. Крім того, через цей застосунок можна подавати заяви на отримання соціальних виплат, реєструвати бізнес, а також брати участь у громадських опитуваннях і голосуваннях щодо суспільно важливих питань.

Запровадження «Дії» сприяє підвищенню рівня доступності державних послуг, що особливо актуально для населення у віддалених регіонах. Крім того, цей інструмент зміцнює принципи прозорості та підзвітності завдяки можливості швидкого доступу до інформації та контролю за статусом поданих запитів. Функціонал «Дії» продовжує розширюватися, охоплюючи нові послуги та можливості, що підтверджує ефективність цифрових рішень у контексті модернізації публічного управління та активізації громадянської участі [290, с. 112].

Інтегроване відкрите управління є основним напрямом розвитку сучасних державних систем у багатьох країнах світу, що сприяє підвищенню прозорості та підзвітності публічного управління завдяки цифровим технологіям і відкритим даним. Ця модель управління ґрунтується на використанні платформ доступу до відкритих даних, електронних консультацій та моніторингу державних програм, що забезпечує активну участь громадськості в прийнятті рішень. Міжнародний досвід свідчить, що

успішна реалізація інтегрованого відкритого управління залежить від технологічної інфраструктури, ефективної нормативно-правової бази та рівня цифрової компетентності громадян. Перехід до цієї моделі потребує не лише технологічних інновацій, але й фундаментальної трансформації організаційної культури державних установ, відмову від ієрархічних структур на користь гнучких мережевих взаємодій між стейкхолдерами.

У багатьох країнах Європи та Північної Америки впроваджено комплексні системи відкритого управління, які стали зразком для інших держав. Зокрема, інтегровані платформи забезпечують взаємодію громадськості з державними установами, контроль за використанням бюджетних коштів та обговорення суспільно значущих рішень (табл. 3.5).

Таблиця 3.5

Основні елементи інтегрованого відкритого управління в міжнародній практиці

Країна	Основні елементи інтегрованого відкритого управління	Релевантні практики для України	Потенційні переваги для України
Естонія	Платформа X-Road для обміну даними між державними установами; забезпечення цілісного цифрового середовища для громадян і бізнесу	Упровадження єдиного цифрового простору для інтеграції державних реєстрів	Підвищення ефективності міжвідомчого обміну інформацією та зменшення бюрократії
	Розробка інтегрованих електронних послуг, доступних громадянам через єдиний інтерфейс	Впровадження єдиного інтерфейсу для доступу до послуг та інформації державних установ	Підвищення зручності для громадян і бізнесу у спілкуванні з державою
Велика Британія	Портал «Data.gov.uk» для розкриття даних; система публікації відкритих даних для забезпечення прозорості держави	Створення централізованого порталу з розширеними можливостями моніторингу державних витрат	Підвищення прозорості бюджетного процесу і управління фінансами
	Інтегровані сервіси бюджетної прозорості, що дозволяють громадянам контролювати державні витрати	Розробка інструментів для аналізу виконання бюджету з можливістю зворотного зв'язку	Підвищення довіри до держави шляхом залучення громадян до контролю за фінансами

Продовження таблиці 3.5

Країна	Основні елементи інтегрованого відкритого управління	Релевантні практики для України	Потенційні переваги для України
Франція	Платформа «data.gouv.fr» з доступом до інформації про державні закупівлі, соціальні проєкти та статистику	Інтеграція відкритих реєстрів закупівель разом з оприлюдненням звітів про реалізовані контракти	Краща прозорість у сфері державних закупівель, запобігання корупції
	Надання відкритих даних про державні витрати для громадськості та бізнесу	Створення механізмів для аналізу і публікації даних про витрати	Стимулювання конкуренції серед постачальників завдяки відкритим даним
Канада	Платформи електронних консультацій та електронного голосування на всіх рівнях влади	Упровадження багаторівневих платформ для електронних консультацій у національному та регіональному форматах	Залучення більшої кількості громадян до процесу ухвалення рішень
	Використання цифрових платформ для активізації громадських обговорень та залучення до прийняття рішень	Впровадження системи збору побажань та коментарів від громадян	Підвищення рівня демократії і відповідальності перед громадськістю
Німеччина	Платформа «GovData» для доступу до наборів відкритих даних; інтерактивні платформи для обговорення нормативних актів	Розширення функціоналу електронних сервісів для інтерактивного обговорення законодавчих ініціатив	Активізація участі громадян у формуванні законодавства
	Підтримка комплексного доступу до даних та платформи для візуалізації даних для покращення розуміння їх змісту	Інтеграція з технологіями для візуалізації даних у зручному форматі	Поліпшення комунікації між громадянами та органами державної влади

Джерело: сформовано автором на підставі [291, с. 78-80; 293;304-308]

Досвід Естонії демонструє на практиці ефективність створення єдиної цифрової платформи для взаємодії між державними установами та громадянами [304], що дає можливість здійснювати доступ до державних послуг онлайн та значно скорочує час обробки запитів. У Великій Британії портал «Data.gov.uk» [305] надає відкритий доступ до великої кількості

наборів даних, які використовуються для досліджень та громадського моніторингу. Це сприяє прозорості управлінських процесів та покращує звітність державних органів.

У Франції платформа «data.gouv.fr» [306] дає змогу отримувати інформацію про фінансування державних програм та соціальні ініціативи, що підвищує підзвітність щодо використання бюджетних коштів. У Канаді активно використовуються платформи електронних консультацій, які забезпечують можливість громадянам долучатися до обговорення нормативних актів та соціальних проєктів у цифровому форматі [307]. Німеччина пропонує портал «GovData» [308], що поєднує функції доступу до відкритих даних та інтерактивного обговорення урядових ініціатив.

Для України корисним є впровадження багатофункціонального порталу для відкритого доступу до даних державних закупівель, соціальних програм і бюджетних звітів, а також розвиток електронних консультаційних платформ на регіональному рівні [288, с. 108-109]. Це дасть можливість забезпечити прозорий процес прийняття рішень, розширити можливості громадського контролю та сформувати довіру до публічних інституцій. Водночас важливим є врахування аспектів кібербезпеки та підтримки цифрової інфраструктури для безпечного обміну інформацією.

Серед важливих кроків у впровадженні відкритого врядування в Україні варто відзначити створення урядового вебсайту «Громадянське суспільство і влада» [309], що спрощує доступ до обговорення суспільно важливих проєктів і заходів уряду, а також функціонування центрів надання адміністративних послуг та Єдиного державного порталу адміністративних послуг. Окрему роль відіграють електронні петиції на офіційних сайтах Верховної Ради та Президента України, які забезпечують прямий канал комунікації між громадянами та владою.

Запроваджені електронні системи, такі як Prozorro [310] та Національний портал відкритих даних [311], стали ефективними інструментами підвищення прозорості державних закупівель і доступу до

інформації. Використання інформаційних технологій також передбачає сервіси для громадян, такі як електронний кабінет платника податків, онлайн-калькулятори субсидій і системи відстеження громадського транспорту [292, с. 65]. Упровадження таких елементів електронного врядування сприяє покращенню якості надання адміністративних послуг, підвищенню доступності інформації та посилює зв'язок між державними органами та громадськістю. Проте стабільність цього процесу потребує ефективного діалогу між владою, громадськими організаціями та громадянами, оскільки комунікаційні процеси відіграють вирішальну роль у формуванні, ухваленні та реалізації управлінських рішень.

Однією з основних проблем, пов'язаних з упровадженням інтегрованого відкритого управління, є цифрова нерівність, що характеризується обмеженим доступом до цифрових ресурсів у певних соціальних групах та регіонах. Ця нерівність проявляється у нерівномірному доступі до високошвидкісного інтернету, недостатній забезпеченості сучасними пристроями та низькому рівні цифрової грамотності. Особливо актуальною ця проблема є для сільських територій, де технічна інфраструктура часто відстає від стандартів, необхідних для ефективного використання електронних сервісів. Як наслідок, це обмежує можливості громадян брати участь у процесах електронного врядування та отримувати доступ до державних послуг.

Проблема кібербезпеки є не менш значущою, оскільки використання відкритих даних і цифрових платформ створює нові виклики для захисту інформаційних ресурсів держави та громадян. Зростання кількості кібератак на державні інформаційні системи підвищує потребу у впровадженні сучасних технологій для моніторингу та запобігання кіберзагрозам. Це потребує посилення контролю за безпекою каналів передачі даних, розробки політик управління ризиками та створення ефективних механізмів реагування на інциденти. Окрім того, важливим є впровадження міжнародних стандартів у сфері кіберзахисту та організація регулярного

аудиту безпеки державних платформ для виявлення потенційних загроз.

Захист персональних даних є одним із важливих аспектів упровадження інтегрованого відкритого управління, оскільки електронні платформи обробляють значні обсяги інформації про громадян [296, с. 28-30]. Це вимагає забезпечення належного рівня конфіденційності та дотримання прав користувачів на захист їхньої приватності. У багатьох випадках проблеми виникають через відсутність належних механізмів контролю за зберіганням і використанням даних, а також через обмежену поінформованість користувачів про свої права у сфері цифрової безпеки. Відсутність ефективної нормативно-правової бази або її неузгодженість із міжнародними стандартами може спричинити порушення конфіденційності та неправомірне використання персональних даних. З огляду на це одним із важливих напрямів є впровадження прозорих процедур використання даних та створення механізмів зворотного зв'язку для громадян щодо управління їхньою інформацією.

Створення ефективної нормативно-правової бази для запровадження інтегрованого відкритого управління є важливою умовою забезпечення прозорості, підзвітності та інклюзивності державних процесів. Основна мета нормативного регулювання полягає у формуванні комплексної системи правових актів, які визначають принципи обміну даними, правила обробки персональної інформації та механізми взаємодії між державними органами, громадянами та бізнесом. Ефективна нормативно-правова база має відповідати міжнародним стандартам, ураховувати національні особливості та адаптуватися до швидкого розвитку цифрових технологій.

У сучасних умовах цифровізації відбувається суттєва трансформація змісту і форм державних і суспільних ініціатив. eGovPro стають основним інструментом реалізації політик на державному рівні, забезпечуючи інтеграцію сервісів електронного урядування, систем моніторингу публічних фінансів та електронної взаємодії «держава – громадянин». Проте це створює нові виклики і проблеми, які необхідно вчасно виявляти та вирішувати.

eGovPro підтримують розвиток волонтерських рухів, краудфандингу, самоорганізації громад і горизонтальних мереж підтримки в умовах війни і криз. Справжня цінність цифровізації виявляється на стику державних і громадських ініціатив, де виникають інструменти спільного управління: електронні консультації, петиції, відкритий моніторинг виконання рішень. Важливо підкреслити, що саме синергія цих ініціатив, опосередкована цифровими платформами, може суттєво посилити соціальну згуртованість, проте вона також потребує належної правової бази для забезпечення її ефективності.

Одним з основних аспектів інтегрованого відкритого управління є розроблення та ухвалення законодавчих актів, що регламентують доступ і обробку персональних даних. Хоча це включає визначення категорій відкритих даних, процедур їх публікації і обмежень щодо конфіденційної інформації, існують істотні проблеми. По-перше, недостатня чіткість у законодавстві може призвести до неоднозначного тлумачення понять «великі дані» та «персональна інформація». Розгляд цих категорій можуть ускладнити нові технології, такі як штучний інтелект (ШІ), який активно використовує дані для навчання та прийняття рішень.

Важливим елементом є імплементація положень про прозорість діяльності державних органів, що передбачає регулярну публікацію звітів та інформації про прийняті рішення в зручних для аналізу форматах. Однак лише 40% органів влади в Україні регулярно публікують звіти, що підкреслює серйозну проблему недостатньої відкритості. Значним викликом є також регламентація використання цифрових платформ для проведення громадських консультацій та обговорень нормативних актів. Це вимагає створення ефективних правових механізмів, які б регулювали порядок електронних консультацій, їх терміни та процедури врахування отриманих пропозицій громадян. Наразі майже 60% консультацій не мають реального впливу на прийняття рішень, що веде до відчуження громадян від процесу управління (додаток Д).

У сфері кібербезпеки необхідно закріпити обов'язкові вимоги до захисту державних інформаційних систем, включаючи аудит та реагування на інциденти. Однак, наразі відсутні чіткі стандарти безпеки для систем електронного урядування, що підвищує ризики витоку персональних даних та кібератак. Також необхідно врахувати термін «кібер-загроза», який вживається для визначення нових форм ризиків, пов'язаних з динамічно змінюваним цифровим середовищем. Нормативні акти мають містити положення щодо сертифікації програмного забезпечення для відкритого управління та навчання персоналу органів влади основам захисту даних. Суттєвою проблемою є недостатня підготовка кадрів до роботи в умовах нових цифрових реалій. Крім того, варто регламентувати співпрацю між державними органами та громадськими організаціями у сфері моніторингу діяльності органів влади. Це може включати створення нових інструментів для громадського контролю. Поняття «громадський аудит» стає актуальним, оскільки має на меті активізацію процесів контролю за витратами державних коштів та реалізацією державних програм.

Запровадження правового механізму зворотного зв'язку є ще одним важливим напрямом, що дасть змогу громадянам повідомляти про проблеми у використанні цифрових сервісів і надсилати пропозиції щодо їх покращення. Це відповідно має на увазі створення терміну «цифровий зворотній зв'язок», що передбачає систематичний збір думок користувачів у формі електронних опитувань та анкетування. Важливим напрямом є впровадження багаторівневих систем навчання для підвищення рівня цифрової грамотності серед громадян і працівників державного сектору. Необхідно розробити концепції підвищення «цифрової компетентності», що включають навчальні програми та семінари. Це дозволить забезпечити належний рівень освіти для всіх верств населення, зокрема для тих, хто недостатньо володіє технологіями.

Перспективи подальших досліджень передбачають поглиблене вивчення механізмів адаптації міжнародного досвіду до українського

контексту, аналіз ефективності вже наявних електронних платформ та оцінку впливу цифрових інновацій на якість прийняття рішень у публічному управлінні. Зокрема, варто дослідити концепцію «індикаторів цифрового успіху», що дозволить вимірювати ефективність впроваджуваних ініціатив. Урахування цих аспектів сприятиме створенню стійкої системи відкритого управління, здатної забезпечити сталий розвиток цифрового суспільства та підвищити довіру громадян до державних інституцій. Таким чином, інтегроване відкрите управління може стати основою для зміцнення зв'язків між державою та суспільством, забезпечуючи активну участь громадян у процесах ухвалення рішень та створюючи умови для розбудови демократичного правління в Україні.

3.3. Цифрові управлінські платформи як фактор зміцнення соціальної стабільності та безпеки функціонування управлінських систем

Сучасний світ характеризується наявністю викликів, які вимагають від управлінських структур не лише швидкої адаптації, але й інноваційних рішень. Цифрові управлінські платформи (eGovPro) стають важливими інструментами в управлінні, оскільки вони здатні ефективно вирішувати складні задачі і забезпечувати гнучкість у прийнятті рішень. eGovPro не лише автоматизують процеси, але й формують нові механізми участі громадян у державному управлінні, що, в свою чергу, сприяє соціальній стабільності та безпеці. У безпековому вимірі вони підтримують системи раннього попередження, моніторинг загроз та координацію реагування; у соціальному – забезпечують доступність послуг, адресність допомоги та зменшення нерівності в доступі до ресурсів; в інституційному – сприяють прозорості, підзвітності й зниженню корупційних ризиків; у когнітивному – формують нові практики взаємодії з державою, підтримують інформаційну стійкість і національну ідентичність у цифровому середовищі.

В умовах сучасної динамічної та складної соціально-економічної

ситуації, управлінські системи зазнають дедалі більшого тиску на ефективність, прозорість і адаптивність. Для досягнення цих цілей важливо спиратися на певні ключові принципи, які можуть бути інтегровані в концепцію функціонування eGovPro [312]. Ці принципи – зворотний зв’язок, адаптивність і модульність – є базовими для забезпечення комплексного підходу до управління.

По-перше, *принцип зворотного зв’язку*, що є критично важливим елементом, який забезпечує постійне вдосконалення процесів і рішень. Завдяки функції зворотного зв’язку системи можуть отримувати інформацію про результати своїх дій. Це дозволяє вчасно коригувати стратегії, залежно від змін у зовнішньому середовищі чи внутрішніх показниках ефективності.

У рамках eGovPro принцип зворотного зв’язку можна реалізувати через інтеграцію систем моніторингу та аналітики, які постійно оцінюють результати управлінських рішень. Наприклад, у системах електронного урядування зворотний зв’язок може бути організований через платформу для збору думок громадян про якість отримуваних адміністративних послуг. Цей механізм не лише підвищує рівень прозорості, але й забезпечує можливість швидко реагувати на потреби суспільства, що є надзвичайно актуальним у контексті швидкоплинних змін.

По-друге, *адаптивність* є ключовим принципом, що охоплює можливість системи змінювати свою поведінку залежно від зовнішніх умов або внутрішніх параметрів. У сучасному управлінні важливо, щоб системи могли швидко і ефективно реагувати на нові виклики: зміна законодавства, соціальні рухи чи навіть економічні кризи. Такі умови вимагають гнучкості в процесах управління, що забезпечить стабільність і стійкість системи. В рамках eGovPro адаптивність може бути реалізована шляхом використання аналітичних платформ, які здійснюють моніторинг змін у зовнішньому середовищі. Ці платформи можуть використовувати дані в реальному часі для оцінки ситуацій та автоматичного коригування процесів. Наприклад, система управління громадськими витратами може швидко адаптуватися до

змін у фінансовій ситуації, забезпечуючи при цьому прозорість і підзвітність.

По-третє, модульність – означає, що системи повинні складатися з незалежних модулів, які можуть функціонувати окремо або у взаємозв'язку. Модульність є основою інституціонального дизайну eGovPro, що дозволяє створювати й інтегрувати нові елементи в існуючі системи без істотних витрат часу і ресурсів. У цифрових управлінських платформах модульність може бути реалізована через використання мікросервісної архітектури, де кожен компонент відповідає за виконання специфічних функцій. Це дає змогу організаціям швидше розвивати нові функції або змінювати існуючі без ризику для загальної стабільності системи. Наприклад, у системі електронного голосування модулі можуть бути спеціально розроблені для аутентифікації виборців, обробки голосів або створення звітності, що дозволяє зберігати високу якість та надійність цілого процесу.

Окремо важливо розглянути принцип структурної композиції eGovPro. – *принцип інституційного дизайну*, який є ключовим у створенні цифрових управлінських платформ, завдяки своїй здатності адаптуватися і реагувати на зміни в умовах, у яких функціонують державні інститути. Цей принцип підкреслює важливість структурного підходу до організації систем, де функціональні модулі можуть бути інтегровані і налаштовані відповідно до вимог користувачів та зміни суспільних умов. Інституційний дизайн базується на модульній архітектурі, що дозволяє компонуванню незалежних елементів, які можуть виконувати специфічні завдання в рамках комплексної системи. Основною перевагою принципу інституційного дизайну є можливість швидкого впровадження змін, що є необхідною умовою для адаптації до нових викликів і вимог суспільства. Цифрові управлінські платформи, які реалізують цей принцип, здатні швидко оновлювати, змінювати або додавати нові модулі без значних зусиль у перебудові всієї архітектури системи. Наприклад, у системі електронного урядування модуль аутентифікації або модуль обробки даних можуть бути змінені, щоб впроваджувати нові методи доступу або управління даними без впливу на

інші компоненти, що забезпечує безперервність та стабільність функціонування платформи.

Проте, у реалізації принципу інституційного дизайну існують певні виклики. Складність управління взаємозв'язками між модулями може призводити до потенційних проблем із інтеграцією. Необхідно забезпечити чітку координацію та ефективне спілкування між компонентами, щоб зменшити ризики та запобігти дисфункції системи. Це вимагає додаткового зусилля в управлінні та уваги до налаштування інтерфейсів між модулями.

Яскравим прикладом застосування принципу інституційного дизайну в цифрових управлінських платформах є архітектура систем електронного голосування. У таких системах модулі можуть бути спеціально розроблені для аутентифікації виборців, обробки голосів та створення звітності. Кожен модуль може функціонувати автономно, але при цьому забезпечує інтеграцію з іншими, що спрощує управління і дозволяє швидко адаптувати систему до нових вимог, наприклад, введення нових методів голосування або зміни в законодавстві.

Принцип інституційного дизайну також підтримує швидке впровадження інновацій. Оскільки організації мають змогу легко комбінувати та налаштовувати різні модулі, вони можуть швидко тестувати нові ідеї або функціональності. Цей підхід дозволяє значно знизити терміни реалізації нових проєктів, зменшуючи витрати на розробку та програми тестування. Більше того, принцип інституційного дизайну сприяє зміцненню соціальної стабільності та безпеки функціонування управлінських систем. Ефективна та адаптивна цифрова платформа дозволяє державним інститутам швидше реагувати на соціальні виклики та потреби населення, таким чином створюючи довіру до державних структур. Це, в свою чергу, підвищує загальний рівень безпеки та стабільності в суспільстві, оскільки громадяни відчують, що їхні інтереси забезпечуються, а питання вирішуються оперативно і професійно (таблиця 3.6).

Таблиця 3.6

Реалізація принципу інституціонального дизайну в концептуалізації eGovPro

Аспект	Принцип інституційного дизайну	Традиційні управлінські системи	Примітки	Емпіричні приклади
Структура	Модульна архітектура дозволяє інтеграцію незалежних компонентів, які можуть бути легко додані або змінені відповідно до потреб. Завдяки цьому, системи можуть швидко адаптуватися до змін у середовищі	Формальна структура, зазвичай централізована, що ускладнює швидку адаптацію і оновлення. Важко здійснювати зміни без значних зусиль	Модульна структура сприяє гнучкості та стратегічному розвитку управлінських практик, а також дозволяє упроваджувати нові технології без значних витрат на перепроєктування	Наприклад, система eGovPro в Україні за період 2020-2023 років зменшила середній час обробки документів на 30%, що доводить ефективність модульної архітектури
Гнучкість	Висока гнучкість у адаптації до змін, що відбуваються в суспільстві та на ринку. Це дозволяє системам впроваджувати нові функції та технології без значних зусиль	Гнучкість обмежена, що призводить до затримок у реакції на зміни. Зміни потребують тривалих узгоджень і процедур, що уповільнює процеси	Гнучкість системи стимулює швидке реагування на зовнішні зміни і виклики, що є критично важливим в умовах сучасної динаміки	Після запровадження нових заходів під час пандемії COVID-19, країни, які швидко адаптували онлайн-системи, такі як телемедицина, зафіксували зростання задоволення пацієнтів на 40%
Адаптація до змін	Швидка адаптація до змін в умовах, що постійно змінюються, забезпечує прийняття нових політик та технологічних рішень, зокрема у сфері освіти, охорони здоров'я та соціальних послуг	Повільна адаптація; система часто зазнає затримок через процедури, що ускладнюють терміни виконання рішення	Своєчасна адаптація є ключовим чинником для ефективного функціонування та уникнення кризових ситуацій	У Сінгапурі система Smart Nation за 2 роки впровадила нові технології для управління трафіком, скоротивши затори на 20% завдяки використанню даних у реальному часі
Стабільність	Принцип інституційного дизайну дозволяє зберігати стабільність, навіть коли вносяться зміни до окремих компонентів системи, що знижує ризик відмови	Стабільність може бути поставлена під загрозу при внесенні змін, які нерідко призводять до перебоїв у системах. Втрата довіри з боку громадян може бути критичною	Безперебійна робота систем є необхідною для підтримки довіри громадян до державних інститутів	В Естонії, під час переходу на електронне голосування, система показала 99.8% успішного виконання без помилок, що підвищило довіру виборців до виборчого процесу

Продовження таблиці 3.6

Управління взаємо-відносинами	Вимога високої координації між модулями, що забезпечує успішну інтеграцію та взаємодію. Зручні інтерфейси забезпечують актуальність інформації	Зазвичай проста та ієрархічна структура, що ускладнює рішення та створює ситуації для конфліктів	Слід забезпечити ефективну комунікацію між усіма складовими системи для запобігання можливим суперечкам	В Іспанії впровадження цифрової адміністрації дозволило зменшити конфлікти між міністерствами на 30%, покращивши взаємодію та знижуючи бюрократію
Швидкість інновацій	Швидке впровадження інновацій, що дозволяє організаціям набутися конкурентних переваг через новітні технології та послуги. Запровадження нових рішень відбувається в стислі терміни	Обмеження інновацій через затримки у внутрішніх процесах, що впливають на загальну ефективність. Ресурси і часові витрати потребують більшого часу на реалізацію	Баланс між впровадженням новітніх технологій і управлінням ресурсами є важливим для оптимізації роботи системи.	У США платформа Change.gov впровадила більше 300 нових ініціатив протягом одного року, що дозволило зафіксувати підвищення задоволеності громадян на 25% завдяки швидкому реагуванню на потреби
Соціальна стабільність	Підтримує соціальну стабільність та довіру населення через ефективний доступ до послуг і швидке реагування на потреби	Висока бюрократія може призводити до негативних реакцій та невдоволення з боку громадян	Довіра до державних інститутів забезпечується через ефективність і прозорість їх діяльності	У Швеції впровадження системи електронних послуг підвищило рівень задоволеності населення на 20%, що є сильним показником соціальної стабільності
Безпека функціонування	Підвищує безпеку державних систем шляхом швидкої реакції на кризові ситуації та виклики. Комплексний підхід до управління ризиками	Низька готовність до швидкого реагування на ризики досі є проблемою в багатьох традиційних системах	Забезпечення готовності до криз у державному управлінні є ключовим для захисту здоров'я та збереження життя громадян	В Норвегії система управління НС забезпечує реагування у реальному часі, що призвело до зниження ризиків на 30% під час природних катастроф
Приклад застосування	Системи електронного голосування та різноманітні платформи для електронного урядування демонструють ефективність реалізації принципів інституційного дизайну в практиці	Традиційні системи, такі як централізовані документообіги, часто відстають у порівнянні з новими технологіями через обмеженість функціоналу	Практики з eGovPro демонструють не лише ефективність, а й прогресивність в управлінні сучасними технологіями	Наприклад, електронне голосування в Естонії, яке стало першим у світі з використанням технології блокчейн, забезпечило повну інтеграцію та довіру серед виборців, з 40% голосів, поданих онлайн

Джерело: розроблено автором на основі аналізу [313-316]

Отже, принцип інституційного дизайну, як засадничий для створення цифрових управлінських платформ (eGovPro), слугує важливим інструментом для забезпечення їхньої гнучкості, відповідності та здатності

швидко адаптуватися до змінюваних умов ринку та вимог користувачів. Реалізація цього принципу в управлінських системах суттєво підвищує їхню ефективність та стійкість, що є критично важливим у сучасному управлінні, зокрема в контексті забезпечення соціальної стабільності та підвищення рівня безпеки.

Комплексне впровадження принципу інституційного дизайну дозволяє створити ефективні механізми управління, від державного до локального рівня. Саме завдяки цим принципам управлінські системи можуть реагувати на зміни в суспільстві, забезпечуючи при цьому стабільність та безпеку: ефективність у прийнятті рішень, підвищення довіри громадськості, гнучкість і готовність до змін, можливість масштабування та вдосконалення. При цьому позитивний вплив eGovPro залежить від рівня захисту даних, якості управління ризиками, інклюзивності цифрових сервісів і здатності держави протидіяти інформаційним маніпуляціям (таблиця 3.7).

Таблиця 3.7

Впровадження інклюзивних цифрових сервісів

Аспект	Зміст	Зарубіжний досвід	Україна
Захист даних	Високий рівень захисту особистих та державних даних є критично важливим для забезпечення довіри до цифрових платформ	У 2020 році 35% громадян європейських країн були впевнені у безпеці даних при використанні е-послуг. Після впровадження нових протоколів шифрування в Скандинавії, цей показник зріс до 65%	В Україні, після початку агресії РФ у 2022 році, державні органи ввели нові стандарти захисту даних, включаючи систему реалізації стандартів ISO 27001, що підвищило рівень довіри до цифрових послуг на 25%
Якість управління ризиками	Ефективне управління ризиками дозволяє організаціям мінімізувати наслідки загроз, що виникають під час використання цифрових платформ	За даними OECD, країни з високим рівнем інтеграції управління ризиками, такими як Норвегія та Фінляндія, змогли зменшити збої у наданні державних послуг під час пандемії COVID-19 на 30%	Під час війни в Україні зростання загроз змусило державу впровадити систему управління ризиками, що включає постійний моніторинг кібератак та реагування на них, що дозволило зменшити успішність атак на 40%
Інклюзивність цифрових сервісів	Здатність цифрових платформ надавати доступ до послуг для всіх верств населення, включаючи вразливі групи	У Канаді 80% населення, яке користується електронними послугами, заявили про легкість доступу до державних сервісів. Програма Digital Canada 2020 включила дії, які забезпечили інклюзивність для 10 мільйонів людей	В Україні 70% мало-забезпечених родин отримали доступ до соціальних сервісів через онлайн-платформи в умовах війни, що підвищило інклюзію. 85% користувачів задоволені новими інклюзивними сервісами

Продовження таблиці 3.7

Аспект	Зміст	Зарубіжний досвід	Україна
Протидія інформаційним маніпуляціям	Активні заходи протидії дезінформації та інформаційним маніпуляціям забезпечують чесність і прозорість державних платформ	У Фінляндії була впроваджена кампанія з навчання громадян, яка з 2016 року зменшила вплив дезінформації на 50%. Результати свідчать про зростання медіаграмотності серед населення до 76% проти 45% на початку кампанії	В Україні з початку війни запущено декілька кампаній протидії дезінформації, у тому числі через соціальні мережі, що зменшило вплив пропаганди на 35%. У 2023 році близько 70% населення повідомили про підвищення розуміння дезінформації
Протидія корупції	Запровадження прозорих і підзвітних систем управління сприяє зменшенню корупційних проявів у державному секторі	Дослідження Transparency International показують, що країни з високими показниками цифровізації мають нижчий рівень корупції. Наприклад, у Латвії запровадження електронного урядування зменшило корупцію на 20%	В Україні завдяки проекту «Прозорро» у сфері закупівель у 2022 році було зафіксовано економію понад 50 мільярдів гривень (близько 2 мільярдів доларів), що є наслідком прозорих тендерних процедур
Суспільні проекти	Розвиток суспільних проектів через цифрові платформи має великий потенціал для залучення громадян до процесів прийняття рішень	У Сінгапурі програма участі громадян у бюджеті дозволила збільшити залученість населення до 40%. Суспільні проекти, запропоновані громадянами, мають високий рівень реалізації	В Україні програма «Громадський бюджет» охопила 10083 проекти, сприяє розвитку місцевих інфраструктур і послуг. Кількість реалізованих проектів зросла на 45% (Дніпропетровська область 1187 проектів)
Державницькі реформи	Запровадження комплексних реформ у державному управлінні з використанням цифрових платформ сприяє підвищенню ефективності та прозорості	Країни, які здійснюють широкомасштабні реформи в сфері державного управління, демонструють поліпшення показників ефективності. Як приклад, Грузія після реформ у 2003 році покращила рейтинг Doing Business на 60%	В Україні за період з 2014 року реалізовано ряд реформ, зокрема децентралізацію, яка дала змогу місцевим громадам отримати більшу автономію і бюджет, завдяки чому обсяг інвестицій у розвиток інфраструктури зріс на 30% у 2021 році
Цифровізація управління	Запровадження ЦТ у державне управління підвищує ефективність, скорочує бюрократію та прискорює процеси прийняття рішень	Дослідження Всесвітнього банку показали, що країни, які активно запроваджують цифрові рішення в управлінні, демонструють зменшення часу на отримання послуг до 50%	В Україні цифровізація державного управління, зокрема через ініціативу «Держава в смартфоні», дозволила скоротити час отримання адмін.послуг до 30%, зокрема в сфері реєстрації бізнесу та надання соціальних послуг

Джерело: систематизовано автором на основі [317;318]

Феномен eGovPro варто формалізувати через поєднання інституційного, функціонального, технологічного й соціального аспектів. Саме тому eGovPro мають розглядатися як інтегровані блоки екосистеми

National E-Resilience, які забезпечують циркуляцію даних між рівнями та секторами управління, перетворення даних на управлінські рішення, зворотний зв'язок між державою, суспільством і бізнесом, а також інституціоналізацію й масштабування суспільних ініціатив. Адже eGovPro в Україні стали важливими інструментами для забезпечення ефективності та прозорості управлінських практик. Інтеграція інституційних, функціональних, технологічних та соціальних аспектів у цю екосистему дозволяє створити стійке управління, здатне адаптуватися до змін і викликів сучасності. Перспективи на майбутнє включають подальшу цифровізацію держуправління, що підвищить рівень послуг для громадян та зміцнить взаємодію між державою і суспільством в умовах динамічного і непередбачуваного середовища.

В умовах трансформаційних змін у технологічному та соціальному середовищі, Україна на шляху до впровадження цифрових управлінських платформ стала свідком численних трансформацій у державному управлінні. eGovPro сьогодні розглядаються як інтегровані вузли в екосистемі національної моделі стійкості (National E-Resilience), які забезпечують циркуляцію даних, зворотний зв'язок та інституціоналізацію суспільних ініціатив. Важливо зазначити, що цифрові управлінські платформи відіграють критичну роль у забезпеченні соціальної стабільності та безпеки функціонування управлінських систем в Україні.

Декларація про державний суверенітет України 1990 р. стала першим кроком до створення гнучкої та сучасної системи управління. Після проголошення незалежності [319]. Акт проголошення незалежності України 24 серпня 1991 р. Україні визначив потребу адаптувати адміністративну систему до нових економічних і політичних реалій [320]. Наслідком цього став процес формування нових державних інститутів, реформування управлінських структур та необхідність модернізації державних послуг. Однак, попри намагання впроваджувати електронні технології, більшість державних послуг залишалася традиційними, що викликало значні труднощі

у забезпеченні ефективності управління.

Однак, на початкових етапах комп'ютеризація державних структур відбувалася повільно. У результаті недостатньої технічної бази, інформаційні системи залишалися переважно паперовими. У цей період не було системного підходу до впровадження технологій, і адміністративні процеси відбувалися в умовах нерегулярного фінансування та недостатньої інвестиційної підтримки. У 1995 році було прийнято Закон України «Про інформацію», який визначав основи інформаційних технологій в Україні, але реалізація даного закону була недостатньо активною [321]. Відсутність чіткої стратегії цифровізації привела до хаотичних ініціатив, що ще більше ускладнювало процес. Після здобуття незалежності Україні не вдалося налагодити ефективну інфраструктуру для впровадження електронних послуг. Брак належного обладнання, низька швидкість інтернету, а також відсутність технічного обслуговування призводили до обмеження можливостей запровадження нових технологій. Багато працівників державних установ не мали достатнього рівня комп'ютерної грамотності. Це ускладнювало впровадження цифрових інструментів та технологій, оскільки адміністративний персонал часто не був готовий до роботи в новому цифровому середовищі. Відсутність чіткої політичної волі і підтримки з боку державної влади затримувала впровадження електронних ініціатив. Відсутність державної стратегії в цій сфері свідчила про те, що електронізація не вважалася пріоритетом, хоча існувала гостра потреба у цій трансформації. Україна отримала міжнародну допомогу для розвитку технологічної інфраструктури. Однак становлення таких проектів часто уповільнювалося через нестачу координації на державному рівні. Програми співпраці з міжнародними організаціями, зокрема ПРООН, розвивали окремі елементи електронного управління, але їх реалізація потребувала державних гарантій і інституційної підтримки. Всі ці фактори призвели до усвідомлення необхідності реформ у сфері електронного управління.

Концепція формування системи національних електронних

інформаційних ресурсів, затверджена постановою КМУ від 2003 року, сформувала основу для створення національної системи електронних інформаційних ресурсів, що дозволила: визначити стратегію формування, використання та захисту національних електронних ресурсів, сприяти інтеграції інформаційних ресурсів у державному управлінні для покращення доступу громадян до інформації. У Концепції було визначено ключові терміни, які стануть в нагоді для подальшого аналізу: 1) національні ресурси – інформація незалежно від її змісту, форми, та призначення, що забезпечує потреби громадян, суспільства та держави; та 2) система національних ресурсів – організована сукупність національних ресурсів, необхідних для вирішення завдань соціально-економічного розвитку. Водночас, у концепції вказано на проблеми формування системи національних ресурсів: галузевий принцип інформатизації, що обмежує використання ресурсів, відсутність правових норм для регулювання доступу до інформації, непридатність суспільних відносин у контексті сучасних викликів інформаційних технологій [322].

22 травня 2003 року був прийнятий Закон України «Про електронні документи та електронний документообіг», який став важливим кроком у правовому регулюванні електронної інформації в Україні. Основні терміни і визначення, викладені в законі, становлять основи, на яких ґрунтуються подальші правові та технологічні ініціативи в галузі електронного управління:

1) *електронний документ* – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Це визначення свідчить про те, що електронний документ є повноцінним документом з усіма правами та обов'язками, що виникають у результаті його використання;

2) *електронний документообіг (обіг електронних документів)* – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів,

які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів;

3) *електронний підпис* (прямого визначення у законі не наведено) – аналог підпису на паперовому документі, який застосовується для підтвердження достовірності і цілісності електронного документа. Електронний підпис є ключовим елементом електронного документообігу, забезпечуючи юридичну силу документів на електронних платформах;

4) *суб'єкти електронного документообігу* – автор, підписувач, створювач електронної печатки, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу. *Отже, це фізичні та юридичні особи, які беруть участь у процесах створення, обробки та передачі електронних документів.*

Визначення, надані в Законі, свідчать про усвідомлення потреби у чіткому правовому регулюванні електронного документообігу. Якість цих визначень є достатньо високою, оскільки вони надають базу для подальших правових норм і технологічних рішень. Однак, у контексті швидко змінюваної технологічної екосистеми Україні необхідно регулярно оглядати та оновлювати ці визначення, щоб вони відповідали актуальним технологіям та міжнародним стандартам. Для прикладу, з упровадженням нових технологій, таких як блокчейн, може виникнути потреба в уточненні статусу електронних документів, видів електронного підпису або нових форм взаємодії суб'єктів. Адже очевидно, що цифрові управлінські платформи в Україні, такі як «Дія», покликані спростити доступ громадян до державних послуг через автоматизацію та цифровізацію процесів управління. Легітимність і ефективність таких платформ безпосередньо залежить від законодавчої бази, закладеної в Законі про електронні документи. Вони не лише надають можливість громадянам використовувати електронні сервіси, але й полегшують адміністративні процедури для державних органів (таблиця 3.8).

Таблиця 3.8

Формалізація цифрових управлінських платформ у контексті Закону України
«Про електронні документи та електронний документообіг»

Аспект	Норми закону	Цифрові управлінські платформи	Сфера охоплення громадян	Вплив норм закону на eGovPro
Сфера дії	Регулює відносини щодо електронних документів і документообігу	Інтегрує електронні документи у державні послуги для громадян	67% усіх адміністративних послуг на платформі «Дія» реалізується через електронні документи	Висока навантаженість на процеси обробки документів і систему управління даними
Правова основа	Визначає правовий статус електронних документів	Базується на законах про електронні документи, формуючи правове поле для впровадження	Правила реєстрації 95% електронних документів затверджені відповідно до законодавства	Середня навантаженість, оскільки потребує постійного оновлення правових норм
Електронний підпис	Використовується для підтвердження справжності електронних документів	Необхідний для автентифікації користувачів і захисту даних	За даними, 80% державних послуг вимагають електронного підпису, що підвищує зручність для користувачів	Висока, оскільки забезпечення електронного підпису є критично важливим для довіри
Організація документообігу	Визначає процеси створення, обробки та обміну електронними документами	Реалізує автоматизацію процесів документообігу через цифрові платформи	У 2023 році оброблено більше 3 мільйонів електронних документів через державні електронні сервіси	Висока навантаженість на управлінські системи через великий обсяг документів
Забезпечення безпеки	Встановлює вимоги до захисту інформації в електронних документах	Включає заходи щодо забезпечення інформаційної безпеки на рівні платформ	70% платформ реалізують двофакторну автентифікацію для підвищення безпеки	Висока, оскільки безпека є ключовим чинником для довіри до цифрових сервісів
Управлінська структура	Кабінет Міністрів України відповідає за реалізацію політики електронного документообігу	Платформи потребують координації між різними державними організаціями	Відзначено 25% зусиль держави на координацію між різними відомствами для здійснення електронного документообігу	Середня навантаженість на управлінські структури, потребує удосконалення
Доступність інформації	Вимагає забезпечення доступності електронних документів та підтвердження їх цілісності	Платформи повинні гарантувати швидкий та зручний доступ до державних послуг	90% громадян відзначають зручність та швидкість доступу до державних послуг через електронну платформу «Дія»	Висока навантаженість через великий обсяг запитів користувачів

Джерело: розроблено автором на основі [323]

З позицій впливу даного закону на цифрові управлінські платформи слід вказати на такі спеціальні правові інструменти:

1) забезпечення легітимності – оскільки інформація в електронних документах має такий самий статус, як і паперові документи, це дозволяє цифровим платформам надавати послуги, що вимагають юридичної певності;

2) аутентифікація – використання електронного підпису робить документи на цифрових платформах безпечними та підтверджує їх достовірність. Це особливо важливо, коли йдеться про угоди, договірні зобов'язання, або будь-які юридично значущі документи;

3) спрощення документообігу – закон визначає процедури електронного документообігу, що допомагає скоротити час обробки документів та зменшує адміністративні бар'єри, які традиційно існували в паперовому форматі.

З позицій формування сучасного формату eGovPro виступив також Закон України «Про електронний цифровий підпис» (від 22.05.2003 № 852). Варто виокреми такі категорії, наведені у цьому законі:

- електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

- електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

- засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису [324].

У 2017 р. цей закон припинив свою чинність, натомість було прийнято Закон України «Про електронну ідентифікацію та електронні довірчі

послуги», у межах якого фактично була побудована раціональна модель eGovPro (відповідно до авторської системної класифікації) [325]. Новий закон запроваджував важливі норми категорії для регулювання відносин у сфері цифровізації (загалом,

- електронна послуга – будь-яка послуга з надання певного матеріального чи нематеріального блага на користь іншої особи, яка надається через інформаційно-комунікаційну систему;

- електронний підпис – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис;

- електронні дані – будь-яка інформація в електронній формі;

- ідентифікація особи – процес використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, у результаті якого забезпечується однозначне встановлення фізичної, юридичної особи або уповноваженого представника юридичної особи та перевірка належності особі таких даних;

- інтероперабельність – технологічна сумісність технічних рішень, що використовуються для надання електронних послуг, та їх здатність взаємодіяти між собою;

- компрометація засобу електронної ідентифікації – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до засобу електронної ідентифікації [325].

У сукупності наведені закони України формують інтегровану правову системи для цифрових управлінських платформ, що забезпечує юридичну силу цифрових документів та підтвердження особи у межах автоматизованих сервісів. Законодавчі акти взаємодоповнюють один одного, створюють правову і технічну основу для сталого і безпечного розвитку цифрових управлінських платформ в Україні (таблиця 3.9).

Таблиця 3.9

Порівняльний аналіз Закону України «Про електронні документи та електронний документообіг» і «Про електронну ідентифікацію та електронні довірчі послуги» у контексті концепції цифрових управлінських платформ

Аспект	Закон України «Про електронні документи та електронний документообіг»	Закон України «Про електронну ідентифікацію та електронні довірчі послуги»	Ключові співвідношення з концепцією платформ	Навантаженість / виклики
Сфера застосування	Регулює створення, обробку і зберігання електронних документів	Регулює ідентифікацію і довірчі послуги для забезпечення безпеки платформ	Обидва закони закладають правову базу для безпечної інтеграції електронних сервісів	Висока потреба у нормативній гармонізації
Забезпечення юридичної сили	Забезпечує законодавче визнання електронних документів та підписів	Зазначає правила і сертифікацію електронних підписів та довірчих сервісів	Об'єднує механізми підтвердження і автентифікації для платформ	Висока навантаженість на технічний і правовий рівень
Аутентифікація користувачів	Не регулює безпосередньо автентифікацію, лише окремі аспекти підписання	Регулює процедури і механізми електронної ідентифікації та сертифікації	Основна роль у забезпеченні безпеки та довіри у платформі	Висока; критична для безпеки систем
Інфраструктура і засади	Визначає поняття електронного документа і документообігу	Визначає засади електронної ідентифікації, сертифікації та довірчого обслуговування	Комплементарність для створення цілісної платформи, від обміну документами до підтвердження особи	Висока, потребує цілісної інтеграції нормативів
Функціональні можливості	Врегульовує процеси обміну, зберігання і обробки електронних документів	Врегульовує процеси ідентифікації, підпису і підтвердження особи	Основа для створення автоматизованого документообігу і систем безпеки	Висока, що вимагає технічної й правової стандартизації
Безпека і довіра	Визначає вимоги до захисту електронних документів і їх цілісності	Визначає вимоги до електронних сертифікатів, довірчих сервісів, зокрема щодо безпеки і автентифікації	Ключові елементи забезпечення довіри в електронних платформах	Висока, оскільки системи мають бути захищені від зовнішніх і внутр. загроз
Реалізація та управління	Визначає механізми та органи контролю за використанням електронних документів	Регулює створення центрів сертифікації і управління довірчими послугами	Інфраструктурна базова частина для цілісних цифрових платформ	Висока, потребує централізованого управління та моніторингу
Взаємодія з користувачами	Стандартизація форматів і процесів роботи з електронними документами	Регулює рівні і процедури ідентифікації, сертифікації, довірчих послуг	Забезпечує єдину систему підтвердження особи для інтегрованих платформ	Висока, потребує широких інфраструктурних і правових заходів

Джерело: узагальнено автором на основі [323-325]

Наведені для аналізу закони України у поєднанні з авторською концепцією цифрових управлінських платформ формують цілісну систему, яка забезпечує юридичну силу електронної взаємодії, безпечне підтвердження особи і захищене електронне мовлення документів. За результатами досліджень, у 2022 році понад 75% державних послуг в Україні вже надавалися через електронні платформи. У 2024 р. понад 55% громадян упродовж 2024 року скористалися хоча б однією державною електронною послугою. 84% позитивно оцінили досвід їх отримання, що підтверджує зростаючу реальність їх застосування у сфері державного управління.

Розподіл найбільш популярних державних послуг у 2024 році:

- 1) застосунок чи портал «Дія» – 42%
- 2) послуги, що стосуються особистого транспорту – 15%
- 3) платні послуги отримання інформації з реєстрів – 13%
- 4) питання пенсійного забезпечення – 10%
- 5) отримання паспортів, інші контакти з Державною міграційною службою – 10%.

Відповідно до дослідження, серед людей до 30 років – понад 70% зверталися за ними упродовж року. Серед людей, віком понад 70 років, – 22%. Диференціація у розрізі віку пов'язана із інтенсивністю користуванням інтернетом, так із потребами різних вікових груп [326].

Висока навантаженість у цій системі пов'язана з необхідністю безперервного удосконалення правового регулювання, інфраструктурної підтримки та технічної безпеки. Наприклад, у 2023 році кількість електронних підписів, сертифікованих Центром сертифікації ключів, зросла більш ніж на 30%, що свідчить про дедалі активніше поширення довірчих послуг у цифровому просторі. Окрім того, кількість зареєстрованих документів у системах електронного документообігу за минулий рік сягнула понад 10 мільйонів, що говорить про масштабність і високу навантаженість відповідних систем. Для забезпечення належної роботоздатності таких

платформ Україна інвестує в інфраструктуру: у 2022 році було створено понад 50 центрів сертифікації ключів по всій країні, а також запроваджено багато елементів криптографічного захисту. Це дозволяє стабільно функціонувати системам і забезпечує високу рівень безпеки – зокрема, у 2023 році було зафіксовано всього 0,5% інцидентів, що пов'язані з компрометацією електронних сертифікатів, що говорить про високий рівень захищеності [326].

Отже, емпіричні дані свідчать: високий рівень навантаженості системи обумовлений дедалі більшим обсягом оброблюваних даних, розширенням сервісів та необхідністю постійної модернізації правового і технічного середовища. Це підтверджує актуальність і необхідність безперервного розвитку нормативної бази, інфраструктурних і технологічних складових для забезпечення сталого функціонування системи, що відповідає сучасним стандартам та потребам суспільства.

3.4. Запровадження алгоритму оцінки цифрової стійкості (Digital Resilience Assessment, DRA) у межах теоретичної концепції National E-Resilience

Сучасна теорія державного управління та корпоративного менеджменту тривалий час спиралася на парадигму «ефективності» та «стабільності». Існуючі інструменти оцінювання, такі як e-Government Development Index (EGDI) ООН [327], Digital Economy and Society Index (DESI) Європейської Комісії [328] або класичні аудити за стандартами ISO 27001 [329], фокусуються на лінійному прогресі, наявності сервісів або статичній захищеності периметра. Однак події 2022-2025 рр., зокрема збройна агресія РФ проти України, продемонстрували когнітивну несконанальність цих інструментів. Певна адміністративна система може мати високий індекс цифровізації послуг, але миттєво колапсувати при фізичному знищенні дата-центру або порушенні каналів зв'язку. Традиційні методології

вимірюють стан системи у «мирний час» (peace-time metrics), ігноруючи зміни параметрів системи в умовах екстремальної ентропії (war-time / crisis-time metrics). Отже, виникла нагальна потреба в інструменті, який би вимірював не стан (state) системи, а її потенціал до відновлення та адаптації (capacity to recover and adapt). Саме цей розрив між статичною безпекою та динамічною живучістю заповнює методологія *Digital Resilience Assessment (DRA)*.

У сучасних умовах глобалізації, цифрової трансформації та зростаючої залежності від інформаційних технологій питання забезпечення цифрової стійкості набуває надзвичайної актуальності. З урахуванням темпів розвитку цифрових управлінських платформ, зростання кіберзагроз і викликів, що постають перед державними інституціями, бізнесом і громадянським суспільством, необхідно сформувати й впровадити системний інструмент для об'єктивного аналізу та моніторингу рівня цифрової стійкості на національному рівні. На сучасному етапі розвитку інформаційного суспільства визначена потреба у створенні універсальної та практично налаштованої системи оцінювання цифрової спроможності та здатності системи швидко реагувати і відновлюватися після кібератак, технічних збоїв або інших негативних інцидентів. Аналіз світової практики показує, що ефективна оцінка цифрової стійкості базується на багатовекторному підході, який передбачає врахування інфраструктурної, кібернетичної, операційної та організаційної складових. Поточні тенденції у сфері цифрової безпеки та управління ризиками доводять, що традиційні підходи до оцінки безпеки вже недостатньо враховують рівень підготовки системи до довгострокових викликів і здатність до оперативного відновлення. Враховуючи ці обставини, українська національна сфера цифрової безпеки прагне впровадити інноваційний, цілісний підхід до вимірювання та підвищення рівня цифрової стійкості – саме це і закладено у концептуальну основу DRA.

З цих позицій National E-Resilience визначається як інтегрована модель управління державою, що забезпечує безперервність функціонування

публічних інституцій, безпеку громадян та економічну активність через тотальну цифрову трансформацію процесів прийняття рішень. В основі концепції лежить теза про те, що в умовах гібридної війни цифрова стійкість не є окремим технічним завданням (функцією ІТ-департаментів), а стає синонімом національної стійкості (НМС). National E-Resilience – це здатність держави використовувати цифрові інструменти для поглинання системних шоків (військових, економічних, соціальних) та швидкої реконфігурації ресурсів для відповіді на них. Концепція National E-Resilience базується на чотирьох взаємопов'язаних структурних елементах, які трансформують традиційну ієрархію влади в мережеву екосистему (таблиця 3.10).

Таблиця 3.10

Структурно-функціональна матриця концепції National E-Resilience

Компонент концепції	Сутність та функціональне призначення	Інструменталізація (Приклади реалізації в Україні)	Очікуваний ефект для НМС
1. Централізована цифрова управлінська платформа	Єдиний інформаційний простір, що агрегує дані з усіх державних реєстрів для забезпечення «єдиної версії правди» (Single Source of Truth) для вищого військово-політичного керівництва	ІАС «СОТА» (РНБО), екосистема DREAM (відновлення), Реєстр пошкодженого майна	Усунення фрагментації даних, підвищення швидкості та якості стратегічних рішень
2. Адаптивні механізми функціонування інституцій	Здатність держорганів миттєво змінювати алгоритми надання послуг та виконання функцій без зміни законодавства (code-as-law), автоматизація процесів для виключення людського фактору	Послуги «Відновлення», автоматичні виплати ВПО в «Дії», шеринг документів	Забезпечення безперервності сервісів навіть при втраті фізичного доступу до офісів чи персоналу
3. Інтеграція цифрових технологій у всі рівні	Наскрізне проникнення цифри: від стратегічного рівня (Кабмін, РНБО) до тактичного (муніципалітети, комунальні підприємства). Принцип «Digital First» для будь-якої взаємодії	Електронний документообіг, система «Трембіта» (інтероперабельність), платформи Smart City.5	Підвищення прозорості, горизонтальна координація між відомствами без бюрократії
4. Розвиток інституційної гнучкості (Institutional Agility)	Нормативна та організаційна спроможність легалізувати інновації (хмарні технології, ШІ) та масштабувати успішні практики в режимі реального часу	Легалізація хмарних сховищ (Cloud First), екстериторіальність реєстрів, кластер Brave1.7	Швидка адаптація правового поля до нових безпекових реалій та технологічних трендів

Варто деталізувати складники такої матриці. По-перше, у контексті **централізована цифрова управлінська платформа (С-eGovPro)** – це не просто ІТ-система, а стратегічний актив держави. Це інтегроване програмно-апаратне середовище, яке агрегує дані з розрізнених джерел (реєстрів, датчиків, звітів) та перетворює їх на верифіковану інформацію для прийняття рішень вищим військово-політичним керівництвом. Досвід війни показав, що традиційна модель, де кожне міністерство має свою ізольовану базу даних («колодязь даних»), є вразливою і неефективною. С-eGovPro вирішує дві екзистенційні задачі: 1) забезпечення Single Source of Truth – усунення суперечливих даних про мобілізаційні ресурси, запаси палива чи руйнування; 2) забезпечення Real-time Situational Awareness – здатності моніторити державу «на долоні» в режимі реального часу, а не через паперові звіти тижневої давнини.

Основою платформи С-eGovPro є система електронної взаємодії «Трембіта», яка не зберігає дані, а забезпечує їх безпечний транзит між реєстрами різних відомств на основі децентралізованого обміну. Отже, коли в системі «СОТА» формується звіт про ВПО, дані підтягуються безпосередньо з реєстру Мінсоцполітики через шлюз «Трембіти». При цьому якщо один реєстр зазнає атаки, це не паралізує всю систему. Обмін даними шифрується та підписується КЕП, що гарантує юридичну значущість. Інфраструктурний шар С-eGovPro – Cloud-First Strategy, а ключовим елементом виживання стала міграція державних даних у хмарні середовища (Amazon AWS, Microsoft Azure, Google Cloud). Саме тому фізичне знищення дата-центрів в Україні російськими ракетами не призвело до втрати даних. С-eGovPro фактично стала екстериторіальною, що унеможливило її «обезголовлення» кінетичними методами.

Таким чином, у представленій концепції National E-Resilience С-eGovPro передбачає створення єдиного інформаційного простору, здатного агрегувати дані з усіх державних реєстрів, надає можливість доступу до актуальної інформації та супроводжує прийняття рішень на всіх рівнях

управління. Основним завданням є забезпечення «єдиної версії правди», що критично важливо для координування дій у надзвичайних ситуаціях. На даний час основними інструментами С-eGovPro у сфері військового управління виступають:

1) інформаційно-аналітична система «COTA» – система, що діє в Апараті Ради національної безпеки і оборони України, до якої Міністерство оборони України щодня передає інформацію про отримані озброєння та військову техніку та про плани щодо подальшого їх отримання;

2) «LOGFAS» (Logistic Functional Area Services) – інтегрований набір програмних систем, розроблений для підтримки логістичного забезпечення НАТО, що використовується для координації логістики між державами – членами НАТО та з 15 жовтня 2022 року офіційно запроваджений для використання Збройними Силами України;

3) «КОРОВАЙ» – спеціальне програмне забезпечення, розроблене у співпраці Сполучених Штатів Америки, Великої Британії та України, яке з 1 вересня 2022 року використовується Збройними Силами України. Моніторинг цієї системи здійснює Міністерство цифрової трансформації України, наповнення – Міністерство оборони України. З боку міжнародних партнерів відповідальним є Міжнародний координаційний центр донорів (IDCC). Програмне забезпечення дає можливість підключати всіх користувачів, які беруть участь у плануванні потреб і відстежуванні руху матеріальних засобів до об'єднаного центру Збройних Сил України;

4) «SAP» – система, призначена для автоматизації процесів планування логістики, яка наразі використовується для обліку запасних частин, планування ремонту, технічного обслуговування військової техніки та автоматизації речового забезпечення;

Очікуваний ефект для НМС – завдяки інтеграції інформації про ресурси, кризи та потреби, державні органи отримуватимуть змогу ухвалювати швидкі й обґрунтовані рішення, що суттєво підвищує якість та швидкість їх реагування на загрози. При цьому доцільно виокремити три

спеціалізовані рівні , які покривають різні аспекти управління державою у війну:

Рівень 1: 1) стратегічна безпека – ІАС «COTA» (G2G) (військовий модуль – моніторинг постачання зброї (інтеграція з логістичними системами партнерів, наприклад, LOGFAS), карта бойових дій, облік втрат та резервів. Дозволяє відстежувати кожну одиницю західного озброєння до рівня батальйону; 2) енергетичний модуль – баланс генерації та споживання, стан атомних блоків, запаси вугілля та газу (критично важливий під час блекаутів); 3) санкційний модуль – Реєстр підсанкційних осіб та активів, моніторинг спроб обходу санкцій; 4) модуль загроз – аналіз інформаційного поля (виявлення ІПСО) та кіберзагроз.

ІАС «COTA» (Інформаційно-аналітична система «COTA») – це високозахищена, гнучка та відкрита система, яка перебуває на вищому рівні захисту інформації. Вона функціонує в Апараті Ради національної безпеки і оборони України та інтегрується з Міністерством оборони. Основне її призначення – повний моніторинг, аналіз та прогнозування ключових процесів, що відбуваються в державі, забезпечуючи повне розуміння ситуації.

Рівень 2: відновлення та ресурси – екосистема DREAM (G2B/G2C). DREAM (Digital Restoration Ecosystem for Accountable Management) – це платформа прозорого управління відбудовою, яка забезпечує довіру донорів. Її унікальні характеристики: 1) наскрізний трекінг (end-to-end), коли кожен проект має унікальний ID. Система відстежує життєвий цикл об'єкта за алгоритмом: фіксація руйнування (звіт) → проектна документація → тендер (Prozorro) → фінансування → акт виконаних робіт.

Варто виокремити додаткові складники: 1) антикорупційний запобіжник через автоматичну перевірку ризиків (Risk Management System), отже, якщо ціна, наприклад, на бетон у кошторисі перевищує ринкову, система сигналізує про аномалію; 2) публічний доступ – інвестори та громадяни бачать прогрес на дашбордах, що перетворює платформу на

інструмент суспільного контролю.

Рівень 3: Взаємодія з громадянином – Дія / Мрія / Армія+ (G2C/G2M), головний складник держави, де збираються первинні дані. Так, «Дія» виконує функцію сенсора соціального стану (кількість ВПО, заявки на «Відновлення»), «Армія+» – цифровізує рутину військових (рапорти, ID), забезпечуючи Генштаб даними про реальний стан особового складу без паперової тяганини, «Мрія» як освітній реєстр дозволяє відстежувати міграцію учнів та освітні втрати.

У рамках нашої методології DRA, функціонування *C-eGovPro* детермінується циклом OODA (Observe, Orient, Decide, Act), який прискорений завдяки цифровізації: 1) збір (observe) – сенсори (IoT на енергооб'єктах дає можливість отримувати в реальному часі інформацію про стан енергетичних систем; наприклад, сенсори можуть відстежувати рівень споживання електроенергії, стежити за можливими аваріями або перебоями в електропостачанні), звіти громадян («Ворог», дозволяє громадянам оперативно інформувати про ворожі дії чи підозрілі ситуації, що дозволяє державі швидко реагувати на загрози), транзакції в реєстрах автоматично надходять до Data Lak – єдиного сховища даних, де зберігається вся інформація, необхідна для подальшого аналізу; 2) обробка (orient) – AI-алгоритми аналізують дані на аномалії. Алгоритми аналізують інформацію, шукаючи відхилення від нормального стану. Наприклад, різке зростання цін на продукти в певному регіоні може свідчити про логістичну блокаду або інші ринкові аномалії, що потребують термінового реагування; 3) візуалізація (decide) – дані виводяться на дашборди «COTA. Ці візуальні елементи полегшують сприйняття інформації та дозволяють ухвалювати зважені рішення на рівні Ради національної безпеки і оборони (РНБО), й на основі виявлених патернів і аномалій, автоматизовані системи пропонують варіанти дій, що дозволяє значно зменшити час ухвалення рішень 4) дія (act) – прийняття рішення (наприклад, перенаправлення гуманітарних вантажів або запуск резервних ліній електромереж).

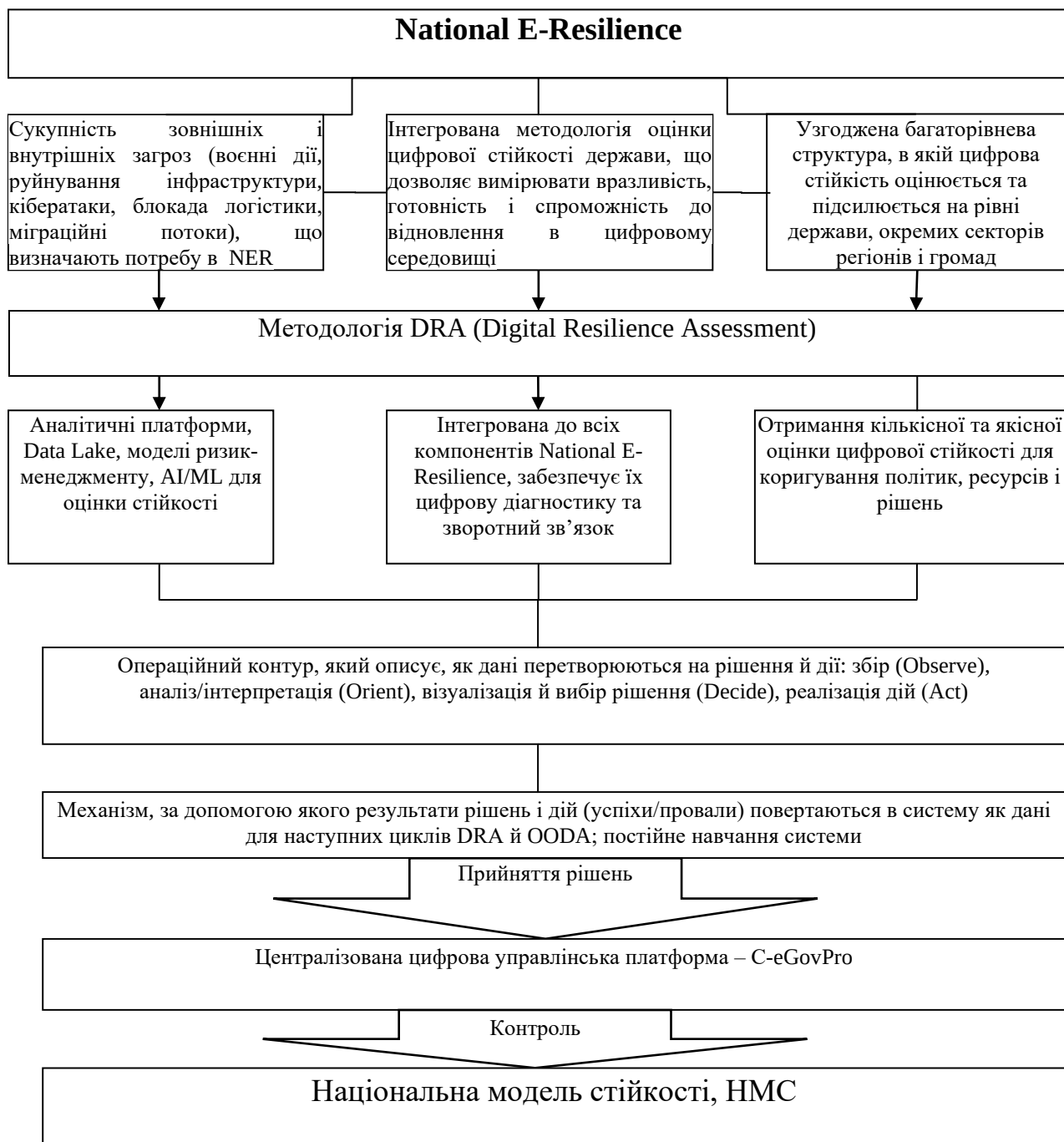


Рис. 3.2. Інтегрована цифрова платформа моніторингу на основі методології DRA (Digital Resilience Assessment) у структуру НМС

Таким чином, методологія DRA, через механізм циклу OODA, забезпечує інтеграцію новітніх цифрових технологій у процеси збору, обробки, візуалізації та реагування на інформацію. Цифровізація цих етапів не лише оптимізує робочі процеси, але й суттєво підвищує ефективність реагування на виклики національної безпеки. Завдяки цьому, Україна отримує можливість швидше та якісніше справлятися з різноманітними

загрозами, забезпечуючи стійкість не лише державних інститутів, але й суспільства в цілому.

У парадигмальному вимірі National E-Resilience пропонує розглядати державне управління не як закриту замкнену структуру влади, що повільно «передає» рішення згори донизу, а як мережеву, динамічну, багаторівневу екосистему, в якій: 1) дані, сигнали, запити та ресурси циркулюють по численних каналах; суб'єкти управління (центральні органи, регіони, громади, інституції, громадяни) виступають не пасивними «ланками», а мережевими хабами, які одночасно генерують, сприймають і трансформують інформацію; 2) цифрова інфраструктура (платформи, реєстри, сервіси, сенсори, канали комунікації) стає не додатком до «реальної» держави, а її онтологічною основою – тобто тим, через що і завдяки чому держава взагалі здатна діяти. У цій логіці національна цифрова стійкість означає не просто захищеність ІТ-систем, а спроможність держави як цілісної мережі: зберігати функціональність під тиском криз; самоорганізовуватися й адаптуватися; не лише відновлюватися після викликів, а й якісно змінюватися у процесі цих викликів, закріплюючи нові, більш ефективні практики. Ця концепція поєднує в собі кібернетичну логіку управління (зворотні зв'язки, контури регулювання), системну теорію (держава як складна відкрита система) та *цифровий базис* (держава як сукупність платформ, на яких вибудовуються сервіси, політики й взаємодії).

1. *Перша здатність у межах National E-Resilience* – швидко сприймати сигнали з середовища – задає парадигму «сенсорної держави». У традиційній моделі управління держава «дізнається» про реальність через: звіти чиновників, паперові звіти органів статистики, повільні бюрократичні канали. У парадигмі National E-Resilience держава функціонує як розширений цифровий сенсорний механізм, у якому: фізична інфраструктура (енергетика, транспорт, зв'язок, медицина, освіта) містить мережу цифрових сенсорів. При цьому громадяни виступають активними носіями сенсорної функції: мобільні застосунки на кшталт «єВорог» дозволяють перетворити масові

спостереження на структурований потік даних; цифрові звернення, скарги, запити – це не лише механізм участі, а й канал оперативного виявлення криз.

При цьому адміністративні транзакції та реєстрові записи стають «цифровими слідами» стану системи: різкі зміни у кількості зареєстрованих пошкоджених об'єктів; стрибки в показниках реєстрації ВПО, заяв на соціальну допомогу, змін місця проживання тощо. Усе це разом формує суцільне поле сприйняття, де будь-який осередок кризи (руйнування, дефіцит, блокада, міграційний сплеск) присутній у цифровому просторі у вигляді даних; держава перестає бути «сліпою» і «глухою» у реальному часі – вона бачить і чує власну територію через множинні цифрові канали.

2. З позицій концепту інтерпретації National E-Resilience здійснюється перехід до *алгоритмічної держави та III як інфраструктури розуміння*. Саме тому друга ключова здатність National E-Resilience – *інтерпретувати сигнали за допомогою аналітики й штучного інтелекту формулюється як парадигма алгоритмічної інтерпретації*. Якщо перший рівень – це сукупність «неявних сигналів», то другий рівень – це перетворення таких сигналів на знання, оцінки, гіпотези й прогнози. В термінах теоретичної концепції National E-Resilience держава постає як аналітичний суб'єкт, здатний не лише накопичувати дані, а й рефлексувати над ними. Штучний інтелект і аналітичні алгоритми стають інфраструктурою державного розуміння – від фіксації аномалій до побудови сценаріїв. Це означає:

по-перше, перехід від описового до предиктивного управління, коли система більше не обмежується фіксацією факту події («ціни вже зросли», «мережа вже впала»), а виявляє патерни, що передують кризі; формує ймовірнісні сценарії (як розгортатимуться події без втручання).

по-друге, багаторівнева інтерпретація даних, коли інформація з «датчиків» та реєстрів зливається в Data Lake, де 1) алгоритми виявляють аномалії: різкі коливання цін, навантаження на мережі, міграційні потоки; 2) ці аномалії контекстуалізуються (наприклад, стрибок цін в окремому регіоні інтерпретується як можливий наслідок: логістичної блокади, знищення

транспортних вузлів, панічного попиту;

по-третє, машинне навчання як механізм «еволюції розуміння», коли з кожним новим циклом кризи алгоритми навчаються розрізняти типові й нетипові ситуації, знижується кількість хибних спрацьовувань, якість класифікації загроз і критичних станів поступово зростає.

За такої ситуації держава більше не покладається лише на інтуїцію й досвід вузького кола експертів; натомість вона: базує рішення на масивній, статистично обґрунтованій, багатовимірній аналітиці; поєднує людське стратегічне мислення із машинною здатністю обробляти складні патерни.

3. З позицій концепту *прийняття рішень у реальному часі National E-Resilience трансформує державу у часово стиснуту систему управління*. Традиційна бюрократична держава діє в повільних часових інтервалах: тижні й місяці для аналітики, довгі погодження між відомствами, процедури, що не враховують динаміки кризи. National E-Resilience орієнтує державу на: скорочення часових лагів між подією, її усвідомленням та управлінським рішенням; побудову циклів управління, що працюють із хвилинами та годинами, а не лише з місяцями й роками. Це досягається завдяки:

1) *візуалізації в реальному часі*. Аналітичні результати (з DRA, із систем моніторингу) подаються на: інтерактивні дашборди; теплові карти, графіки, сигнальні панелі для ключових центрів прийняття рішень. Тут не йдеться просто про «картинку» – візуалізація стає формою існування системи, яка концентрує увагу на «перетинах напруги» та дозволяє миттєво помічати зони ризику.

2) *інституціональній організації швидкого рішення*. Головні структури управління (РНБО України, урядові штаби, кризові центри отримують не розрізнені звіти, а цілісні аналітичні формати стану системи; можуть запускати скорочені процедури ухвалення рішень, де частина кроків автоматизована чи формалізована наперед;

3) поєднання стратегічного й тактичного підходів, адже рішення в реальному часі не відміняють довгострокового планування, але стратегія

задає рамки і правила реагування; тактика наповнює їх конкретними діями в конкретних кризах. Отже, держава перестає бути інерційним апаратом і набуває рис системи, здатної швидко перерозподіляти увагу, ресурси, потоки взаємодій.

4. *Парадигма дії: цифрово-інституційна операційність.* Четверта здатність – діяти через цифрові сервіси й адаптивні процедури – формує парадигму цифрово-інституційної операційності. У цій парадигмі управлінське рішення – це не лише ухвалена постанова або підписаний наказ. Це насамперед запуск або переналаштування цифрових процесів, що безпосередньо змінюють досвід громадянина; впливають на розподіл ресурсів; перебудовують маршрути послуг.

Така дія проявляється в кількох вимірах. По-перше, цифрові сервіси як носії державної дії, отже, коли держава вирішує підтримати населення в умовах війни чи катастрофи, це виражається у: 1) створенні й налаштуванні електронних програм (виплати ВПО, компенсації за зруйноване житло, адресна допомога); 2) відкритті відповідних послуг у цифрових застосунках; 3) зміні логіки взаємодії «людина – держава» (менше черг, поїздок, паперу, більше натискань кількох кнопок). Отже, державна політика втілюється в цифровому коді, архітектурі сервісу, бізнес-процесі платформи. При цьому регламент, який раніше існував як статична інструкція чи паперовий регламент, перетворюється на набір алгоритмічних правил у цифровій системі (хто має право, за яких умов, які кроки), гнучку схему, яку можна змінити шляхом конфігурації без переписування всього законодавчого масиву. Це забезпечує операційну адаптивність: держава може швидко змінити порядок нарахування виплат, маршрути погодження рішень, критерії доступу до допомоги – просто коригуючи цифрову логіку сервісів.

5. Інституційна «розподіленість» дії. І ідеалі цифрова дія держави не «замикається» в одному міністерстві чи відомстві, а реалізується через взаємодію багатьох платформ і реєстрів; дозволяє численним суб'єктам (центральному, регіональному, муніципальному) діяти скоординовано,

спираючись на одну «версію функціоналу». Таким чином, інфраструктура цифрових сервісів стає матеріальним носієм волі держави, головним каналом, через який вона здійснює конкретні втручання в реальність, важливою умовою її стійкості, адже саме завдяки цифровим сервісам держава зберігає здатність діяти навіть тоді, коли зруйновані будівлі, порушені ланцюги фізичної присутності.

Отже, теоретичну концепцію National E-Resilience слід описати як концепцію національної цифрової стійкості, у межах якої держава функціонує як мережева, цифрово опосередкована екосистема, здатна завдяки інтегрованій цифровій інфраструктурі, аналітиці та інституційній гнучкості:

1) швидко сприймати сигнали з внутрішнього й зовнішнього середовища через розгалужений цифровий формат (сенсори, платформи, реєстри, громадянські повідомлення);

2) інтерпретувати ці сигнали за допомогою алгоритмічної та інтелектуальної обробки даних, перетворюючи їх на знання, оцінки та прогнози;

3) ухвалювати управлінські рішення в режимі реального часу, спираючись на візуалізовану картину стану системи та скорочені контури погодження;

4) діяти через цифрові сервіси, адаптивні процедури й гнучкі інституційні механізми, що забезпечують безперервність публічних функцій навіть в умовах екстремальних викликів.

У цьому сенсі авторська концепція National E-Resilience є не тільки технічною чи організаційною моделлю, а насамперед новою парадигмою державності, в якій цифрова інфраструктура дорівнює інфраструктурі влади, дані стають первинним матеріалом політики, алгоритми та сервіси виступають основними інструментами реалізації публічного інтересу, а стійкість визначається не відсутністю негативного впливу, а здатністю системи вчитися, адаптуватися й відновлюватися в режимі постійної

цифрової взаємодії з реальністю.

Теоретична концепція National E-Resilience не виникає «з нуля»; вона вбудовується в більш розгалужений інтелектуальний ландшафт, де вже існують напрацьовані традиції осмислення стійкості (resilience), саморегуляції складних систем (кібернетика) та трансформації держави в платформену інфраструктуру. Її новизна полягає не в запереченні цих підходів, а в їх синтезі на ґрунті цифрової трансформації, війни та гібридних викликів.

Власне, класичні теорії resilience (стійкості) виходять із уявлення про систему – економічну, екологічну чи соціальну, – яка неминуче зазнає зовнішніх шоків та внутрішніх відмов, але водночас зберігає цілісність, базову функціональність і здатність до відновлення після кризи. У межах цієї традиції зазвичай розрізняють два ключові типи стійкості. Перший – так звана «інженерна стійкість» (engineering resilience), що зосереджується на здатності системи повернутися в попередній, «нормальний» стан після збою, мінімізуючи амплітуду відхилень і скорочуючи час простою. Другий – екологічна або еволюційна стійкість (ecological / evolutionary resilience), яка наголошує не лише на витримуванні відмов, а й на спроможності системи перебудовувати свої внутрішні структури, змінювати режими функціонування, адаптуватися до нових умов, при цьому залишаючись життєздатною.

Авторська концепція National E-Resilience органічно тяжіє саме до другого, більш розвиненого розуміння стійкості. Вона принципово не обмежується уявленням про «повернення до нормальності» – до довоєнного стану, до паперових і процедурно перевантажених процесів, до повільних і жорстких ієрархій ухвалення рішень. Навпаки, вихідною тезою є те, що для України війна, масовані кібератаки, руйнування критичної інфраструктури та гібридні загрози не є тимчасовою «відмовою», після якої можна просто «повернутися» до попередньої конфігурації суспільних відносин. Це нова, тривала, структурна умова існування системи державного управління. У

таких обставинах завдання полягає не лише у відновленні зруйнованого, а у трансформаційному пристосуванні – зміні архітектури управління, логіки прийняття рішень, інституційних форм і цифрової інфраструктури.

Емпірично це добре ілюструють події з 2022 року, коли після перших ракетних атак по урядовим будівлям, дата-центрам і енергетичній інфраструктурі стало очевидно, що державна система, побудована навколо фізичних офісів, паперових архівів і локальних серверних, є радикально вразливою. Відповіддю на ці загрози стала не спроба «повернути все як було», а прискорене перенесення ключових державних реєстрів у хмарні середовища, поява екстериторіальних дата-центрів, розгортання системи резервного доступу до критичних баз даних, широке використання супутникового інтернету та інших рішень, які вже не вписуються в класичну інженерну логіку «полагодити й відновити статус-кво». Держава почала змінювати саме устрій власної цифрової життєдіяльності.

У термінах *resilience* це означає, що держава як система розглядається передусім як соціо-технічна екосистема, в якій цифрові платформи, інфраструктури та сервіси є не просто допоміжними інструментами, а структурними елементами стійкості. На практиці це проявляється в тому, що зміни в цифровій інфраструктурі здатні радикально змінювати межі можливої стійкості – як зменшувати вразливість, так і посилювати або послаблювати адаптивність. Показовим є приклад застосунку «Дія», який під час повномасштабної війни перетворився з інструменту «зручних послуг» на ключовий канал реалізації програм підтримки: компенсацій за зруйноване житло, виплат внутрішньо переміщеним особам, цифрової ідентифікації для доступу до соціальних сервісів. Відмови чи відсутність такого каналу сьогодні означали б не просто «тимчасові незручності», а системний дефект у здатності держави підтримати власних громадян. Відповідно, цифрова стійкість (*E-Resilience*) у межах цієї концепції інтегрує кілька вимірів.

По-перше, це *класична здатність до поглинання ударів* – захищеність даних, наявність резервних каналів зв'язку, дублювання критичних реєстрів у

хмарних інфраструктурах, використання георезервування та криптозахисту. Так, перенесення низки українських реєстрів у хмарні середовища ЄС та країн-партнерів дало змогу зберегти й оперативно відновлювати доступ до даних навіть за умов прямої фізичної загрози дата-центрам на території України.

По-друге, це *здатність до адаптації*, яка проявляється в тому, як держава перебудовує власні цифрові сервіси, оновлює алгоритми надання допомоги, змінює процедурні ланцюжки в динаміці. Прикладом є швидкий запуск і поетапне розширення програми «Відновлення», а також автоматизованих виплат ВПО, коли спочатку моделювалися базові сценарії, а з часом критерії, алгоритми перевірки та маршрутизації змінювалися з урахуванням нових типів зловживань, масштабів руйнувань і бюджетних можливостей.

По-третє, і це ключовий вимір, цифрова стійкість у концепції National E-Resilience означає *здатність до трансформації*. Йдеться про перехід від ієрархічної моделі управління до мережевої – коли дані, сервіси та органи влади взаємодіють через горизонтальні цифрові зв'язки; від паперових і фрагментованих процедур до процесів, які «by default» є цифровими; від людиноцентричної бюрократії, де людина змушена «носити документи» між інституціями, до людиноцентричних, але цифрово опосередкованих сервісів, де тягар координації беруть на себе платформи та реєстрова інтероперабельність. В українських реаліях це видно на прикладі інтеграції через платформу «Трембіта» десятків баз даних, що дає можливість ухвалювати рішення про призначення допомоги, субсидій чи компенсацій без вимоги до громадянина фізично підтверджувати інформацію, уже наявну в державних системах.

Таким чином, National E-Resilience можна інтерпретувати як розвиток класичних теорій resilience у площині держави, яка стала принципово невіддільною від власної цифрової складової. Стійкість у цьому випадку означає не тільки «відремонтувати те, що зламали», а перебудувати спосіб

існування й дії держави за рахунок цифрової інфраструктури, аналітики й інституційної гнучкості, які довели свою критичність на практиці під час повномасштабної війни.

Другою важливою теоретичною опорою концепції National E-Resilience є традиція теорії управління складними системами та кібернетики. Кібернетика, у найзагальнішому вигляді, ставить у центр уваги зворотні зв'язки, інформаційні потоки та регулювання поведінки системи через постійне коригування на основі нових даних. У цьому сенсі запропонована у дисертації модель є кібернетичною за своєю суттю: вона описує державу як систему, що безперервно спостерігає за середовищем, інтерпретує сигнали, ухвалює рішення й реалізує дії, після чого знову оцінює результати у вигляді зворотного зв'язку.

Використання циклу OODA (Observe–Orient–Decide–Act) у методології Digital Resilience Assessment по суті є конкретною реалізацією такого кібернетичного контуру. На етапі спостереження держава отримує сигнали з середовища – від сенсорних мереж на енергооб'єктах і транспортній інфраструктурі до масових повідомлень громадян через застосунки та потоків транзакцій у реєстрах. Орієнтація передбачає інтерпретацію цих сигналів: аналіз аномалій у споживанні електроенергії, раптових стрибків цін на продукти у конкретних регіонах, нетипового зростання кількості звернень по соціальну допомогу. Рішення формуються на основі аналітичних звітів, теплових карт, дашбордів – наприклад, у системі «СОТА» при РНБО України, яка консолідує різні типи даних у єдиному інтерфейсі для вищого керівництва держави. Дія означає безпосереднє регулювання – перенаправлення гуманітарних вантажів у регіони ризику, запуск резервних ліній електромереж уразі загрози блек-ауту, зміна алгоритмів виплат для певних категорій населення. Повторне спостереження дозволяє оцінити, чи дало таке втручання бажаний ефект, і, за потреби, скоригувати параметри.

Ця логіка підкреслює роль інформації як центрального ресурсу управління. У класичній кібернетиці інформація – це те, що дозволяє

зменшувати невизначеність, а ефективність управління безпосередньо залежить від якості інформаційних потоків. В умовах National E-Resilience централізована цифрова платформа, побудована за принципом Single Source of Truth, виступає інфраструктурою інформаційної єдності: вона агрегує дані з розрізнених джерел, усуває суперечності, забезпечує єдину базу для рішень. Сенсори, реєстри, цифрові сервіси формують потік даних, який постійно «живить» управлінські контури. Від швидкості, з якою ці дані рухаються між підсистемами, від їх інтегровуваності й доступності залежать темп реакції та точність коригування поведінки системи загалом.

Важливим тут є й принцип керованої складності, відомий із кібернетики: складну систему можна ефективно регулювати лише тоді, коли різноманіття її управляючих механізмів не менше, ніж різноманіття викликів середовища. В українських реаліях це означає, що держава змушена паралельно розвивати багатоканальність сприйняття (сенсорні мережі на інфраструктурі, краудсорсингові інструменти на кшталт «єВорог», аналітичні платформи, міжнародні потоки даних), множинність інструментів реагування (гнучкі цифрові сервіси, адаптивні адміністративні процедури, платформені рішення в різних секторах) та інституційну здатність швидко перебудовувати власні правила гри, щоби відповідати складності реального світу. Прикладом такої керованої складності є поєднання централізованих безпекових рішень (на рівні РНБО) з децентралізованими ініціативами громад і волонтерських спільнот, що діють у загальній цифровій рамці, але мають простір для локальної ініціативи.

Крім того, National E-Resilience розглядає державу як саморегульовану систему. Йдеться не про ручне управління кожною ситуацією з одного центру, а про наявність механізмів автоматичного й напіваавтоматичного коригування. У практичному вимірі це, наприклад, тригери, які автоматично запускають виплати за певних умов (наплив ВПО, фіксація руйнувань у реєстрі), змінюють маршрути постачання чи пріоритетність відновлювальних робіт. Паралельно формується навчальна модель, коли результати дій – їх

успішність чи помилки – стають матеріалом для оновлення алгоритмів, програмних модулів, політик і сервісів. Це видно, зокрема, на прикладі послідовних оновлень цифрових програм підтримки, коли від однієї хвили допомоги до іншої змінюються як критерії, так і логіка перевірок, виходячи з виявлених зловживань чи нових соціальних потреб. У такій структури авторського підходу перспектива дозволяє побачити в National E-Resilience не просто «цифрову державу» (яка оцифрувала послуги), а саме керовану, здатну до самокорекції й навчання систему, де інформаційні потоки, контури зворотного зв'язку та операційні рішення замикаються в єдину логіку саморегуляції.

Третім теоретичним полем, із яким резонує концепція National E-Resilience, є ідея платформеної держави (platform state, platform government) [332-334]. У цьому форматі держава мислиться не як монолітний апарат із набором закритих відомств і не як механічна сума окремих органів влади, а як платформна інфраструктура, що надає базові цифрові «траєкторії» – ідентифікацію, реєстри, платіжні механізми, комунікацію, інтероперабельність. На цих напрямках будуються державні послуги для громадян і бізнесу, реалізується взаємодія між відомствами, формуються екосистеми публічно-приватної співпраці.

У межах National E-Resilience логіка платформ радикалізується за рахунок того, що на неї накладається інституціональний вимір стійкості. Якщо platform state держава насамперед зосереджується на ефективності послуг, зручності користувача та економії ресурсів, то національна цифрова стійкість додає критерій виживання та функціонування в умовах екстремальних загроз – війни, масованих кібератак, руйнування фізичної інфраструктури. Тому вимоги до платформ тут значно суворіші: вони мають бути не лише зручними, а й стійкими до збоїв, здатними до резервування, дублювання, екстериторіальності, а також до швидкого масштабування під час кризи.

У цьому контексті поняття цифрових управлінських платформ

фактично розширюється до рівня національної безпекової інфраструктури. Централізована цифрова платформа управління, що забезпечує «єдину версію правди» для вищого керівництва, – це вже не просто технічне рішення: це місце, де перетинаються потоки даних із різних секторів, формується спільне розуміння ситуації і підтримуються рішення, які безпосередньо впливають на безпеку регіонів, критичних галузей і мільйонів людей. Руйнування або компрометація такої платформи означали б удар не лише по сервісах, а по здатності держави мислити й діяти як цілісна система.

Водночас platform state, інтегрована з логікою E-Resilience, формує екосистему співтворення (co-creation) стійкості. Громадяни, бізнес, громади, міжнародні партнери перестають бути лише об'єктами політики і стають повноцінними акторами, що вносять вклад у функціонування платформи через дані, сервіси, інновації. Громадяни подають репорти про руйнування, фіксують ворожу активність, реєструють потреби; бізнес забезпечує технологічні рішення, хмарну інфраструктуру, засоби кіберзахисту, аналітичні інструменти; держава формує нормативну рамку, визначає базові стандарти безпеки та інтероперабельності, інвестує в критичну цифрову інфраструктуру. У такому розподілі ролей стійкість перестає бути суто державною функцією й перетворюється на спільний продукт, вироблений через взаємодію різних суб'єктів на спільних платформах.

Отже, National E-Resilience можна розглядати як специфічну, «мілітарно- та кризово-орієнтовану» модифікацію платформеної держави, в якій цифрові платформи більше не є лише інструментами модернізації послуг, а стають несучими конструкціями національної безпеки та стійкості. У підсумку ця концепція синтезує три логіки: resilience-логіку, що описує здатність не просто витримати удар, а адаптуватися й трансформуватися; кібернетичну логіку – управління через інформацію, зворотні зв'язки та контури OODA; і платформену логіку – державу як інфраструктуру цифрових платформ, на яких будуються сервіси, політики та взаємодії. Саме в цьому трикутнику – resilience → кібернетика → платформена держава –

National E-Resilience набуває свого повного теоретичного змісту як модель національної цифрової стійкості, релевантна умовам України в ситуації тривалих гібридних та воєнних загроз і підтверджена конкретними емпіричними практиками останніх років.

Принципово важливим є те, що включення цих чотирьох блоків показників до Digital Resilience Assessment дозволяє вийти за межі вузького технократичного розуміння цифрової зрілості, яке зводиться до оцінки наявності IT-рішень, їхньої формальної функціональності чи відповідності стандартам. У розширеній DRA-моделі цифрові управлінські платформи – зокрема, С-eGovPro як централізована платформа НМС – оцінюються не лише як технологічні об’єкти, а як інституційно-соціальні феномени, що впливають на здатність системи до ініціативності, суспільної мобілізації, безпеки, координації та скорочення часових лагів між проблемою й реакцією. Іншими словами, DRA починає вимірювати не просто «цифровість заради цифровості», а ступінь внеску цифрових платформ у реальну стійкість управлінських систем – їхню здатність витримувати, адаптуватися і трансформуватися в умовах тривалих криз.

У цьому сенсі спеціально розроблений набір показників для цифрових управлінських платформ стає не додатком, а критичним компонентом загальної архітектури DRA. Він дозволяє побачити, наскільки платформа справді працює як операційне ядро National E-Resilience в межах Національної моделі стійкості, та дає можливість цілеспрямовано посилювати її сильні сторони й усувати вразливості. Такий підхід створює підґрунтя для переходу від декларативної цифровізації до емпірично керованої цифрової стійкості, коли проектування, модернізація й масштабування платформних рішень спираються на системні вимірювання їхнього реального впливу на стійкість держави.

Висновки до розділу 3

1. У розділі теоретично обґрунтовано перехід від традиційних ієрархічних ІС до платформної моделі державного управління. Цифрові управлінські платформи розглядаються як складні соціотехнічні системи, що створюють суспільну цінність не лише через оптимізацію внутрішніх процесів, а передусім через мережеві ефекти та фасилітацію взаємодії держави, бізнесу й громадян. Показано, що саме платформний підхід здатний забезпечити необхідну гнучкість, адаптивність та стійкість управлінських систем в умовах високої ентропії, експоненційного зростання даних і гібридних загроз.

2. Сформовано й формалізовано концепт інтегрованого відкритого управління як теоретичний зв'язок між відкритим урядуванням і цифровими платформами. Доведено, що інтегроване відкрите управління поєднує принципи прозорості, підзвітності, цифрової інклюзії та участі громадян з інструментами відкритих даних і електронних сервісів. На основі аналізу міжнародного й українського досвіду показано, що саме платформи відкритих даних, е-консультацій та громадської участі створюють цілісний інформаційний простір для взаємодії влади й суспільства, знижують корупційні ризики та підвищують довіру до інституцій.

3. Розроблено систему принципів інституційного дизайну цифрових управлінських платформ та показано їхній вплив на ефективність і стійкість управління. Обґрунтовано ключову роль модульної архітектури, інтероперабельності, зворотного зв'язку, адаптивності й інституційної гнучкості як конструктивних засад платформ. На основі порівняльного аналізу (табл. 3.1, 3.2, 3.6–3.7) доведено, що такі платформи забезпечують раціональне впровадження інновацій, краще управління ризиками, вищий рівень захисту даних та інклюзивність сервісів порівняно з традиційними управлінськими системами.

4. Емпірично підтверджено, що цифрові управлінські платформи є факторами зміцнення соціальної стабільності та безпеки функціонування

управлінських систем. На прикладі українських (застосунок і портал «Дія», «Прозорро», «Єдиний вебпортал використання публічних коштів», електронна демократія, «Громадський бюджет») та зарубіжних практик (Естонія, Сінгапур, скандинавські країни, тощо) показано зменшення часу отримання послуг, зростання задоволеності громадян, скорочення корупції та підвищення ефективності реагування на кризи. Наведені кількісні показники (економія бюджетних коштів, частка користувачів е-сервісів, рівень довіри та задоволеності) демонструють, що платформи реально підсилюють соціальну згуртованість і безпеку.

5. Здійснено комплексний аналіз нормативно-правового забезпечення цифрових управлінських платформ в Україні та виявлено ключові прогалини. Показано, що закони про електронні документи, електронний документообіг, електронну ідентифікацію та довірчі послуги формують інтегроване правове підґрунтя для функціонування платформ, надаючи юридичну силу електронним документам, електронному підпису та електронній ідентифікації. Водночас доведено наявність проблем – недостатня гармонізація норм, відсутність єдиних стандартів кібербезпеки, низька регулярність публікації звітів (близько 40% органів влади), слабкий вплив е-консультацій на рішення (до 60% без реальних наслідків), – що вимагає цільового оновлення законодавства.

6. Обґрунтовано авторську концепцію національної цифрової стійкості як нову парадигму державного управління в умовах війни та гібридних загроз. У межах цієї концепції держава описується як мережева, цифрово опосередкована екосистема, що спирається на централізовану цифрову управлінську платформу, адаптивну інфраструктуру, аналітичний контур (Data Lake, системи ризик-менеджменту, аналітичні платформи) та рівень взаємодії з громадянами (Dіia, «Мрія», «Армія+» тощо). Показано, що концепція синтезує теорії стійкості, кібернетики та платформеної держави й передбачає перехід від ієрархічної, паперової моделі до мережевої, де дані, сервіси й інституції пов'язані горизонтальними цифровими зв'язками.

7. Запропоновано й теоретично обґрунтовано методологію оцінки цифрової стійкості держави (Digital Resilience Assessment), інтегровану в цикл OODA (Observe–Orient–Decide–Act. Завдяки цій методології дані із сенсорів, реєстрів, звернень громадян та платформ агрегуються, аналізуються на виявлення аномалій, візуалізуються в аналітичних дашбордах і оперативно трансформуються в управлінські дії. Науковим результатом є перехід від описового до предиктивного, даноцентричного управління, де цифрові управлінські платформи оцінюються не лише як ІТ-рішення, а як інституційно-соціальні феномени, що визначають здатність системи до ініціативності, швидкого реагування, навчання й трансформації в реальному часі.

Основні результати дисертаційного дослідження, що надані у цьому розділі, були опубліковані у фахових наукових виданнях зі спеціальності «Публічне управління і адміністрування» і включені до списку публікацій автора [27-32].

РОЗДІЛ 4

ХАРАКТЕРИСТИКА МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ
МОДЕЛІ СТІЙКОСТІ В УМОВАХ ЦИФРОВОГО СУСПІЛЬСТВА

4.1. Теоретико-методологічні засади системного проєктування механізмів забезпечення національної моделі стійкості в умовах цифрової трансформації

Сучасна архітектура глобальної безпеки переживає тектонічні зрушення, зумовлені конвергенцією геополітичної нестабільності, кліматичних змін та безпрецедентної технологічної експансії. В цих умовах традиційні концепції «захисту» та «оборони», що базувалися на ідеї недоторканності периметра та статичної стабільності, демонструють свою неспроможність. На зміну їм приходить National Resilience як динамічна характеристика держави та суспільства, що визначає здатність системи абсорбувати шоківі впливи, адаптуватися до змін у реальному часі та відновлювати функціональність на якісно новому рівні після криз. Особливої уваги заслуговує застосування системного підходу до проєктування та оцінювання механізмів реалізації Національної моделі стійкості (НМС) в умовах тотальної цифрової трансформації. Цифровізація в цьому контексті розглядається не як окрема галузь, а як всеосяжне операційне середовище, що фундаментально змінює природу загроз та інструментарій реагування. Актуальність теми зумовлена необхідністю переходу від реактивного управління кризами до проактивного дизайну державних систем, здатних функціонувати в умовах високої невизначеності та ентропії.

Ключовою проблемою, що ідентифікується в аналізі існуючих підходів до формування національної стійкості, є розрив між декларативними стратегічними документами та реальними механізмами їх імплементації. У багатьох випадках концепції стійкості фіксуються у вигляді стратегій, доктрин, концепцій безпеки чи цифрової трансформації, але залишаються

переважно на рівні політичних заяв і ціннісних орієнтирів, не трансформуючись у конкретні інженерні, алгоритмічні та процедурні рішення. Це призводить до ситуації, коли офіційний дискурс декларує високий рівень готовності до криз, комплексність підходів, міжвідомчу координацію, однак на практиці механізми реагування залишаються фрагментарними, реактивними й часто неузгодженими між собою. Такий розрив між «задекларованою стійкістю» та фактичною спроможністю системи адаптуватися до шоків і підтримувати життєздатність у кризових умовах стає основною перешкодою для реального втілення Національної моделі стійкості (НМС).

У цьому форматі системний підхід постає не просто як одна з можливих методологічних опцій, а як необхідна передумова для подолання згаданого розриву. Його сутність полягає в тому, що держава розглядається як *складна адаптивна система* (Complex Adaptive System, CAS) [334], у якій жоден елемент не може бути адекватно зрозумілий ізольовано, без урахування його взаємодії з іншими елементами та з середовищем. Системний підхід фокусує увагу не на окремих документах, інституціях чи технологіях, а на їхніх взаємозв'язках, контурах зворотного зв'язку, потоках інформації та ресурсів, механізмах самоналаштування і навчання системи. У межах такого бачення кожен елемент, від законодавчого акта до протоколу обміну даними в серверній, від організаційної структури міністерства до конкретного алгоритму прийняття рішень у цифровій платформі є частиною єдиної архітектури реалізації НМС.

Розгляд держави як CAS дозволяє виявити низку властивостей, які принципово змінюють підхід до проєктування та оцінювання механізмів стійкості. По-перше, йдеться про нелінійність: незначні зміни в одному компоненті (наприклад, у протоколах обміну даними між відомствами) можуть призвести до непропорційно великих наслідків для всієї системи (затримки в реагуванні на кризу, помилки у пріоритезації ресурсів, провали в комунікації з населенням). По-друге, система має емерджентні властивості:

стійкість не є просто сумою стійкості окремих міністерств, регіонів чи інформаційних систем; вона проявляється на рівні взаємодії, узгодженості та адаптивності всієї конфігурації. По-третє, складні адаптивні системи характеризуються здатністю до навчання: на основі досвіду попередніх криз, збоїв і успіхів вони можуть змінювати свої внутрішні правила, алгоритми та структури, посилюючи власну стійкість у довгостроковій перспективі.

У традиційних підходах до формування стратегій стійкості як у технічних, так і в управлінських системах домінує лінійна логіка: від політичного бачення до загальних принципів, від принципів до набору заходів, від заходів до індикаторів виконання. У такій логіці кожен рівень розробляється відносно автономно, а зв'язки між ними залишаються слабо формалізованими. Саме тут виникає описаний розрив: стратегічні документи, навіть будучи концептуально виваженими, не мають механізмів «прошивання» в інституційні процедури, цифрові сервіси, алгоритми прийняття рішень. Системний підхід, навпаки, наполягає на тому, що будь-яка стратегія стійкості має від початку проєктуватися як елемент багаторівневої архітектури CAS, де чітко простежуються траєкторії трансляції політичних рішень у конкретні регуляторні, організаційні, технологічні та інформаційні зміни.

Ключовим інструментом такого проєктування стає архітектурне моделювання НМС. Йдеться не лише про візуалізацію організаційних структур або інформаційних потоків, а про цілісний опис «ландшафту стійкості», що включає кілька взаємопов'язаних рівнів. На нормативному рівні формуються цілі, принципи та рамкові вимоги до стійкості; на інституційному визначаються ролі та відповідальність органів влади, процедурні механізми координації; на організаційно-процесуальному проєктуються конкретні процеси реагування, відновлення, адаптації; на технологічному підбираються та інтегруються цифрові інструменти, платформи, засоби захисту; на даних і алгоритмах – визначаються моделі даних, протоколи обміну, алгоритми аналізу та прийняття рішень. Усі ці

рівні розглядаються не як послідовні «поверхи», а як взаємопов'язані шари єдиної системи.

Якщо повернутися до вихідної проблеми, стає очевидним, що розрив між стратегіями й механізмами часто виникає саме через відсутність системного архітектурного бачення. Стратегічні документи створюються в одних інституційних контурах, тоді як цифрові управлінські платформи, інформаційні системи та регламенти процесів розробляються іншими командами, з іншими пріоритетами й часовими горизонтами. У результаті політичні заяви про національну стійкість рідко мають безпосереднє відображення в налаштуваннях систем управління ризиками, у регламентах міжвідомчого обміну даними або в логіці роботи алгоритмів у критичних цифрових сервісах. Системний підхід пропонує розглядати всі ці артефакти як елементи єдиної CAS, що потребує узгодженого проектування, тестування та постійного перегляду.

Суттєвим компонентом системного підходу є розуміння ролі зворотних зв'язків. У межах CAS не можна обмежитися одноразовим «надсиленням» стратегічних рішень згори донизу; необхідним є постійний обмін інформацією між рівнями та підсистемами. Реалізація НМС передбачає наявність розгалужених контурів зворотного зв'язку, де результати впровадження заходів, відгуки користувачів цифрових сервісів, дані про фактичні ефекти тих чи інших політик повертаються до центрів ухвалення рішень і стають підставою для корекції стратегій, регламентів і технічних рішень. Це означає, що проектування механізмів стійкості не може бути завершеним у традиційному сенсі; воно набуває характеру безперервного процесу калібрування системи.

У цифрову епоху саме цифрові платформи та аналітичні системи стають ключовим середовищем для реалізації таких контурів зворотного зв'язку. З огляду на це системний підхід неминуче включає в себе цифровий вимір, у якому реалізується концепція National E-Resilience. Якщо раніше було достатньо говорити про «електронний уряд» як про засіб надання

послуг, то в контексті НМС і CAS цифрові управлінські платформи виконують набагато глибшу функцію: вони є «операційною системою» стійкості. Через них відбувається збір даних про стан підсистем, аналіз ризиків і вразливостей, моделювання сценаріїв, підтримка прийняття рішень, а також автоматизована чи напівавтоматизована реалізація управлінських дій. Проте сама наявність цифрової платформи ще не гарантує подолання розриву між стратегією та практикою. Критичною є логіка її проєктування: чи вбудовані в неї принципи НМС, чи узгоджені дані, якими вона оперує, з індикаторами стійкості, передбаченими в стратегічних документах, чи відображає архітектура платформи реальну структуру взаємодії між акторами CAS. Якщо стратегія проголошує пріоритет міжвідомчої координації, а платформа фактично закріплює відомчі масиви даних, то системна невідповідність лише посилюється. Тому системний підхід наполягає: будь-яке цифрове рішення, яке позиціонується як інструмент реалізації НМС, має проєктуватися через призму архітектури CAS і цільової моделі стійкості.

Окремим виміром дослідження стає питання оцінювання ефективності механізмів реалізації НМС. Традиційні метрики, орієнтовані на виконання планів, обсяги фінансування чи кількість ухвалених нормативних актів, виявляються недостатніми для CAS. Вони не фіксують ні здатності системи адаптуватися до несподіваних подій, ні якості зворотних зв'язків, ні рівня інтегрованості цифрових інфраструктур. Тому системний підхід потребує нової покоління методик оцінювання, які б поєднували якісні та кількісні індикатори, враховували мережеві властивості системи, її динаміку та здатність до навчання. У цьому контексті модель Digital Resilience Assessment (DRA) постає як приклад такої методики, що фокусується саме на цифровій складовій CAS, але водночас вбудовується в загальну архітектуру НМС. DRA у системному контексті дозволяє оцінювати не лише технічні аспекти (кібербезпеку, відмовостійкість, доступність сервісів), а й ступінь того, наскільки цифрові платформи реально підтримують реалізацію

стратегічних цілей стійкості. Це означає вимірювання глибини інтеграції платформ із ключовими управлінськими процесами, здатності до швидкого переформатування сервісів під нові політики, рівня включеності громадян у цифрові контури прийняття рішень. Таким чином, оцінювання стає не зовнішнім «додатком» до стратегії, а внутрішньою частиною CAS, що впливає на подальше проєктування й калібрування механізмів.

Важливо також підкреслити, що системний підхід до НМС у цифровому середовищі вимагає переосмислення ролі людського фактора. У рамках CAS політики, державні службовці, ІТ-спеціалісти, аналітики, громадяни не є пасивними «ресурсами», а виступають активними агентами, які формують і змінюють правила гри, впливають на траєкторії розвитку системи. Стійкість у такій системі визначається не лише наявністю інституцій чи технологій, а й когнітивними, культурними, мотиваційними параметрами: готовністю до навчання, спроможністю працювати з невизначеністю, довірою до цифрових інструментів, готовністю делегувати частину рутинних рішень алгоритмам. Тому проєктування механізмів реалізації НМС має включати й елементи «когнітивної інженерії»: розвиток компетентностей, формування спільної мови між інженерами, управлінцями та політиками, створення інституційних умов для міждисциплінарної взаємодії.

Ще одним аспектом, що впливає із системного підходу, є необхідність моделювання сценаріїв розвитку CAS. Оскільки система функціонує в умовах високої невизначеності та множинних шоків, однозначне планування «від поточного стану до бажаного» виявляється непридатним. Натомість потрібне проєктування механізмів НМС таким чином, щоб вони були життєздатними в низці можливих сценаріїв. Це означає, що архітектура системи має містити елементи надлишковості, модульності, можливості швидкої перебудови ланцюгів процесів і маршрутів даних. У цифровому вимірі це реалізується через використання хмарних інфраструктур, мікросервісної архітектури платформ, відкритих стандартів

інтероперабельності. У нормативно-інституційному реалізується через гнучкі правові режими, механізми тимчасових регуляторних експериментів, децентралізовані формати співуправління.

Нарешті, системний підхід дозволяє інакше осмислити питання відповідальності за реалізацію НМС. У лінійній логіці можна намагатися призначити одного «відповідального» суб'єкта за стійкість, тоді як у CAS відповідальність розподіляється між численними акторами, які впливають на різні елементи архітектури. Це не знімає потреби в координаційному центрі, проте змінює його функцію: йдеться не стільки про директивне управління всіма процесами, скільки про налаштування правил взаємодії, інтерфейсів, стандартів, форматів обміну даними, а також про формування та підтримку культури спільної відповідальності. У цифровому шарі це втілюється в управлінні архітектурою національних платформ, стандартами відкритих API, політиками доступу до даних, механізмами контролю якості інформації.

Таким чином, наше дослідження, побудоване на вихідному фрагменті, дозволяє аргументовано стверджувати, що розрив між декларативними стратегіями стійкості та реальними механізмами їх імплементації є наслідком відсутності системного бачення держави як складної адаптивної системи. Подолання цього розриву потребує переходу від фрагментарних, відомчо орієнтованих рішень до архітектурно узгоджених механізмів, у яких кожен елемент, від закону до протоколу в серверній, проєктується як частина єдиної CAS. Умовою успішності такого переходу є інтеграція цифрових управлінських платформ в саму логіку НМС, формування контурів зворотного зв'язку, впровадження методик на зразок DRA для оцінки цифрової стійкості, а також розвиток інституційних і когнітивних спроможностей, що дозволяють системі вчитися та адаптуватися. Лише за таких умов стійкість перестає бути політичною декларацією й набуває статусу операційної властивості держави як складної адаптивної системи.

Обґрунтування системного підходу набуває особливої ваги, якщо розглядати НМС у контексті становлення цифрового суспільства. Саме

цифровізація радикально ускладнює як структуру державного управління, так і конфігурацію взаємодій між державою, суспільством і зовнішнім середовищем. З одного боку, з'являються нові можливості – великі масиви даних, аналітичні платформи, автоматизовані процедури, смарт-інфраструктури; з іншого – зростає щільність взаємозалежностей і швидкість поширення збоїв, що робить систему значно більш уразливою до каскадних ефектів. У таких умовах НМС не може бути просто «сукупністю політик» чи «набором планів реагування»: вона повинна постати як цілісна архітектура, що охоплює як інституційний, так і цифровий, когнітивний та інформаційний виміри. Саме системний підхід дозволяє коректно описати цю архітектуру та задати правила її еволюції.

Місце НМС у цифровому суспільстві визначається тим, що вона фактично виконує роль «керуючої надсистеми», яка координує та узгоджує численні потоки даних, рішень, ресурсів і впливів. Якщо в індустріальну епоху стійкість держави забезпечувалася переважно через фізичні резерви, інженерні споруди й інституційну ієрархію, то в цифровому суспільстві вирішальними стають властивості інформаційних та когнітивних процесів: наскільки швидко система здатна побачити загрозу, інтерпретувати її значущість, згенерувати й реалізувати адекватну відповідь. Це переводить НМС у площину не лише «управління ресурсами», а й «управління знанням» – структурованими даними, аналітикою, сценаріями, колективними уявленнями про реальність. Таким чином, цифрове суспільство робить стійкість не лише фізичною чи організаційною, а глибоко інформаційною та когнітивною категорією.

У цьому контексті зв'язок між НМС і концепцією National E-Resilience набуває принципового значення. Якщо НМС окреслює цілісний формат стійкості держави та суспільства, то National E-Resilience фокусується на її цифровому вимірі – на тому, як саме цифрові інфраструктури, платформи, сервіси та алгоритми підтримують або, навпаки, підривають здатність системи витримувати удари, адаптуватися та трансформуватися. Іншими

словами, National E-Resilience можна розглядати як операціоналізацію цифрового виміру НМС – це сукупність принципів, механізмів та інструментів, завдяки яким стратегії стійкості «втілюються» у вигляді конкретних цифрових управлінських рішень. У системному підході ці дві конструкції не конкурують, а доповнюють одна одну: НМС задає цілі й структуру CAS на макрорівні, тоді як National E-Resilience забезпечує її функціонування в цифровому середовищі, створюючи основу для інтегрованого моніторингу, координації та адаптації.

Ключовою передумовою такої інтеграції є наявність інтегрованої цифрової інфраструктури, яка об'єднує розрізнені інформаційні системи, реєстри, платформи в єдиний, керований простір. Без такої інфраструктури будь-які спроби впровадити НМС залишаються на рівні декларацій: кожен орган влади будує власні IT-рішення, визначає власні пріоритети, формує власні уявлення про ситуацію. У результаті держава функціонує не як єдина CAS, а як сукупність частково пов'язаних підсистем із різними моделями реальності. Інтегрована цифрова інфраструктура – це не просто технічна сумісність; це узгоджені стандарти даних, єдина логіка ідентифікації суб'єктів, спільні протоколи обміну, загальні принципи безпеки й доступу. Саме вона дозволяє реалізувати на практиці ідею єдиного інформаційного простору НМС, у якому рішення ухвалюються на основі цілісної, а не фрагментарної картини.

У національному контексті роль такої інтегрованої інфраструктури може виконувати централізована цифрова управлінська платформа типу C-eGovPro, що «прошиває» між собою ключові публічні реєстри, аналітичні системи, сервіси для громадян і бізнесу, ситуаційні центри, галузеві моніторингові платформи. Як елемент CAS, ця платформа не є просто технічним «хабом»; вона стає ядром інформаційно-аналітичної системи НМС, через яке здійснюється збір, фільтрація, агрегування й візуалізація даних, а також реалізація алгоритмів підтримки прийняття рішень. З точки зору системного підходу, саме наявність такого ядра дозволяє перетворити

розрізнену сукупність цифрових рішень у цілісну архітектуру National E-Resilience, інтегровану в НМС.

Однак цифрова інфраструктура сама по собі не гарантує правильного функціонування CAS. Не менш важливим є когнітивно-інформаційний вимір, що включає способи, якими інформація сприймається, інтерпретується й використовується людьми та інституціями. НМС у цифровому суспільстві неможливо звести до технічного управління даними; потрібні інституційно закріплені когнітивно-інформаційні механізми, які визначають, які саме дані вважати релевантними, які моделі застосовувати для аналізу, як уникати спотворень і маніпуляцій, яким чином забезпечувати прозорість та зрозумілість управлінських рішень. У термінах CAS це означає, що важливо не лише «прошити» канали комунікації й обміну даними, а й налаштувати правила, за якими система обробляє інформацію та вчиться на її основі.

Когнітивно-інформаційні механізми охоплюють кілька взаємопов'язаних рівнів. На макрорівні це стратегічні наративи й рамки інтерпретації, що задають суспільне розуміння стійкості, загроз, пріоритетів розвитку [335-336]. Вони визначають, наприклад, чи сприймається цифрова трансформація як інструмент посилення обороноздатності та соціальної згуртованості, чи лише як технократична модернізація послуг. На мезорівні це інституційні процедури аналізу інформації: методики оцінки ризиків, стандарти підготовки аналітичних записок, протоколи роботи ситуаційних центрів, вимоги до сценарного моделювання. І нарешті, на мікрорівні – це компетентності конкретних фахівців, їхня здатність працювати з великими даними, критично оцінювати джерела, використовувати інструменти аналітики й візуалізації, усвідомлювати обмеження алгоритмів і моделей.

У межах системного підходу такі когнітивно-інформаційні механізми розглядаються як невід'ємна частина архітектури НМС. Якщо цифрова платформа є «мозком» системи в технічному сенсі, то когнітивні механізми – це її «свідомість», тобто спосіб, яким система формує уявлення про себе та світ. Від того, наскільки узгоджені між собою технічні й когнітивні

компоненти, залежить, чи зможе НМС уникнути двох крайнощів: технократичного фетишизму (довіра до цифр і алгоритмів без належного критичного осмислення) та інформаційного хаосу (надмір даних без здатності їх інтерпретувати й перетворювати на знання).

У такій динамічній моделі НМС постає не як статична «структура безпеки», а як жива, «навчальна» CAS, що постійно коригує власну архітектуру під впливом досвіду криз і трансформацій. Системний підхід забезпечує методологічну рамку для опису й проектування цієї еволюції: він дозволяє врахувати складну мережу взаємодій між цифровою інфраструктурою, інституціями, політиками, культурами, знаннями. National E-Resilience у цій рамці є не просто галузевою концепцією «кіберстійкості» чи «цифрової трансформації», а функціональним ядром НМС у цифровому середовищі, яке робить можливим перехід від декларацій до операційної стійкості. Інтегрована цифрова інфраструктура, своєю чергою, виступає матеріальним носієм цього ядра, а когнітивно-інформаційні механізми – інтелектуальним «двигуном», що перетворює дані на знання, а знання – на адекватні рішення й адаптивні дії.

Таким чином, обґрунтування системного підходу до НМС в умовах цифрового суспільства неминуче спирається на чотири взаємопов'язані опори:

- 1) розуміння держави як складної адаптивної системи;
- 2) визнання центральної ролі National E-Resilience як цифрового виміру стійкості;
- 3) розбудову інтегрованої цифрової інфраструктури як технічної основи цієї стійкості;
- 4) формування когнітивно-інформаційних механізмів як інтелектуальної й культурної основи її функціонування (таблиця 4.1).

Лише синхронний розвиток усіх цих елементів дає змогу перетворити НМС з декларативної конструкції на дієву, динамічну систему, здатну витримувати, переосмислювати й трансформувати виклики цифрової доби.

Таблиця 4.1

Концептуалізація авторської парадигми НМС

Компонент системного підходу	Зміст у Національній моделі стійкості (НМС)	Зміст у National E-Resilience	Емпіричний приклад (Україна)
1. Онтологічний статус	Макрорівнева рамка стійкості держави й суспільства як цілісної системи; задає цілі, принципи, базові виміри (безпековий, економічний тощо)	Цифровий шар НМС, що оперує інфраструктурами, платформами, даними й алгоритмами, через які реалізуються цілі стійкості	Стратегії національної стійкості, воєнної безпеки, цифрової трансформації (через «Дію», «Трембіту», хмарні рішення
2. Об'єкт фокусу	Інститути, політики, процедури, що забезпечують стійкість фізичних, соціальних та управлінських підсистем	Канали обміну даними, механізми кіберзахисту, аналітичні системи, які підтримують рішення і забезпечують безперервність управління	Перенесення критичних реєстрів у хмару, побудова ситуаційних центрів на базі інтегрованих даних («COTA», DREAM)
3. Тип домінуючих механізмів	Нормативно-правові, організаційно-інституційні, стратегічно-планувальні механізми; розподіл повноважень	Техніко-організаційні механізми: інтегровані платформи (C-eGovPro), API, протоколи обміну даними, автоматизовані процеси, кіберзахист	Впровадження «Трембіти» як системи міжвідомчої взаємодії, «Дії» як єдиного фронт-енду для послуг, нац. системи резервного копіювання даних
4. Роль даних та інформації	Дані розглядаються як ресурс для стратегічного планування, оцінки ризиків і формування політик у різних вимірах стійкості	Дані є центральним об'єктом управління: збираються в реальному часі, інтегруються, аналізуються й перетворюються на аналітику та тригери для автоматизованих дій	Використання великих даних для координації енергетичного балансу, моніторингу міграції ВПО, таргетованих виплат через «єДопомогу», «єПідтримку»
5. Когнітивно-інформаційні механізми	Формують спільні уявлення про загрози, пріоритети, допустимі ризики; задають рамки інформаційної політики, освіти, комунікації	Реалізуються через аналітичні модулі, системи раннього попередження, моделі машинного навчання, що підтримують інтерпретацію ситуації та сценарне моделювання	Систематичний аналіз інформаційного середовища, реагування на дезінформацію, когнітивна діагностика; використання аналітичних панелей
6. Характер адаптації та навчання системи	Адаптація відбувається через перегляд стратегій, зміну інституційної архітектури, оновлення законодавства та процедур	Адаптація реалізується шляхом оновлення алгоритмів, конфігурації платформ, правил обміну даними; впровадження нових сервісів і цифрових модулів у відповідь на кризи	Швидке створення і розвиток сервісів «єВорог», «єВідновлення», модулів для обліку руйнувань та відновлення інфраструктури після 2022 року
7. Типові ризики та вразливості	Інституційна інерція, фрагментація політик, низька координація, дефіцит довіри	Кіберзагрози, технологічні залежності, нерівний доступ до цифрових сервісів, перевантаження даними без належних когнітивних механізмів	Масовані кібератаки на державні реєстри, нерівномірна цифрова спроможність регіонів, потреба у посиленні цифрової інклюзії влади

Авторська позиція дослідження виходить із того, що Національна модель стійкості може бути реально ефективною лише за умови, коли НМС проєктується і функціонує як цілісна соціотехнічна система, в якій стратегічні цілі, інституційні механізми, цифрові інфраструктури та когнітивно-інформаційні практики взаємопов'язані в єдину архітектуру. У цьому контексті особливого значення набуває чітке розмежування й одночасно узгодження макрорівневої рамки НМС та її цифрового виміру, який концептуалізується як National E-Resilience.

У такому підході НМС визначається як онтологічний «формат» стійкості держави й суспільства, адже саме на її рівні формуються загальне розуміння стійкості, основні виміри (безпековий, економічний, соціальний, інформаційний, екологічний тощо), а також принципи й цілі, що задають спрямованість політик та інституційних перетворень. Це макрорівневе бачення закріплюється в стратегічних документах, доктринах, комплексних планах відновлення, які окреслюють, якою має бути життєздатна, здатна до адаптації й розвитку держава. Однак у цифровому суспільстві самої рамкової НМС недостатньо, адже така модель обов'язково повинна мати власний цифровий зміст, де стійкість «живе» у вигляді конкретних платформ, реєстрів, даних, алгоритмів і цифрових сервісів. Саме цей шар описується поняттям National E-Resilience. Отже, якщо НМС відповідає на запитання «для чого» і «у яких вимірах» забезпечується стійкість, то National E-Resilience відповідає на запитання «за допомогою яких цифрових інструментів, інфраструктур та процесів ця стійкість реалізується на практиці». Цифрові платформи, інтегровані реєстри, міжвідомчі шлюзи обміну даними, аналітичні модулі, системи кіберзахисту – усе це не є другорядним або обслуговувальним елементом, а формує логічну структуру НМС, через яку циркулюють дані, відбувається координація дій, запускаються механізми реагування.

Емпірично в українських умовах така подвійна онтологія – НМС як макрорівнева рамка та National E-Resilience як її цифровий вимір

проявляється через взаємопов'язаність стратегій національної безпеки, цифрової трансформації, кібербезпеки, планів відновлення й модернізації критичної інфраструктури. Ці нормативно-правові акти не існують у вакуумі: вони реалізуються через конкретні цифрові рішення – державні реєстри, застосунок «Дія» як єдиний фронт-енд для громадян, систему міжвідомчого електронного обміну «Трембіта», міграцію даних до хмарних середовищ, розгортання ситуаційних центрів і галузевих моніторингових платформ. Саме через такі інструменти принципи функціонування НМС втілюються в операційні практики National E-Resilience.

Відповідно, змінюється й об'єкт фокусу на різних рівнях. У НМС у центрі аналізу й проєктування перебувають інститути, механізми, політики та процедури, що забезпечують стійкість фізичних, соціальних та управлінських систем: оборонного сектору, економіки, соціального захисту, системи охорони здоров'я, критичної інфраструктури. Тут вирішальними є питання розподілу повноважень, нормативно-правового забезпечення, процедур кризового управління, мультиакторної взаємодії. Водночас, у межах National E-Resilience фокус зміщується на цифрові платформи та інфраструктури, канали обміну даними, аналітичні й моніторингові системи, механізми кіберзахисту, тобто на ті елементи, які забезпечують безперервність управління в реальному часі. Без цього цифрового виміру ґрунтовно спроектовані інститути та політики НМС залишаються фрагментарними, нездатними до оперативного реагування на динамічні загрози.

Українська практика останніх років наочно демонструє, що перенесення критичних реєстрів у хмарні середовища, створення ситуаційних центрів на основі інтегрованих даних (як-от системи «СОТА», платформа DREAM у сфері відбудови), впровадження уніфікованих каналів обміну інформацією між відомствами – це не просто ІТ-проєкти, а ключові інструменти реалізації НМС. Вони дозволяють органам влади на всіх рівнях отримувати цілісну картину стану систем, координувати ресурси, моделювати наслідки рішень, а відтак – втілювати смарт-резильєнтні

регіональні стратегії на основі реальних, а не уявних даних.

При цьому тип домінуючих механізмів державного управління у двох вимірах також суттєво різниться, але саме їхнє поєднання визначає ефективність НМС. На рівні самої моделі стійкості домінують нормативно-правові та організаційні механізми: закони, стратегії, доктрини, координаційні органи, міжвідомчі формати взаємодії, регламенти кризового управління. Вони окреслюють, хто за що відповідає, якими є цілі, які принципи мають бути дотримані під час реагування на кризи, як вибудовується вертикаль і горизонталь взаємодії.

Натомість у вимірі National E-Resilience та цифрової інфраструктури домінують *техніко-організаційні механізми – інтегровані цифрові платформи (централізована управлінська платформа на кшталт C-eGovPro), стандартизовані API та протоколи обміну даними, моделі даних, автоматизовані бізнес-процеси, комплекси кіберзахисту, системи резервного копіювання та відновлення*. Саме вони відповідають за те, щоб стратегічно визначені процеси реально могли бути виконані в потрібний час, у потрібному масштабі і з потрібною швидкістю.

Емпіричними ілюстраціями такої взаємодії є впровадження «Трембіти» як національної системи міжвідомчого електронного обміну, розбудова «Дії» як єдиного фронт-енду державних послуг, формування національних рішень для резервного копіювання й географічного рознесення критичних реєстрів. Усі ці технічні кроки напряду пов'язані з реалізацією НМС, оскільки дають змогу підтримувати безперервність базових державних функцій – реєстрації, ідентифікації, виплат, доступу до послуг – навіть в умовах масованих атак чи руйнування фізичної інфраструктури.

У системному підході центральним стає питання ролі даних та інформації. На рівні НМС дані розглядаються як ресурс для стратегічного планування, оцінки ризиків, моніторингу виконання політик у різних секторах. Вони дають можливість ухвалювати обґрунтовані рішення щодо пріоритетів відновлення, розподілу ресурсів, посилення вразливих регіонів,

оцінювати ефективність реалізованих програм. У вимірі National E-Resilience дані набувають ще вагомійшої ролі – вони стають центральним об'єктом управління. Йдеться не лише про накопичення статистики, а про організований збір даних у режимі близькому до реального часу, їх інтеграцію з різних джерел (державні органи, місцеве самоврядування, бізнес, громадянське суспільство, міжнародні партнери), подальший аналіз за допомогою сучасних аналітичних інструментів, а також використання цих аналітичних продуктів для запуску автоматизованих або швидких управлінських реакцій.

Прикладами такого підходу в Україні є використання великих даних для балансування енергосистеми в умовах масових атак на енергетичну інфраструктуру, моніторинг переміщення внутрішньо переміщених осіб і таргетовані соціальні виплати через цифрові інструменти («ЄДопомога», «ЄПідтримка»), аналітика щодо потреб громад у відновленні та розвитку. У цих кейсах дані не є абстрактною категорією – вони виступають основою для конкретних управлінських рішень, а отже, і складником стійкості.

Водночас ефективність використання даних неможлива без належних когнітивно-інформаційних механізмів. У НМС вони включають ті елементи, які формують спільні уявлення про загрози, ризики, пріоритети розвитку, прийнятні рівні ризику, сценарії майбутнього. Це – інформаційна політика, система освіти та підвищення кваліфікації, публічні комунікації, що задають рамки осмислення реальності суспільством та елітами. На рівні National E-Resilience когнітивно-інформаційні механізми реалізуються у вигляді аналітичних модулів, ситуаційних дашбордів, систем раннього попередження, моделей штучного інтелекту й машинного навчання, що підтримують інтерпретацію складних масивів даних, виявлення аномалій, побудову сценарних прогнозів. Без поєднання цих двох складових – людської здатності до критичного мислення та технологічних інструментів аналітики – цифрова інфраструктура ризикує перетворитися на «фабрику цифр» без реальної здатності генерувати знання та підтримувати обґрунтовані

управлінські рішення. Українська емпірика в цьому вимірі включає, зокрема, розгортання систем когнітивної діагностики інформаційного простору, реагування на дезінформаційні кампанії, використання аналітичних панелей у РНБО, урядових штабах, галузевих міністерствах. Ці практики демонструють поступовий перехід від реактивного реагування на інформаційні загрози до проактивного моніторингу й управління інформаційним середовищем як невід’ємним елементом НМС.

Не менш важливим елементом системного підходу є характер адаптації та навчання системи. На рівні НМС адаптація виявляється передусім у перегляді стратегій, реформуванні інституцій, оновленні законодавства й процедур. Це – інституційне навчання, коли держава, суспільство й управлінська система в цілому роблять висновки з криз, коригують свої «правила гри», змінюють архітектуру владних відносин, створюють нові органи координації, укріплюють регіональний вимір стійкості. Натомість у вимірі National E-Resilience адаптація набуває форми постійного оновлення алгоритмів, модифікації конфігурацій платформ, зміни правил обміну даними, розроблення нових цифрових сервісів і модулів у відповідь на специфічні кризові виклики. Тут важливою є не лише здатність системи витримати удар, а й її здатність швидко перепроєктувати власні цифрові інструменти так, щоб вони відповідали новим реаліям.

Показовими є приклади створення у надзвичайно короткі терміни цифрових сервісів «ЄВорог» для повідомлення про пересування ворога, «ЄВідновлення» для подання заявок на відшкодування за зруйноване житло, рішень для системного обліку руйнувань та планування відбудови інфраструктури, побудови смарт резильєнтних регіональних стратегій на основі даних про ризики, ресурси та вразливості кожного регіону. Ці кейси ілюструють, як Національна модель стійкості, будучи вплетеною в цифрову інфраструктуру, набуває властивостей навчальної системи, здатної еволюціонувати разом із середовищем.

Нарешті, системний розгляд НМС і National E-Resilience потребує

чіткого усвідомлення типових ризиків та вразливостей. *На рівні НМС ключовими загрозами є інституційна інерція, фрагментація політик, слабка координація між рівнями влади й секторами, низький рівень довіри громадян до інституцій. Ці чинники підривають здатність держави до консолідованої відповіді на кризи, сприяють дублюванню функцій, виникненню конфліктів повноважень, повільній імплементації рішень. На рівні National E-Resilience ризики мають інший, хоча й тісно пов'язаний характер – кіберзагрози, технологічна залежність від окремих провайдерів та технологій, «вільний рух» даних, коли кожен орган влади тримає інформацію «у себе», цифрова нерівність між регіонами й соціальними групами, перевантаження системи даними без достатньо розвинених когнітивних та аналітичних механізмів.*

Український досвід останніх років показав, наскільки масовані кібератаки можуть паралізувати роботу органів влади, як різний рівень цифрової спроможності регіонів впливає на можливість швидко розгортати нові сервіси, як дефіцит цифрової інклюзії у вразливих груп населення обмежує ефект від впровадження навіть найкращих цифрових рішень. У цьому контексті авторська позиція особливо наголошує: саме створення інтегрованої цифрової інфраструктури моніторингу НМС, підтримане смарт-резильєнтними регіональними стратегіями й інституційно закріпленими когнітивно-інформаційними механізмами, є необхідною умовою подолання зазначених вразливостей.

Інтегрована цифрова інфраструктура моніторингу – це горизонтальний вектор стійкості, який поєднує всі розглянуті вище виміри: забезпечує постійний збір і аналіз даних, підтримує адаптацію через оновлення алгоритмів, зменшує ризики фрагментації. Смарт-резильєнтні регіональні стратегії забезпечують вертикальну конкретизацію НМС, враховують унікальні профілі ризиків, ресурсів і вразливостей кожного регіону та вплітаючи їх у загальнонаціональну архітектуру стійкості. Інституційно закріплені когнітивно-інформаційні механізми, як системної інформаційної політики так і у вигляді структур з когнітивної діагностики й

аналітики гарантують, що дані будуть інтерпретовані належним чином, а прийняті рішення не лише технічно коректні, а й соціально легітимні та стратегічно виважені. Лише в такій формалізації НМС виходить за межі декларацій і перетворюється на дієву модель, яка в цифровому суспільстві здатна забезпечити стійкість, адаптацію та розвиток держави навіть в умовах тривалих воєнних і гібридних викликів.

На етапі аналізу НМС у дисертації стало очевидно, що класичні, «лінійні» моделі управління та оцінювання стійкості не пояснюють ключовий розрив між декларативними стратегіями й реальними механізмами їх реалізації. У межах аналізу систем державного управління було встановлено, що запровадження систем індикаторів, рейтингів, показників ефективності саме по собі не гарантує посилення стійкості, а подекуди навіть призводить до протилежного ефекту – формалізації, імітації діяльності, «підгонки» реальності під показники. Це прямо вивело приводить до проблеми ролі спостерігача й оцінювача в управлінській системі, адже той, хто вимірює, задає показники й інтерпретує результати, фактично впливає на поведінку об'єкта, змінюючи конфігурацію всієї системи.

Класична концепція складної адміністративної системи виходить із припущення про «зовнішнього спостерігача», який бачить об'єкт «зі сторони» й не впливає на нього фактом вимірювання [335]. Проте в умовах цифрової трансформації, коли кожен індикатор стійкості вбудовується в цифрові платформи, алгоритми прийняття рішень, системи стимулів, таке припущення стає неприйнятним. Саме тому в дослідженні нами пропонується перехід до підходу, який принципово визнає, що спостерігач і засоби оцінювання є частиною НМС, а не зовнішнім додатком до неї. Це дозволяє по-іншому побачити як інтегровану цифрову інфраструктуру моніторингу, так і смарт резильєнтні регіональні стратегії та когнітивно-інформаційні механізми стійкості – не лише як інструменти, а як елементи рефлексивної, самодетермінованої системи.

У межах дисертаційного дослідження методологічний апарат

системного аналізу використовується не як формальна декларація, а як принципова епістемологічна рамка проектування та оцінювання НМС в умовах цифрової трансформації. Системний аналіз задає логіку розгляду держави як складної адаптивної системи (CAS) з багаторівневою структурою, численними зворотними зв'язками, емерджентними властивостями та нелінійною динамікою. Надалі така рамка уточнюється, отже, будь-яка система управління й оцінювання не є зовнішньою щодо об'єкта, а включає спостерігача у контур системи. Це означає, що суб'єкти, які проєктують НМС, формують індикатори, здійснюють моніторинг і оцінювання, самі стають частиною CAS та впливають на її поведінку.

Зазвичай, у сучасних дослідженнях системи державного управління фігурує модель «система – середовище – зовнішній спостерігач», натомість ми пропонуємо апріорно виходити з того, що будь-яке спостереження, вимірювання й оцінка є конструкціями конкретного суб'єкта, обумовленими його цілями, цінностями, інституційними рамками й когнітивними обмеженнями. У контексті НМС це має подвійне значення. По-перше, показники стійкості, алгоритми моніторингу, моделі ризиків конструюються певними інституціями (державні органи, експертні спільноти, міжнародні організації) і відображають їхню картину бажаного стану системи. По-друге, як тільки ці показники вбудовуються в механізми управління (стають основою для розподілу ресурсів, оцінки ефективності, політичної відповідальності), вони починають змінювати поведінку об'єктів регулювання.

Власне, авторська методологія формалізації НМС спирається на ефект (закон) Ч.Гудгарта, за яким «коли показник стає метою, він перестає бути нормальним показником» («Any observed statistical regularity will tend to collapse once pressure is placed upon it for control purposes») [336]. У рамках НМС це означає, що будь-який індикатор стійкості – наприклад, відсоток цифрових послуг, доступних онлайн; частка інтегрованих реєстрів; кількість проведених навчань із кібербезпеки; формалізований рівень готовності

регіону – у момент, коли він фіксується як ключова мета і прив’язується до стимулів (фінансування, політичні оцінки, рейтинги), починає спотворювати реальну динаміку системи. Суб’єкти управління прагнуть «покращити показник», а не реальну стійкість: формально інтегрують системи без реальної інтеоперабельності, проводять квазі-навчання, створюють регіональні стратегії на папері без фактичної цифрової підтримки їх виконання. Уникнути цього ефекту можна лише тоді, коли механізми оцінювання й моніторингу самі розглядаються як частина НМС, тобто підлягають рефлексії, корекції та оцінюванню.

У нашому дослідженні це безпосередньо пов’язано з концепцією інтегрованої цифрової інфраструктури моніторингу та моделлю Digital Resilience Assessment (DRA). *Авторська позиція* полягає в тому, що система індикаторів і алгоритмів оцінки стійкості має проєктуватися не як жорсткий набір методик, а як адаптивний контур спостереження другого порядку, який, по-перше, фіксує не лише стан об’єктів (інфраструктур, процесів, інститутів), а й те, як самі індикатори впливають на поведінку суб’єктів; по-друге, включає регулярний перегляд переліку показників, питомої ваги і порогових значень у контексті виявлених стратегій «обходу» або формального виконання; по-третє, поєднує кількісні (цифрові, формалізовані) та якісні (експертні, когнітивно-інформаційні) оцінки, мінімізуючи ризик редукації складних явищ до однієї-двох метрик.

У практичному вимірі це означає, що інтегрована національна цифрова управлінська платформа моніторингу НМС C-eGovPro (як елемент National E-Resilience) має бути здатною не лише збирати й візуалізувати показники, а й підтримувати мета-моніторинг: аналізувати закономірності змін самих індикаторів, виявляти аномальні патерни поведінки (наприклад, різкі стрибки виконання показників у певних регіонах, що можуть свідчити про формальне «підтягування звітності»), корелювати цифрові метрики з незалежними емпіричними джерелами (опитування, польові спостереження, дані громадянської науки). Такий підхід напряду пов’язаний із

когнітивно-інформаційними механізмами стійкості: спостерігач (аналітик, інституція, алгоритм) має усвідомлювати власну роль у конструюванні реальності й закладати в систему можливість самокорекції.

У цьому контексті авторська методологія дозволяє формалізувати і концептуалізувати смарт-резильєнтні регіональні стратегії (СРРС). Традиційний (класичний) підхід зводився б до розроблення типових наборів індикаторів для регіонів держави (індекс цифрової готовності, рівень інвестицій, частка відновленої інфраструктури тощо) з подальшим порівнянням числових значень. Дисертаційне дослідження виходить з того, що такі стратегії мають будуватися як рефлексивні конструкти, де регіональні суб'єкти долучені до спільної розробки індикаторів, усвідомлюють, як саме їхні дії впливають на метрики, і разом з національним центром стійкості беруть участь у періодичному перегляді системи оцінювання. Ми у дослідженні визначаємо регіон виступає не просто об'єктом вимірювання («регіон - Автономна Республіка Крим, області, міста Київ та Севастополь» – Закон України «Про засади державної регіональної політики» [337], «регіон – територія Автономної Республіки Крим, області, міст Києва та Севастополя» – Закон України «Про стимулювання розвитку регіонів» [338], втратив чинність), а співспостерігачем і співдизайнером НМС, що знижує ризик формального виконання показників і посилює довіру до цифрової інфраструктури моніторингу.

Важливим наслідком такого підходу є визначення для інтегрованої цифрової інфраструктури моніторингу вимоги прозорості та інтерпретованості. Якщо алгоритми обчислення індексів стійкості, порогові значення, ваги показників приховані або зрозумілі лише вузькому колу технічних фахівців, системи НМС ризикують стати «чорними скриньками», які відтворюють упередження спостерігачів та інтереси окремих груп. **Квінтесенція авторської НМС – «спостерігач повинен бути видимим у моделі».** Це означає, що методики DRA, формули інтегральних показників, логіка сценарного моделювання мають бути документовані й комуніковані

ключовим стейкхолдерам (центральному органам влади, регіонам, громадянському суспільству); у цифровій управлінській платформі мають бути реалізовані інструменти пояснюваної аналітики, які дозволяють користувачам бачити, як саме поєднання окремих індикаторів вплинуло на загальну оцінку; забезпечується можливість «розкласти» інтегральний показник на компоненти та ініціювати перегляд системи, якщо виявлено систематичні спотворення чи небажані поведінкові ефекти.

У цьому зв'язку когнітивно-інформаційні механізми стійкості виступають не лише як інструмент боротьби з дезінформацією, а й як захист від внутрішніх викривлень, спричинених некритичним використанням показників. Розвиток цифрової, статистичної та критичної грамотності державних службовців, аналітиків, керівників різних рівнів є не менш важливим елементом НМС, ніж технічна інтеграція реєстрів чи розгортання хмарних рішень. Без цього спостерігач залишається «сліпим» до власного впливу на систему, а отже – підсилює вже згадані ризики ефекту Гудхарта.

Авторська позиція полягає в тому, що методологія системного аналізу дозволяє побачити НМС не як зовнішній набір регуляторних та технічних рішень, а як *рефлексивну, самодетерміновану та самокоригувальну систему, у якій інтегрована цифрова інфраструктура моніторингу не лише збирає й обробляє дані, а й підтримує зворотний зв'язок другого порядку – аналізує власні індикатори, виявляє викривлення, ініціює перегляд алгоритмів; смарт резильєнтні регіональні стратегії формуються за участі регіонів як співспостерігачів, що враховує локальні контексти й знижує ризик формального виконання метрик; когнітивно-інформаційні механізми стійкості забезпечують критичне осмислення показників, пояснюваність аналітики та довіру до цифрових інструментів*. Лише за умов інтеграції цих компонентів – технічних, інституційних і когнітивних – НМС може уникнути пастки «показникової стійкості» та набути якостей справжньої адаптивної системи, здатної не лише вимірювати, а й усвідомлено формувати власну стійкість у цифрову епоху.

4.2. Алгоритм динамічного моніторингу функціонування національної моделі стійкості та його інтеграція у межах Digital Resilience Assessment (DRA)

У форматі теорії систем і системного аналізу система державного управління в умовах цифрової трансформації постає не як «єдина вертикаль влади», а як «система систем» (System of Systems, SoS) [339]. Це не просто термінологічна зміна, а принципова трансформація управлінської детермінанти: ми відходимо від уявлення про державу як ієрархічну «машину» з одним центром прийняття рішень і розглядаємо державного (публічного) управління як сукупність порівняно автономних, але взаємозалежних підсистем (центральні органи виконавчої влади, місцеве самоврядування, незалежні регулятори, державні агенції, публічні сервісні платформи тощо), які мають власну логіку функціонування, але об'єднані спільними цілями стійкості, розвитку та публічної цінності.

До таких підсистем належать, зокрема, енергетика, фінансово-банківський сектор, охорона здоров'я, сектор безпеки й оборони, транспорт і логістика, інформаційний простір і цифрові сервіси, системи місцевого самоврядування тощо. Кожна з них має власні правила гри, суб'єктів, алгоритми функціонування, регуляторні рамки, технологічні платформи, але одночасно включена в загальну архітектуру НМС. Саме тут стає очевидною необхідність інтегрованої цифрової інфраструктури: без неї SoS лишається набором «фрагментів», які погано координують свої дії в кризових умовах. У цифрову епоху ключовою характеристикою такої SoS є емерджентність – поява нових системних властивостей, які не зводяться до властивостей окремих елементів. Емерджентні ефекти можуть бути як позитивними (нові можливості), так і негативними (нові вразливості) [341].

Позитивний бік емерджентності ілюструє згаданий приклад – цифрова інтеграція банківського сектору та державних реєстрів (ідентифікаційні дані, реєстри платників податків, соціальних одержувачів тощо) породжує нову

системну властивість – можливість миттєвих, масових, таргетованих соціальних виплат у кризових ситуаціях. Саме завдяки цьому з'являється програма на кшталт «Підтримка»; коли держава може за лічені години ідентифікувати цільові групи, перевірити їхні права, переказати кошти через інтегровану цифрову інфраструктуру, а громадяни – оперативно отримати підтримку через мобільний застосунок. Водночас та сама інтеграція генерує нову якість вразливості. Коли ключові функції – ідентифікація, верифікація, фінансові операції, облік прав – сходяться в єдині цифрові шлюзи, виникає ризик каскадних відмов, коли одна успішна кібератака на критичний шлюз обміну даними або на центральну платформу може спричинити лавиноподібний збій у багатьох підсистемах – від призупинення соціальних виплат до порушення платіжних операцій, блокування доступу до публічних послуг, втрати довіри до цифрових інструментів. Таким чином, емерджентна стійкість і емерджентна вразливість формують дихотомію цифровізації.

У межах нашого дослідження це означає, що проєктування НМС як SoS неможливе без: 1) архітектурного моделювання зв'язків між підсистемами, а не лише оптимізації кожної з них окремо; 2) усвідомленого управління емерджентними ефектами – передбачення не тільки прямих, а й непрямих наслідків цифрової інтеграції; розроблення інтегрованих механізмів моніторингу та сценарного моделювання, які дозволяють виявляти й тестувати можливі каскадні ефекти ще до того, як вони проявляться в практиці.

З огляду на це, НМС вимагає балансу між інтеграцією та автономією: з одного боку (без цифрової інтеграції неможливо досягти ефективної координації, швидких виплат, гнучкого управління ресурсами), з іншого – надмірна централізація та залежність від окремих вузлів створюють «єдині точки відмови», критичні для всієї системи. У цьому контексті інтегрована цифрова інфраструктура моніторингу, смарт резильєнтні регіональні стратегії та когнітивно-інформаційні механізми, про які йшлося раніше, набувають додаткового сенсу: 1) як інструменти узгодження дій між

підсистемами SoS; 2) як засоби виявлення емерджентних вразливостей (наприклад, через моделювання кібератак і їхніх крос-секторальних наслідків); як механізми навчання системи, здатні перетворювати досвід криз на оновлені архітектурні рішення (перерозподіл функцій, дублювання критичних вузлів, зміна протоколів обміну тощо).

Саме тому проектування механізмів реалізації НМС має базуватися на принципах, адаптованих до державного управління: по-перше, *принцип необхідної різноманітності* («Law of requisite variety») – для ефективного управління системою керуючий механізм повинен мати не меншу різноманітність станів, ніж керована система. У контексті НМС це означає, що арсенал інструментів реагування держави (цифрових, організаційних, силових) повинен відповідати спектру потенційних загроз (гібридних, кінетичних, техногенних). По-друге, гомеостаз через зворотний зв'язок – стійкість забезпечується наявністю негативних зворотних зв'язків, які повертають систему до стабільного стану при відхиленнях; тут цифровізація дозволяє скоротити петлю зворотного зв'язку (feedback loop) до режиму реального часу. По-третє, здатність досягати результату (відновлення функцій держави) різними шляхами, що вимагає альтернативних алгоритмів дій у нормативну базу та технічну архітектуру (таблиця 4.2).

Таблиця 4.2

Формалізація авторського підходу до System of Systems

Аспект	Характеристика НМС як SoS	Емерджентні можливості	Емерджентні вразливості / ризики
Структура	Набір автономних, але взаємопов'язаних підсистем (енергетика, фінанси, охорона здоров'я, транспорт, інформаційний простір, регіональне управління), об'єднаних спільними цілями стійкості	Гнучкість і модульність, можливість пере-розподілу функцій між підсистемами, локальних інновацій, що масштабуються на національний рівень	Ризик фрагментації за відсутності узгодженої архітектури підсистем оптимізуються «для себе», погіршуючи загальну стійкість
Інтеграція через цифрову інфраструктуру	Підсистеми з'єднані через інтегровані платформи, реєстри, шлюзи обміну даними (наприклад, С-eGovPro, «Трембіта», національні хмарні рішення).	Швидка міжсекторальна координація, миттєві виплати, комплексні сервіси («Підтримка», сервіси для ВПО), моніторинг ситуації для всіх рівнів управління	Посилення залежності від центру; можливість каскадного колапсу через атаку або збій у критичному шлюзі чи хмарній платформі

Продовження таблиці 4.2

Аспект	Характеристика НМС як SoS	Емерджентні можливості	Емерджентні вразливості / ризики
Автономія підсистем	Кожна підсистема має власних власників, регуляцію, IT-ландшафт, бізнес-процеси, але повинна дотримуватися загальнонаціональних стандартів інтероперабельності й безпеки	Локальні експерименти й інновації (смарт-рішення на рівні громад, галузеві платформи), які можна інтегрувати в НМС; підвищення адаптивності завдяки різноманітності	Конфлікти стандартів, конкуренція інтересів, повільне узгодження змін; ризик, що одна «слабка» підсистема (наприклад, охорона здоров'я) стане тригером загально-системної кризи
Емерджентні сервіси та функції	Нова функціональність виникає на перетині кількох підсистем (фінанси + реєстри + мобільні платформи; енергетика + геодані + безпека тощо)	Масові цифрові програми підтримки населення й бізнесу під час криз (виплати, компенсації, субсидії), ситуаційні центри, що поєднують дані з різних секторів для ухвалення рішень	Невидимі залежності – збій у «другорядній» підсистемі (наприклад, у геосервісах) може паралізувати критично важливі сервіси (логістику евакуації, енергетичний диспетчинг тощо)
Управління та координація	Мережево-ієрархічна модель - національний рівень задає рамку НМС і архітектурні принципи, галузі та регіони конкретизують і реалізують стратегії	Можливість мультиакторного управління, коли спільне вироблення політик державою, регіонами, бізнесом, громадянським суспільством; координація через єдині цифрові платформи	Ризик «паралічу управління» у кризах за відсутності чітких протоколів: суперечливі команди, дублювання функцій, криза прийняття рішень через множинність центрів впливу
Моніторинг і сценарне моделювання	Інтегрована цифрова інфраструктура моніторингу збирає дані з різних підсистем, підтримує моделювання каскадних ефектів і тестування сценаріїв	Раннє виявлення міжсекторальних ризиків, можливість «проганяти» кризи віртуально до їх фактичного настання, підготовка відповідей	Небезпека надмірної віри в моделі, недооцінка людського фактору, ризик техно-кратичної заміни політичних рішень автоматизованими рекомендаціями
Стійкість і каскадні ефекти	Стійкість розглядається як властивість не окремої підсистеми, а всієї конфігурації SoS з її зв'язками та зворотними зв'язками	Можливість будувати надлишковість і резерви не лише всередині підсистем, а й між ними (крос-секторальні резервні канали, альтернативні ланцюги постачання, дублювання критичних функцій)	Посилення системних ризиків: локальна подія (атака, збій, помилка в алгоритмі) може запускати неконтрольований ланцюг відмов, якщо архітектура не враховує принципів модульності й обмеження зв'язності

Джерело: розроблено автором

Аналіз НМС як System of Systems у поєднанні з попередніми висновками про CAS, National E-Resilience, інтегровану цифрову інфраструктуру дозволяє сформулювати цілісну авторську позицію:

1) *стратегічний рівень* має експліцитно визнавати сутність держави як «система в системі» й детермінувати архітектурні принципи інтеграції підсистем (модульність, відсутність «єдиних точок відмови», стандарти

інтероперабельності, вимоги до сценарного моделювання каскадних ризиків);

2) *цифровий рівень* (National E-Resilience) повинен забезпечити таку інтеграцію, яка одночасно розкриває емерджентні можливості (швидкі сервіси, координація, аналітика) і мінімізує їх (через дублювання критичних вузлів, розподілені архітектури, багаторівневий кіберзахист);

3) на когнітивно-інформаційному рівень має бути можливість виявляти та інтерпретувати емерджентні ефекти, не зводячи складні системні явища до спрощених індикаторів, а навпаки – використовуючи індикатори як інструмент рефлексивного управління SoS (рис.4.2).



Рис.4.2. Концептуалізація НМС на основі принципів проектування механізмів реалізації завдань і функцій системи

Джерело: розроблено автором

Цифрова трансформація змінює саму логіку взаємодії в системі державного управління та НМС, переводить значну частину матеріальних активів, процедур та управлінських рішень у інформаційно-цифрову площину, формуючи т.з. «цифрові двійники» (Digital Twins) ключових інститутів, процесів і навіть цілих підсистем НМС (енергетики, фінансів, соціального захисту, територіальних громад). У контексті нашого дослідження це має щонайменше три критичні наслідки:

1) *сценарне моделювання стійкості*. Цифрові двійники дозволяють проводити моделювання сценаріїв для НМС як System of Systems – тестувати, як локальний збій, кібератака чи зруйнування об’єктів критичної інфраструктури вплинуть на інші підсистеми, без ризику для реальної системи, що є модулюванням ситуації, коли спостерігач може експериментувати з моделлю й коригувати власні індикатори та алгоритми;

2) екстериторіальність та безперервність державних функцій, адже завдяки інтегрованій цифровій інфраструктурі моніторингу та сервісів (National E-Resilience) держава дедалі більше функціонує як платформа, доступна громадянам, бізнесу, органам місцевого самоврядування з будь-якої точки світу. Загалом, це критично для стійкості в умовах війни, масової міграції, тимчасової втрати територій – адже «цифровий двійник» інститутів дозволяє продовжувати надання послуг, здійснювати виплати, вести реєстри незалежно від фізичного розташування органів влади;

3) автоматизація простих рішень і вивільнення когнітивного ресурсу, оскільки алгоритмізація й часткова автоматизація стандартних управлінських процедур (верифікація даних, перевірка прав, нарахування виплат, маршрутизація звернень) дає змогу перенести фокус керівників і аналітиків з операційної рутини на стратегічні завдання – архітектурний дизайн НМС як SoS, управління емерджентними ризиками, інституційний розвиток. Це означає можливість зосередити людський когнітивний ресурс на рефлексії над системою, а не тільки на її обслуговуванні.

4) інституційне навчання та адаптація в реальному часі, адже цифрові двійники дають змогу безперервно акумулювати дані про роботу НМС як System of Systems, виявляти емерджентні ризики й нові патерни поведінки системи, оновлювати порогові значення індикаторів, алгоритми реагування та регламенти взаємодії підсистем. Це перетворює НМС на комплексну адаптивну систему (Complex Adaptive System, CAS), здатну не лише підтримувати стабільність у поточних умовах, а й навчатися на кризах, коригувати власну архітектуру та політики, підвищувати стійкість із кожним

новим циклом спостереження й реагування (таблиця 4.3).

Таблиця 4.3

Трансформація характеристик системи публічного управління
в цифровому суспільстві

Характеристика системи	Аналогова модель (традиційне публічне управління)	Цифрова модель (резильєнтне публічне управління в межах НМС / National E-Resilience)
Топологія	Переважно ієрархічна, «вертикаль влади» – слабка горизонтальна взаємодія між відомствами та рівнями	Мережева, децентралізована конфігурація «системи систем» (SoS) – центральні органи, регіони, громади та сервіси взаємодіють через спільні платформи й стандарти
Потік даних	Вертикальний, дискретний, періодичні звіти «знизу вгору», затримки інформації, втрата деталізації	Горизонтальний і багаторівневий, майже безперервний потік – стріми даних з підсистем у інтегровану цифрову інфраструктуру моніторингу НМС; доступність узгоджених даних для різних акторів у режимі «майже реального часу»
Реакція на помилку / збій	Логіка fail-safe – зупинка системи або процесу для уникнення шкоди; довгі паузи на ручне «розслідування» й перезапуск	Логіка fail-operational / safe-to-fail, коли система продовжує працювати зі зниженою функціональністю, використовуючи резервні канали, дублюючі сервіси, альтернативні сценарії; каскадні ризики моделюються заздалегідь
Природа довіри	Переважно інституційна – печатка, «мокрый» підпис, фізична присутність, персональні контакти; довіра до формального статусу інституції	Алгоритмічно підсилена й прозора – криптографія, електронний підпис, блокчейн/журнали аудиту, публічні реєстри рішень; довіра базується на перевірності даних, відстежуваності дій і пояснюваній аналітиці
Локалізація функцій та даних	Жорстка прив'язка до фізичної адреси органу влади, «кабінетна» модель; критичні дані зберігаються локально (серверні кімнати в установах)	Хмарна та розподілена архітектура – державні «хмари», географічне рознесення й резервування реєстрів, екстериторіальність доступу до послуг; «цифрові двійники» інституцій і процесів, стійкі до фізичних загроз
Спостереження й оцінювання (дослідницький контур)	Спостерігач як зовнішній суб'єкт; акцент на фіксованих індикаторах, звітності «постфактум»	Спостерігач-суб'єкт (держава, регіони, аналітики) є частиною системи; індикатори стійкості, моделі DRA та алгоритми моніторингу регулярно переглядаються з урахуванням їх впливу на поведінку суб'єктів

Джерело: дослідження автора

Як видно з таблиці 4.4., у межах НМС / National E-Resilience потоки даних набувають горизонтального, багаторівневого та майже безперервного

характеру: 1) дані з різних підсистем (енергетика, фінанси, соціальний захист, регіони) надходять у інтегровану цифрову інфраструктуру моніторингу в режимі близькому до реального часу; завдяки єдиним стандартам інтероперабельності та «Трембіті» дані циркулюють як між рівнями, так і між секторами; регіони та громади отримують доступ до спільної інформаційної картини, а не лише до «своєї» локальної статистики.

При цьому очевидно, потік даних дозволяє не лише спостерігати систему, а й спостерігати за самим процесом спостереження (мета-моніторинг) – як змінюються індикатори, які патерни є типовими, де видно перекоси, спричинені прагненням «покращити показник» (ефект Гудхарта). Наслідки для стійкості полягають у тому, що є можливість раннього виявлення кризових тенденцій, оперативного реагування, формування дійсно смарт-резильєнтних регіональних стратегій на основі актуальних даних. Ризиком виступає перенавантаження даними без адекватних когнітивно-інформаційних механізмів (аналітики, інтерпретації, візуалізації) може призвести до «паралічу аналізу» й хаотичних рішень.

Вважаємо, що раціональний алгоритм моніторингу функціонування НМС має розглядатися як цілісний управлінсько-аналітичний контур для «системи систем», що забезпечує комплексну оцінку безпекових, соціально-економічних, інформаційних та управлінських параметрів. Його формування спирається на архітектурне бачення НМС як System of Systems, застосування кібернетики другого порядку та інтегрованої цифрової інфраструктури моніторингу (National E-Resilience), при цьому моніторинг не зводиться до збирання звітності, а виступає механізмом рефлексивного управління, здатним виявляти як емерджентні можливості, так і емерджентні вразливості, що виникають на перетині різних підсистем.

У межах дослідження використовуються реальні дані для показу роботи алгоритму. Наприклад, у 2022–2025 рр. Україна пережила тисячі епізодів ракетних та дронівих ударів по об'єктах критичної інфраструктури; за оцінками, у пікові періоди до 35–40 % енергетичних потужностей

знамали пошкоджень або вимушених відключень. Паралельно, за відкритими даними, кількість зареєстрованих кібератак зросла в 5–6 разів порівняно з довоєнним періодом, й при цьому понад 18–20 млн громадян активно користуються цифровими публічними сервісами. Ці параметри створюють емпіричне тло, на якому тестується запропонована логіка моніторингу.

Наведений алгоритм включає послідовність взаємопов'язаних етапів розвитку НМС, кожен з яких відображає певний вимір стійкості та водночас готує підґрунтя для наступного. *Першим етапом* є діагностика загроз і викликів, що охоплює збройні дії, суспільну дестабілізацію, інформаційну війну, руйнування критичної інфраструктури, фінансові шоки, міграційні кризи та інші типи деструктивних впливів на НМС як систему систем. У практичному вимірі це означає створення карти ризиків, що базується на сукупності показників: кількості атак на об'єкти критичної інфраструктури (наприклад, понад 1000 за рік по енергетичному сектору в умовах повномасштабної війни), частоті масованих кібератак (умовно 200–300 значущих інцидентів на рік за даними профільних CERT-структур), динаміці протестної активності, хвилях внутрішньої та зовнішньої міграції (понад ~ 5 млн осіб, які тимчасово виїхали за кордон), масштабу руйнувань житла та соціальної інфраструктури в окремих регіонах (до 30–60 % об'єктів у прифронтових територіях). На основі таких емпіричних масивів формується карта найбільш уразливих підсистем і територій.

Другий етап – збір та аналіз даних, забезпечує емпіричне наповнення цієї карти ризиків. Тут принципово важливо, що дані надходять не лише з державних органів, а й із громадянського суспільства, засобів масової інформації, міжнародних партнерів, бізнесу та відкритих джерел. За орієнтовними оцінками, інтегрована цифрова інфраструктура може поєднувати дані щонайменше від 40-50 центральних органів виконавчої влади, сотень територіальних громад та понад 200-300 державних реєстрів і інформаційних систем, генеруючи десятки мільйонів транзакцій на добу.

Інструменти обробки великих даних дозволяють автоматично виявляти аномалії (наприклад, різкі стрибки кількості звернень по гуманітарну допомогу в конкретному регіоні, 20–30 % падіння обсягів безготівкових операцій у певному секторі економіки, зростання кількості фейкових повідомлень у соціальних мережах на 50–70 % протягом короткого періоду). Важливо, що інтегрована платформа моніторингу виступає не як сукупність розрізнених «дашбордів», а як узгоджене середовище збору, верифікації та крос-перевірки даних з різних джерел.

Третім етапом є визначення критичних індикаторів стійкості, які дозволяють перетворити масив даних на керовану систему сигналів. Йдеться про такі ключові параметри, як спроможність оборонного сектору (наприклад, частка угруповань сил, забезпечених безперебійним зв'язком і логістикою на рівні не менше 80–90 %), стан та відновлюваність критичної інфраструктури (середній час відновлення енергопостачання після масованих атак – умовно скорочений із 72 годин у листопаді 2022 р. до 24–36 годин у середині 2023 р., 12–24 годин у 2025 р.), рівень соціальної довіри (за результатами опитувань – 55–65 % громадян, які заявляють про довіру до електронних сервісів держави), доступ населення до базових послуг (не менше 85–90 % домогосподарств мають можливість отримати ключові послуги онлайн навіть під час криз), стійкість до дезінформації (зменшення частки населення, яке піддається основним ворожим наративам, наприклад, з 30 % до 20 % у визначених цільових групах), управлінська спроможність (скорочення середнього часу ухвалення міжвідомчих рішень з тижнів до 24–48 годин у кризових ситуаціях) (результати експертного опитування на замовлення ГО ГНО «Фундація публічно-правових ініціатив», додаток Д).

У термінах авторської моделі Digital Resilience Assessment (DRA) на цьому етапі поєднуються кількісні показники (відсотки, години, кількість інцидентів, охоплення населення) та якісні оцінки (експертні опитування, результати аудитів, глибинні інтерв'ю). Водночас, з урахуванням ефекту Гудхарта, система індикаторів проєктується як адаптивна, тобто алгоритм

моніторингу передбачає регулярний (наприклад, щорічний) перегляд переліку показників, їх ваг та порогових значень на основі аналізу того, як зміна метрик впливає на реальну поведінку органів влади, секторів і регіонів.

Четвертий етап – оцінка ефективності реагування – переводить моніторинг із площини «діагностики стану» в площину «оцінювання дій». На цьому етапі застосовується автоматизований та експертний аналіз дій національних інститутів, секторів та регіонів щодо їх відповідності виявленим потребам і загрозам. Наприклад, у випадку масованих ударів по енергетичній інфраструктурі алгоритм може фіксувати, що в перші місяці кризи частка домогосподарств, які залишалися без електроенергії понад 24 години, становила 25–30 %, тоді як через півроку реалізації заходів з підсилення резервних потужностей і перепроєктування мереж ця частка зменшилась до 10–12 %. Аналогічно, під час запуску програм підтримки бізнесу та населення (на кшталт «Підтримки» чи цільових компенсацій) можна оцінювати, який відсоток цільової аудиторії отримав допомогу впродовж перших 72 годин (наприклад, зростання з 40–50 % під час перших хвиль до 70–80 % у наступних), наскільки зменшилась кількість домогосподарств, що опинилися за межею бідності внаслідок кризи, чи вдалося втримати рівень безробіття у визначеному сценарному коридорі (наприклад, не вище 15–17 % навіть за песимістичними сценаріями). Фактично йдеться про метарівень спостереження: система не лише фіксує, «що відбувається», а й аналізує, «Як ми на це реагуємо» та «Чи не погіршує реакція загальний стан НМС».

П'ятим етапом є розробка рекомендацій і коригування стратегій на основі сценарного прогнозування. Тут запропонований алгоритм виходить за межі ретроспективного аналізу та переходить до проактивного моделювання можливих траєкторій розвитку ситуації. На основі поєднання даних, індикаторів і результатів оцінки реагування формуються сценарії «що, якщо», які відображають, як НМС як система систем поводитиметься за різних конфігурацій шоків та управлінських рішень. Аналогічно, у соціально-

економічному вимірі можна моделювати вплив різних схем підтримки (цільові субсидії, податкові канікули, грантові програми) на збереження робочих місць та підприємств (наприклад, утримання 70–80 % малих і середніх підприємств від закриття в найбільш уразливих секторах). Такі сценарії дозволяють не лише обрати найефективніші комбінації політик, а й аргументувати необхідність перерозподілу ресурсів між секторами й регіонами. У таблиці 4.4 відображено зміст ключових етапів алгоритму моніторингу, їхній зв'язок із основними вимірами стійкості та орієнтовні (екстрапольовані) кількісні параметри.

Таблиця 4.4

Аналіз етапів алгоритму моніторингу, зв'язок із основними вимірами
стійкості

Аспект	Запропонований алгоритм (DRA, інтегрований, резильєнтний)	Альтернативний варіант (традиційний, секторально-звітний)	Висновки та рекомендації щодо переходу
Базова логіка	Моніторинг НМС як системи систем із акцентом на взаємозв'язках між безпековими, соціально-економічними, інформаційними та управлінськими вимірами	Моніторинг окремих секторів (оборона, економіка, соц.сфера тощо) з мінімальним аналізом міжсекторальних взаємодій	Потрібно перейти від секторального до системно-архітектурного мислення, формалізувати карту «системи систем» НМС, проєктувати моніторинговий контур
Мета	Підтримка адаптивного управління стійкістю, раннє виявлення ризиків, тестування сценаріїв і коригування стратегій	Формальне інформування про стан окремих сфер, підготовка звітності та обґрунтування вже прийнятих рішень	Необхідно інституціонально закріпити основну мету моніторингу – управління стійкістю, а не лише звітність; це варто відобразити в стратегіях, регламентах і KPI
Структура етапів	5 етапів: діагностика загроз → збір та аналіз даних → визначення критичних індикаторів → оцінка ефективності реагування → сценарне прогнозування та корекція стратегій	3 умовні етапи: збір показників → складання звітів → підготовка загальних висновків без формалізованого сценарного аналізу	Рекомендовано поетапно доповнити чинні процеси двома «відсутніми» ланками: (1) формалізована оцінка реагування; (2) сценарне моделювання і прив'язка до корекції стратегій
Охоплення вимірів стійкості	Комплексне: безпекові, соціально-економічні, інформаційні, управлінські параметри в єдиній рамці	Переважно секторальне: кожен орган збирає «свої» показники, інтегральна картина формується ситуативно й постфактум	Варто розробити національну «матрицю стійкості», де для кожного сектору визначені зв'язки з іншими вимірами (безпека ↔ економіка ↔ соцсфера ↔ інформація ↔ управління)
Інтеграція даних	Єдина/інтегрована цифрова платформа моніторингу; дані від ЦОВВ, регіонів, громадянського суспільства, ЗМІ, міжнародних партнерів, відкритих джерел	Розрізнені бази даних та звіти від різних органів; обмежений обмін інформацією, часто у форматі документів (PDF, листи, презентації)	Кроки переходу: (1) уніфікація форматів даних; (2) побудова шини/платформи обміну; (3) поетапне підключення реєстрів і систем до єдиного моніторингового контуру.

Продовження таблиці 4.4

Частота та режим оновлення	Стрімові потоки та у потоки квазіреального часу + регулярні періодичні оновлення	Переважаю періодична звітність (квартал, рік); несистемний збір оперативних даних у кризах	Рекомендовано виділити перелік показників, які критично потребують майже реального часу (інциденти безпеки, навантаження на КІ, ключові соц.показники)
Індикатори стійкості	Комбінація кількісних і якісних показників (robustness, redundancy, resourcefulness, rapidity); адаптивний перегляд переліку й ваг	Фіксований перелік показників, орієнтований на виконання планів/бюджетів; рідкісний перегляд; ризик «гри з показниками»	Потрібно створити механізм регулярного аудиту індикаторів (1 раз на рік/цикл стратегії) і формалізувати процедуру зміни набору показників та їх ваг на основі емпіричних результатів
Оцінка реагування	Системна: автоматизований аналіз дій інститутів, вимір ефективності й своєчасності реагування, виявлення каскадних ефектів	Обмежена: «розбір польотів» після кризи; відсутні стандартизовані метрики ефективності реагування	Рекомендовано ввести стандартизований набір показників ефективності реагування (час, повнота охоплення)
Сценарне прогнозування	Обов'язковий етап: моделювання сценаріїв «що, якщо», оцінка впливу різних політик на ВВП, зайнятість, бідність, стан КІ, інформаційну безпеку	Слабо розвинене або відсутнє; домінує екстраполяція трендів та якісні експертні оцінки	Варто створити сценарний модуль при платформі моніторингу (на основі системної динаміки) сценарний аналіз до процедур підготовки рішень
Роль регіонів та громад	Регіони – співтворці моніторингу: смарт-резильєнтні регіональні профілі, урахування територіальної специфіки загроз і ресурсів	Регіони переважно надають звіти «догори»; участь у формуванні індикаторів та інтерпретації результатів обмежена	Рекомендується створити регіональні аналітичні лабораторії стійкості, надати їм доступ до даних, права впливати на конфігурацію індикаторів і сценаріїв
Кібернетичний рівень (1-й / 2-й порядок)	Кібернетика другого порядку: моніторяться не лише показники, а й самі моделі, індикатори та управлінські реакції; передбачено перегляд алгоритму моніторингу	Кібернетика першого порядку: система вважається об'єктом спостереження ззовні; набір індикаторів і методик сприймається як «даний»	Слід інституційно закріпити процедури «моніторингу моніторингу»: зовнішній та внутрішній аудит методик, відкритість частини моделей, участь експертного середовища у їх перегляді
Вбудованість в управлінський цикл	Результати моніторингу напряму пов'язані з корекцією стратегій, бюджетним плануванням, пріоритизацією інвестицій у стійкість	Результати часто відокремлені від реальних рішень; звітність виконує переважно формальну функцію	Потрібно нормативно прив'язати ключові рішення (стратегії, бюджети, програми) до показників DRA: без аналізу даних і сценаріїв рішення не можуть вважатися повноцінно обґрунтованими.
Використання емпірики й великих даних	Активне: агрегуються мільйони транзакцій, інцидентів, записів журналів; застосовуються методи виявлення аномалій, порогові значення й кількісні сценарії	Обмежене: домінують агреговані статистичні таблиці, вибіркові соціологічні дослідження й ручна обробка даних	Рекомендовано розвивати державну аналітичну інфраструктуру (data lakes, ETL-процеси, аналітичні сервіси) та інвестувати в компетенції data science у публічному секторі
Здатність до адаптації та навчання	Висока: алгоритм передбачає постійне вдосконалення індикаторів, джерел даних, методик аналізу та сценарних моделей	Низька/середня: зміни у системі моніторингу відбуваються повільно, переважно під тиском зовнішніх вимог або після масштабних збоїв	Потрібно закласти в регламенти циклічну логіку «криза/епізод → аналіз → оновлення архітектури й індикаторів»,

Джерело: розроблено автором

У своїй сукупності наведені етапи і складники формують раціональний алгоритм моніторингу, який інтегрує системно-архітектурний, індикативно-аналітичний, інфраструктурно-технологічний, когнітивно-інформаційний, рефлексивно-кібернетичний, територіально-регіональний та інституційно-нормативний напрями, обґрунтовані в дослідженні. Діагностика загроз забезпечує системне розуміння контексту; збір і аналіз даних – емпіричну базу; визначення критичних індикаторів – перехід до керованої системи сигналів; оцінка ефективності реагування – зворотний зв'язок щодо дій; сценарне прогнозування та розробка рекомендацій – перетворення моніторингу на інструмент адаптивного управління. Включення емпіричних даних дозволяє не лише концептуалізувати НМС, а й перевіряти практичну дієвість алгоритму у різних кризових ситуаціях, порівнювати фактичні показники з цільовими, уточнювати порогові значення та періодично оновлювати систему індикаторів. Така логіка моніторингу узгоджується з авторською моделлю Digital Resilience Assessment та розкриває її прикладний вимір, оскільки дає змогу не лише оцінювати поточний рівень стійкості, а й безперервно коригувати стратегії, політики й архітектуру НМС відповідно до змін середовища й внутрішньої динаміки системи.

Функціонування алгоритму динамічного моніторингу національної моделі стійкості в умовах війни нерозривно пов'язане з техніко-технологічними механізмами, які забезпечують «архітектуру виживання» державного ІТ-ландшафту. Адже за наявності постійних кінетичних та кібернетичних загроз критично важливим є не просто періодичне оцінювання окремих секторів, а єдиний системний підхід до динамічного моніторингу, здатний своєчасно виявляти вразливості, оцінювати ефективність реагування та забезпечувати адаптацію інституцій до змін середовища. Запропонований у дослідженні алгоритм такого моніторингу включає послідовність взаємопов'язаних етапів: діагностику загроз і викликів (збройні дії, суспільна дестабілізація, інформаційна війна, руйнування інфраструктури), збір та аналіз даних (із використанням інструментів обробки великих даних та

інтеграції інформації з державних органів, громадянського суспільства, ЗМІ й міжнародних партнерів), визначення критичних індикаторів стійкості (спроможність оборонного сектору, рівень соціальної довіри, доступ до критичної інфраструктури, стан інформаційної безпеки), оцінку ефективності реагування (автоматизований аналіз дій національних інститутів щодо їх відповідності виявленим потребам і загрозам) та розробку рекомендацій і коригування стратегій на основі сценарного прогнозування. Така поетапна логіка повністю узгоджується з авторською моделлю Digital Resilience Assessment і розкриває її прикладний вимір, оскільки переводить DRA з рівня концептуальної рамки в режим постійно діючого управлінського контуру.

У цьому контексті техніко-технологічні механізми постають не як другорядний інженерний супровід, а як базова умова реалізації зазначеного алгоритму. Проєктування ІТ-ландшафту держави має виходити з презумпції, що будь-який окремий вузол може бути фізично знищений або скомпрометований, а отже, система моніторингу та оцінювання стійкості має бути здатною продовжувати функціонувати навіть за часткового руйнування інфраструктури. Це вимагає впровадження архітектурних патернів хмарних обчислень, мультихмарних рішень та механізмів екстериторіального зберігання даних, які гарантують живучість ключових інформаційних ресурсів і безперервність роботи алгоритму.

Традиційна модель, за якої критичні дані й сервіси розміщуються у фізичних дата-центрах на території держави, є надто вразливою до ракетних ударів, диверсій, тривалого відключення енергопостачання чи окупації. Тому до архітектури динамічного моніторингу інтегрується мультихмарна стратегія: критичні реєстри (демографічний, майновий, податковий, реєстр об'єктів критичної інфраструктури, реєстри соціальних виплат) шифруються, фрагментуються (sharding), а їхні частини розподіляються між кількома незалежними хмарними провайдерами й дата-центрами в різних юрисдикціях. Такий підхід, спираючись на концепцію «цифрових посольств» (Data Embassies), реалізовану, зокрема, Естонією й актуалізовану Україною,

забезпечує екстериторіальність даних, а отже – здатність алгоритму моніторингу та модулів DRA відновлювати доступ до інформації й продовжувати роботу навіть у разі втрати значної частини національної інфраструктури. Відповідне законодавче закріплення можливості зберігання окремих категорій державної інформації та персональних даних у хмарах довірених партнерів трансформує хмарну стратегію з технічного експерименту на норму функціонування НМС.

Водночас, сама лише фізична чи географічна живучість інфраструктури не гарантує надійності даних для DRA. Умови війни та гібридних загроз роблять неефективною класичну модель оборони периметра, коли «внутрішня» мережа вважається безпечною, а «зовнішня» – ворожою. Масовий віддалений доступ, розміщення сервісів у хмарі, розгалужені мережі підрядників і партнерів створюють ситуацію, коли будь-яка точка входу може бути використана для проникнення до критичних систем моніторингу. Саме тому техніко-технологічний фундамент алгоритму динамічного моніторингу НМС повинен спиратися на архітектуру нульової довіри (Zero Trust Architecture), яка повністю відмовляється від презумпції безпечної внутрішньої зони [342].

Архітектура нульової довіри у межах дисертації передбачає, що кожен запит на доступ до будь-якого ресурсу – бази даних, API моніторингової платформи, аналітичної панелі DRA, підсистеми сенсорних мереж, об'єкта критичної інфраструктури чи навіть службової камери спостереження – повинен щоразу проходити автентифікацію та авторизацію, незалежно від того, надходить він з внутрішньої мережі міністерства чи з публічного інтернету. Доступ надається за принципом мінімально необхідних привілеїв, з урахуванням контексту (місце, час, тип пристрою, історія поведінки користувача або сервісу), а всі дії системно узагальнюються й аналізуються на предмет аномалій. У такій конфігурації внутрішній користувач не має «довіри за замовчуванням», а отже, класична інсайдерська загроза втрачає статус окремої, привілейованої категорії ризику: будь-який доступ,

внутрішній чи зовнішній, має бути обґрунтований і підтверджений. Інтеграція Zero Trust у контур динамічного моніторингу й DRA дає змогу істотно підвищити достовірність і цілісність даних, на яких базується оцінка стійкості.

У контексті архітектури виживання та алгоритму динамічного моніторингу національної моделі стійкості ключовим є усвідомлення, що технології лише інструмент, тоді як справжнім суб'єктом стійкості виступає суспільство. Навіть найбільш захищена хмарна інфраструктура й досконала Zero Trust-архітектура втрачають ефективність, якщо «людський шар» залишається вразливим. Емпіричні оцінки показують, що значна частина користувачів продовжує потрапляти на фішингові атаки (за різними міжнародними дослідженнями, рівень кліків на шкідливі посилання у фішингових розсилках часто сягає 10–20 %), а від 30 до 40 % громадян у окремих вибірках не можуть упевнено відрізнити достовірну новину від маніпулятивної або відверто фейкової. В умовах, коли понад 70–80 % населення щоденно користуються соціальними мережами й месенджерами, кожен такий користувач стає потенційною «діркою» в системі безпеки держави – як у кібернетичному, так і в інформаційно-когнітивному вимірі.

Тому цифрова освіта й стратегічні комунікації мають розглядатися не як супровідні, а як структурні елементи алгоритму динамічного моніторингу та моделі Digital Resilience Assessment. Масштабні програми цифрової грамотності й цифрової гігієни, які охоплюють мільйони громадян (наприклад, 3–5 млн користувачів на рік через онлайн-курси, інтерактивні платформи, шкільні та університетські модулі), безпосередньо знижують імовірність успішних фішингових атак, компрометації облікових записів та поширення дезінформації. Паралельно, використання алгоритмів аналізу настроїв та виявлення аномалій у соціальних мережах (обробка сотень тисяч або мільйонів постів і коментарів щодоби) дозволяє фіксувати інформаційні атаки на ранніх стадіях, коли хвиля ворожих наративів лише формується, а не коли вона вже охопила мільйони користувачів. Поєднання таких

аналітичних інструментів з автоматизованим поширенням спростувань через офіційні й довірені канали (державні платформи, верифіковані медіа, лідери думок) перетворює когнітивний простір із зони пасивної вразливості на активний фронт стійкості. Таким чином, інтеграція цифрової освіти й стратегічних комунікацій у алгоритм моніторингу та DRA дозволяє не лише реєструвати інформаційні ризики, а й системно зменшувати їх, роблячи суспільство не об'єктом, а повноцінним суб'єктом національної стійкості.

4.3. Модель «смарт-резильєнтних регіональних стратегій» як інноваційний інструмент просторової диференціації національної моделі стійкості

Розбудова національної моделі стійкості в умовах протидії збройній агресії неможлива як суто «централізований» проєкт. Загрози, ресурси та інституціональна спроможність суттєво відрізняються між прикордонними, прифронтовими, припортовими, аграрними, індустріальними регіонами. Відповідно, у межах єдиного національного формату стійкості виникає потреба у просторовій диференціації – такому налаштуванні політик, інструментів і пріоритетів, яке враховує специфіку кожної території, але не підриває цілісності державної системи.

У цьому контексті пропонується модель «смарт-резильєнтних регіональних стратегій» як інноваційний інструмент просторової диференціації Національної моделі стійкості (НМС), інтегрований у загальний контур Digital Resilience Assessment (DRA) та алгоритм динамічного моніторингу. Модель «смарт-резильєнтних регіональних стратегій» (СРРС) пропонується як інноваційний інструмент просторової диференціації національної моделі стійкості, що безпосередньо впливає з еволюції парадигми державного управління в Україні в умовах війни.

Модель «смарт-резильєнтних регіональних стратегій» (СРРС) пропонується не просто як оновлений формат регіонального планування, а як

якісно новий, інноваційний інструмент просторової диференціації національної моделі стійкості, що безпосередньо впливає з еволюції парадигми державного управління в Україні в умовах війни. Повномасштабне вторгнення, масштабні руйнування інфраструктури, масова внутрішня та зовнішня міграція, глибокі трансформації економіки та постійний інформаційно-психологічний тиск оголили обмеженість традиційних бюрократичних та надмірно централізованих моделей управління. Жорсткі ієрархії, побудовані на суворій вертикалі прийняття рішень, виявилися нездатними достатньо швидко й гнучко реагувати на асиметричні загрози, що в різних регіонах набували різних форм – від безпосередніх бойових дій до перевантаження соціальної інфраструктури чи збоїв логістичних ланцюгів. У цих умовах закономірним став перехід до нового управлінського мислення, яке дедалі більше орієнтується на принципи мережовості, партнерства, співтворення політик та опори на локальні ініціативи.

Якщо реформи попередніх років спиралися переважно на логіку New Public Management з її фокусом на менеджеристві, раціоналізації витрат, запровадженні формалізованих KPI та централізованому проєктуванні змін, то протидія збройній агресії проти України продемонструвала потребу у переорієнтації до парадигми New Public Governance. У межах цієї нової логіки держава розглядається не стільки як монополіст у виробництві публічних послуг, скільки як координатор і модератор складної мережі суб'єктів, що спільно забезпечують стійкість. До цієї мережі входять органи місцевого самоврядування й військові адміністрації, волонтерські спільноти та громадські організації, бізнес-кластери, освітні й наукові інституції, міжнародні партнери та донори. Стихійний розвиток горизонтальних кооперацій під час перших місяців повномасштабної війни – від волонтерських логістичних центрів і ініціатив з евакуації до MilTech-розробок і самоорганізації громад – згодом дедалі частіше знаходив своє продовження в інституціоналізованих державних формах, таких як кластер

Brave1 чи окремі державні програми підтримки релокації бізнесу. Саме на перетині цих процесів формується запит на такі моделі, як СРРС, здатні поєднати мережеве управління, цифрові інструменти та просторову специфіку стійкості.

У цьому контексті *сма́рт-резильє́нтна регіона́льна стра́тегія* є гібридною конструкцією, яка інтегрує принципи «розумного» територіального розвитку та резильєнтності. «Смарт» у цій моделі означає не лише використання цифрових технологій, сенсорних мереж, геоінформаційних систем чи аналітики великих даних, а й запровадження механізмів прийняття рішень на основі даних у реальному або наближеному до реального часу. «Резильєнтність» же передбачає здатність території не лише протистояти шокам, а й адаптуватися до них, зберігаючи ключові функції, та у разі необхідності трансформувати свою економічну, соціальну й інституційну структуру. У поєднанні ці два виміри формують таку модель регіональної стратегії, у якій планування ґрунтується не на статичних уявленнях про розвиток, а на постійному моніторингу ризиків, вразливостей, ресурсів та можливостей.

Інноваційність СРРС полягає також у тому, що вона стає механізмом уніфікації загальнонаціональної моделі стійкості для конкретних територій. Регіони України в умовах воєнного стану опинилися у принципово різних умовах. Для прифронтових і близьких до зони бойових дій територій першочерговим стає забезпечення фізичної безпеки населення, працездатності критичної інфраструктури, автономності енергопостачання, надійності систем оповіщення, оперативності роботи служб реагування. Для тилкових регіонів, що відіграють роль гуманітарних, логістичних і економічних хабів, у фокусі опиняються прийом і інтеграція внутрішньо переміщених осіб, релокація виробництв, розширення потужностей соціальних та медичних послуг, підтримка зайнятості та відновлення ланцюгів доданої вартості. Транскордонні області, через які проходять ключові експортно-імпортні та гуманітарні коридори, змушені акцентувати

увагу на пропускній спроможності інфраструктури, інтеграції з логістичними мережами сусідніх країн, спрощенні митних процедур та космополітичних сервісах для бізнесу і громадян. Одна й та сама національна мета – зміцнення стійкості – у різних просторових контекстах вимагає різних конфігурацій інструментів, інвестицій і управлінських рішень; саме цю задачу виконує СРРС, виступаючи інструментом просторової диференціації.

Ще одна важлива риса моделі полягає в її відповідності принципам співтворення політик. Смарт-резильєнтні стратегії не можуть бути розроблені виключно в стінах центрального органу виконавчої влади чи навіть обласної адміністрації; їхнє змістовне наповнення формується через залучення до процесу планування ключових локальних стейкхолдерів. Органи місцевого самоврядування при цьому не просто «отримують завдання» зверху, а стають повноцінними партнерами, що артикулюють власне бачення загроз і можливостей. Волонтерські та громадські ініціативи надають знання «з поля» про реальну спроможність громад до самоорганізації, наявні локальні мережі солідарності, слабкі й сильні ланки в системах допомоги. Бізнесові кластери та асоціації, зокрема у сферах логістики, агропромислового виробництва, ІТ чи MilTech, пропонують не лише ресурси, а й функціональні рішення, здатні посилити як локальну, так і загальнонаціональну резильєнтність. Міжнародні партнери, своєю чергою, привносять досвід інших країн, фінансову підтримку, доступ до цифрових рішень та експертизи. СРРС, інтегруючи цю множинність голосів у єдиний стратегічний документ, виступає водночас і інструментом координації, і простором для узгодження інтересів.

На відміну від уніфікованої регіональної політики («один формат для всіх»), Україна впроваджує модель функціонального зонування, закріплену законодавчо. Це дозволяє застосовувати різні набори інструментів для різних типів громад (таблиця 4.5).

Таблиця 4.5

Типологія територій та інструменти впливу

Функціональний тип (ФТТ)	Характеристика та критерії	СРРС	Ключові проекти / Інструменти
Території відновлення (Recovery Territories)	Громади з бойовими діями, окупацією, руйнуваннями, втратою >10% населення	Безпека та виживання: Розмінування, відновлення критичних сервісів, модульне житло	Програми «Відновлення, гуманітарне розмінування (дрони, AI), DREAM для донорів
Регіональні полюси зростання (Growth Poles)	Тилові агломерації (Львів, Ужгород, Вінниця) з притоком бізнесу та людей	Масштабування та Інновації: Розвиток індустріальних парків, експорт, інтеграція ВПО	Індустріальні парки, кластери S3, розвиток транспортних хабів
Території з особливими умовами	Прикордонні зони, території з низькою щільністю населення	Цифрова доступність: Забезпечення доступу до послуг через цифрові канали, безпекові дотації	Цифровізація ЦНАПів, мобільні аптеки, Starlink, «розумне село»
Території сталого розвитку	Громади зі збалансованим потенціалом	Зелена трансформація: Енергоефективність, екологічні проекти	Гранти на енергомодернізацію, підтримка МСБ

Регіони трансформують економіку відповідно до своїх унікальних переваг (Strategy for Smart Specialisation), що підтверджується дослідженнями UNDP та кластерним аналізом. 1) Агро-фуд та біотехнології (Вінниця, Черкаси) – перехід від експорту сировини до глибокої переробки («Food-Health-Materials»), використання відходів агросектору для біоенергетики; 2) MilTech та DefenseTech (Київ, Львів, Дніпро) – вимушена спеціалізація. Понад 300 компаній у Дія.City працюють на оборону, й у 2024 році топ-3 DefenseTech компанії згенерували понад 17 млрд грн доходу; 3) логістика та «Блакитна економіка» (Одеса, Миколаїв) – розвиток дунайських портів, мультимодальних терміналів та відновлення суднобудування (морські дрони) [343]. Цифровий вимір моделі дозволяє перетворити регіональну стратегію на живий, постійно оновлюваний документ, а не на формальний план на кілька років. Завдяки використанню систем моніторингу, геоінформаційних платформ, інструментів аналізу соціально-економічних показників, реєстрів об'єктів критичної інфраструктури, даних про переміщення населення та економічну активність, регіон отримує змогу моделювати різні сценарії розвитку подій та оперативно коригувати свої пріоритети. Це робить СРРС

сумісною з більш широкими рамками цифрової оцінки стійкості (Digital Resilience Assessment), в якій регіональні дані стають «вхідними параметрами» для загальнонаціональних моделей. Водночас національний рівень повертає регіонам результати сценарного аналізу та порівняльні оцінки, що дозволяє їм вчитися один у одного, запозичувати успішні рішення та адаптувати їх до власного контексту.

Таким чином, модель СРРС можна розглядати як механізм просторового впровадження нової, мережево орієнтованої та резильєнтної моделі державного управління, яка сформувалася під тиском війни. Вона трансформує національну модель стійкості з абстрактної загальнодержавної конструкції в систему конкретних, диференційованих, але взаємопов'язаних регіональних стратегій, що відображають різноманіття загроз, ресурсів, інституційної спроможності та локальних ініціатив. У результаті посилюється не лише здатність окремих територій протистояти шокам і відновлюватися, а й цілісна резильєнтність держави як системи систем, у якій регіони виступають не пасивними реципієнтами політик, а активними суб'єктами їхнього творення й реалізації.

Масштаб руйнувань, асиметричний характер загроз, надвисока динаміка гуманітарних, економічних та безпекових викликів в умовах збройної агресії проти України каталізували кризу традиційних бюрократичних моделей, побудованих на жорсткій ієрархії, централізованому прийнятті рішень і стандартизованих процедурах. Практика воєнного часу показала, що такі моделі не здатні достатньо швидко і гнучко реагувати на зміну лінії фронту, хвилі внутрішньої та зовнішньої міграції, каскадні аварії інфраструктури та інформаційні атаки. Відповідно, формується нова управлінська логіка, яка відходить від класичного New Public Management із його акцентом на менеджеризм, скорочення витрат і формалізовані KPI, і тяжіє до парадигми New Public Governance (NPG), у якій домінують мережеві взаємодії, співтворення політик і багаторівнева координація.

У межах NPG держава перестає бути єдиним і центральним виробником публічних благ і перетворюється на модератора складної мережі суб'єктів, до якої входять органи місцевого самоврядування, військові адміністрації, волонтерські спільноти, міжнародні донори, бізнес-об'єднання, наукові та експертні інституції. Саме в такій мережевій конфігурації стає можливим формування смарт-резильєнтних регіональних стратегій як інструменту, що поєднує технологічні рішення, локальне знання та горизонтальну самоорганізацію. Ключовим принципом виступає співтворення (co-production) – політика стійкості більше не формується виключно «згори-вниз» через нормативні акти й централізовані програми, а народжується на перетині локальних ініціатив, волонтерських практик, кластерних бізнес-об'єднань і державних рамкових рішень. Показовим є приклад трансформації спонтанних MilTech-ініціатив та волонтерських розробок у сфері безпеки й оборони в інституціоналізовані кластери на кшталт Brave1, коли держава не знижує горизонтальну активність, а навпаки – інтегрує її в стратегічну рамку.

У такому контексті СРРС постає як гібридна конструкція, що поєднує просторову специфіку загроз і ресурсів конкретної території з можливостями цифрових технологій, аналітики даних і мережевого управління. Йдеться про перехід від уніфікованого підходу («одна національна політика стійкості для всіх») до просторово диференційованої моделі, у якій кожен регіон (область, агломерація, кластер громад) вибудовує власний профіль резильєнтності відповідно до функціональної ролі в загальнонаціональній системі. Прифронтові території можуть фокусуватися на мінімізації втрат, укріпленні критичної інфраструктури, розвитку розподіленої енергетики та систем оповіщення; тиллові регіони – на прийомі внутрішньо переміщених осіб, релокації бізнесу, розбудові логістичних та медичних хабів; транскордонні області – на забезпеченні стійких каналів експорту, імпорту та гуманітарної допомоги. Таким чином, просторову диференціацію національної моделі стійкості забезпечує не лише різний набір проєктів, а й різна архітектура

взаємодій між акторами у кожному типі регіону.

Поняття «смарт-резильєнтності» виходить за межі фізичної відбудови (bouncing back). Це здатність системи використовувати цифрові технології та дані для передбачення загроз і здійснення трансформаційного стрибка розвитку (bouncing forward). Стійкість досягається не товщиною стін, а інтелектуалізацією інфраструктури (Smart Grids), інтеграцією сенсорних мереж, цифрових двійників територій та гнучкістю прийняття рішень на основі Big Data. У такому вимірі відбудова розуміється не як повернення до «довоєнної норми», а як конструювання нової, якісно вищої норми, де критична інфраструктура, соціальні сервіси, міський простір і система управління одразу проєктуються з урахуванням високої турбулентності середовища. Наприклад, замість відновлення лінійної енергетичної мережі, вразливої до кількох точкових ударів, впроваджується мережа з розподіленою генерацією, локальними накопичувачами та інтелектуальним балансуванням навантажень, що не лише підвищує її живучість, а й створює можливості для енергетичної демократії, «зелених» інвестицій і нових бізнес-моделей.

Ключовим елементом смарт-резильєнтності є перехід від реактивної до проактивної та предиктивної логіки управління. Цифрові платформи моніторингу, системи аналізу поведінкових і інфраструктурних даних, алгоритми машинного навчання дають змогу не тільки фіксувати факт руйнувань або кризових подій, а й виявляти слабкі місця та зародження трендів задовго до моменту їхнього переростання у виклик. Наприклад, аналіз потоків переміщення населення, показників завантаженості лікарень, освітніх закладів, транспортних вузлів і змін у споживанні ресурсів дозволяє регіону завчасно готуватися до нових хвиль внутрішньої міграції, масштабування соціальних послуг чи розгортання додаткових логістичних потужностей. Аналогічно, застосування алгоритмів виявлення аномалій у даних із промислових об'єктів, енергетичних мереж, систем водопостачання дає можливість запобігати техногенним аваріям або мінімізувати наслідки

ворожих кібератак. У цьому розумінні смарт-резильєнтність – це не стільки про фортифікацію, скільки про здатність бачити «тонкі сигнали» майбутніх загроз і перетворювати їх на драйвери інновації. (рис.4.2).

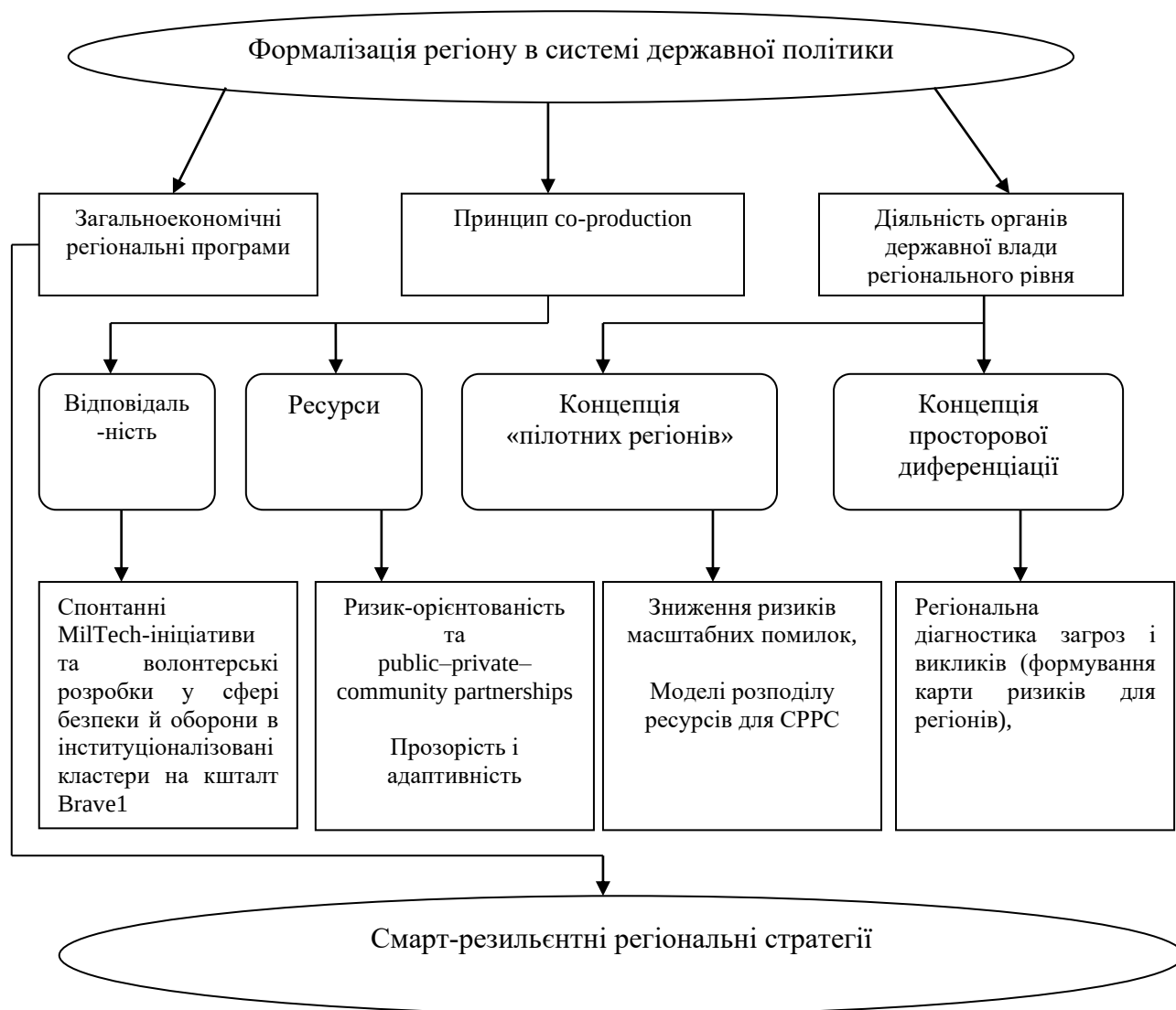


Рис. 4.2. Опис змісту Смарт-резильєнтних регіональних стратегій

Крім того, смарт-резильєнтність змінює саму природу управлінських процесів. Рішення дедалі менше ухвалюються «вручну» на основі інтуїції чи політичної доцільності й дедалі більше ґрунтуються на аналітиці, сценарному моделюванні та багатокритеріальній оцінці. Інструменти Big Data та штучного інтелекту дозволяють оцінювати не лише прямі ефекти тих чи інших рішень (наприклад, відновлення моста чи будівництво нового центру

тимчасового розміщення), а й їхні системні наслідки: як це змінить транспортні потоки, доступ до медичних послуг, ринок праці, податкові надходження, рівень соціальної напруги. Тому смарт-резильєнтність можна трактувати як інтегральну властивість сучасної держави й регіонів, що поєднує технологічну оснащеність, інформаційну прозорість, участь громадян та інституційну гнучкість, роблячи можливим не просто виживання в умовах війни, а цілеспрямований трансформаційний розвиток попри війну.

Інноваційність моделі полягає в тому, що смарт-резильєнтні стратегії спираються на дані в реальному або наближеному до реального часу, використовуючи цифрові платформи моніторингу, геоінформаційні системи, інструменти аналізу настроїв та поведінки населення, реєстри соціально-економічних показників. Це дозволяє не лише фіксувати поточний стан, а й оперативно коригувати регіональні пріоритети, наприклад, перенаправляти ресурси на посилення конкретних громад, які зазнали нових атак, або розгортати додаткові сервіси для хвиль внутрішньої міграції. У термінах New Public Governance така модель працює як «жива мережа», де рішення ухвалюються не одноразово в стратегіях на 5–7 років, а постійно оновлюються через механізми спільного управління – участь місцевих громад, консультації з бізнесом і волонтерами, інтеграцію даних міжнародних партнерів.

Таким чином, модель «смарт-резильєнтних регіональних стратегій» може розглядатися як інструмент операціоналізації переходу від New Public Management до New Public Governance в площині національної стійкості. Вона поєднує мережеву архітектуру управління, співтворення політик і просторову диференціацію, дозволяючи зберегти цілісність держави як системи систем за рахунок посилення суб'єктності регіонів. Умови війни продемонстрували, що реальний потенціал стійкості часто виникає «знизу» – у волонтерських спільнотах, локальних бізнес-кластерах, коопераціях громад, – а завдання держави нового типу полягає в тому, щоб не лише координувати ці енергії, а й вбудовувати їх у формалізовані регіональні

стратегії. Саме тому смарт-резильєнтні регіональні стратегії можуть і повинні стати одним із ключових інструментів просторової диференціації національної моделі стійкості, забезпечуючи узгодження загальнонаціональних цілей із різноманітним локальним контекстом і практик.

На основі нашого наукового підходу СРРС розглядається як цілісна концептуальна рамка, що переводить Національну модель стійкості з рівня абстрактної багаторівневої конструкції на рівень просторово диференційованої практики управління. У цьому контексті смарт-резильєнтні регіональні стратегії трактуються як «моделі другого порядку»: вони не лише адаптують національні цілі до специфіки окремих територій, а й формують зворотний вплив «знизу догори», постачаючи дані, сценарії та інституційні інновації для еволюції самої НМС. Запропонована нами концепція СРРС базується на чотирьох взаємопов'язаних складових, які в сукупності задають логіку просторової диференціації стійкості.

По-перше, індивідуалізація стратегій у нашій моделі виходить за межі традиційного «паспортування» регіонів. Ми пропонуємо розглядати кожен регіон як окрему резильєнтну підсистему зі своїм функціональним призначенням у загальнонаціональній архітектурі: форпост (прифронтальна зона), тиловий хаб, транскордонний шлюз, інноваційно-відновлювальний кластер тощо. Для кожного такого регіону формується не просто описовий, а аналітичний профіль ризиків і можливостей, що включає: конфігурацію економічних ланцюгів та залежність від окремих секторів; параметри ринку праці й людського капіталу (у тому числі міграційні потоки, втрату/притік компетенцій); спектр природних, техногенних та воєнних загроз; щільність і стан об'єктів критичної інфраструктури; інституційну спроможність органів місцевого самоврядування; культурні маркери та рівень соціального капіталу. На цій основі конструюється інтегральний індекс регіональної резильєнтності, що дозволяє визначати критичні вразливості, нішеві переваги та пріоритетні напрями трансформаційного розвитку. Індивідуалізація, таким чином, не зводиться до декларації «особливостей регіону», а виступає

методологічною основою для диференціації цілей, інструментів і показників СРРС.

По-друге, використання цифрових інструментів та інноваційних технологій у нашій концепції СРРС носить системоутворюючий характер і забезпечує перехід від управління «за середніми показниками» до управління в режимі реального часу. Ми виходимо з того, що кожна смарт-резильєнтна стратегія має спиратися на регіональний цифровий двійник, який поєднує геоінформаційну основу (просторові дані про інфраструктуру, населення, екологію), динамічні потоки (енергетика, транспорт, логістика, мобільність населення) та соціально-економічні індикатори (зайнятість, доходи, навантаження на соціальні й медичні системи). До цього ядра інтегруються: системи моніторингу стану об'єктів критичної інфраструктури на основі IoT; смарт-технології управління енергетичними, транспортними та комунальними мережами; інструменти аналізу великих даних і машинного навчання для прогнозування ризиків (від перевантаження лікарень до ймовірних «вузьких місць» у логістиці); модулі аналізу інформаційного середовища для раннього виявлення дезінформаційних або панічних хвиль. У нашій концепції цифровізація не є декоративним елементом, а слугує умовою можливості смарт-резильєнтності як такої, адже саме вона забезпечує предиктивність, варіантність сценарного планування та швидке коригування стратегічних рішень.

По-третє, інтеграція багаторівневих управлінських підходів у межах СРРС осмислюється нами в логіці поліцентричного врядування. Ми відходимо від дихотомії «центр–регіони» і пропонуємо розглядати систему управління стійкістю як мережу центрів прийняття рішень, що функціонують на різних рівнях – від громад і агломерацій до держави та наднаціональних структур. У цій мережі СРРС виконують роль «інтерфейсного формату» між національною рамкою НМС, локальними стратегіями громад та зовнішніми (зокрема, європейськими) програмами підтримки. Вертикальна координація в нашій моделі не означає директивного управління; вона передбачає

узгодження стандартів безпеки, критеріїв оцінки стійкості, принципів розподілу ресурсів і відповідальності. Горизонтальна співпраця між регіонами набуває інструментальної форми через формування міжрегіональних кластерів стійкості (наприклад, логістичних, енергетичних, медичних, освітніх), а також через взаємне резервування потужностей (лікарні, сховища, транспортні коридори, центри розміщення ВПО). Важливим елементом ми також вважаємо «діагональну координацію» – взаємодію регіонів із міжнародними донорами, приватними інвесторами, глобальними технологічними партнерами, котра відбувається у рамках СРРС, але зберігає узгодженість із національними пріоритетами.

По-четверте, створення інтегрованої, регіонально чутливої цифрової платформи моніторингу у нашому баченні є не лише технічним рішенням, а й новою організаційною формою публічного управління. Ми розглядаємо цю платформу як багаторівневу систему підтримки рішень, що працює одночасно для центральних органів влади, регіональних адміністрацій, органів місцевого самоврядування та, в адаптованому вигляді, для громадянського суспільства й бізнесу. На нижньому рівні платформа акумулює дані з локальних сенсорних мереж, реєстрів, відомчих систем і краудсорсингових каналів (звернення громадян, дані з платформ участі, локальні ініціативи). На аналітичному рівні здійснюється агрегація, виявлення трендів, побудова індикаторів стійкості та моделювання сценаріїв. На рівні інтерфейсу ухвалення рішень платформа надає візуалізації, дашборди, системи раннього попередження та інструменти спільного планування (спільні карти ризиків, інтерактивні плани евакуації, матриці перерозподілу ресурсів між регіонами). В архітектурі нульової довіри, яку ми закладаємо в концепцію платформи, особлива увага приділяється сегментації доступу, шифруванню, резервуванню й кіберстійкості, щоб сама система моніторингу не стала вразливістю. Така платформа перетворює СРРС на динамічні, дано-керовані стратегії, здатні еволюціонувати синхронно зі зміною контексту війни, відновлення та довготривалих структурних

трансформацій.

У підсумку, запропонована нами концепція смарт-резильєнтних регіональних стратегій виходить за межі суто планувального документа. СРРС постають як інституційно-технологічні «вузли» в мережі НМС, які одночасно відображають просторову специфіку стійкості, використовують потенціал цифрових технологій та багаторівневого врядування і генерують управлінські інновації, необхідні для переходу від логіки відбудови «як було» до логіки випереджального, трансформаційного розвитку регіонів у надзвичайно турбулентному середовищі.

Інноваційність моделі смарт-резильєнтних регіональних стратегій (СРРС) проявляється у низці принципово нових для української практики публічного управління характеристик. По-перше, просторово диференційована логіка стійкості, за якою СРРС відмовляються від уніфікованого підходу до регіональної політики й пропонують будувати стратегії виходячи з функціональної ролі регіону в Національній моделі стійкості (форпост, тилловий хаб, транскордонний шлюз, інноваційний кластер тощо). Інновація полягає в тому, що стійкість проєктується не як «однакова для всіх» сукупність заходів, а як набір просторово чутливих рішень, прив'язаних до конкретного типу загроз, ресурсів і можливостей території.

По-друге, опора на цифрові двійники регіонів та управління на основі даних, адже як ми зазначали, на відміну від традиційних стратегій, які базуються на періодично оновлюваній статистиці, СРРС передбачають створення регіональних цифрових двійників, що інтегрують геоінформаційні дані, показники функціонування інфраструктури, соціально-економічну динаміку та міграційні потоки. Це дозволяє застосовувати інструменти Big Data та машинного навчання для прогнозування кризових сценаріїв і тестування управлінських рішень до їх реалізації, тобто переходити від реактивної до проактивної моделі стійкості.

По-третє, вбудована мережево-поліцентрична архітектура управління.

СРРС поєднують децентралізацію прийняття рішень на регіональному та місцевому рівнях із вертикальною координацією (рамка НМС) і горизонтальною взаємодією між регіонами. Інноваційність полягає в переході від жорсткої ієрархії до поліцентричної системи, де регіони виступають не пасивними виконавцями державної політики, а активними вузлами мережі, що генерують власні рішення та обмінюються ресурсами (потужності лікарень, логістика, енергетичні резерви, гуманітарна підтримка).

По-четверте, інституціоналізоване спів-творення політик (co-production), коли на відміну від класичних регіональних стратегій, які розробляються вузьким колом посадових осіб і експертів, СРРС формуються як результат взаємодії органів влади, бізнес-кластерів, волонтерських спільнот, наукових інституцій та міжнародних партнерів. Інновація полягає у закладенні механізмів участі та спільної відповідальності за реалізацію стратегії в саму архітектуру СРРС, що наближає їх до стандартів New Public Governance.

По-п'яте, інтегрована цифрова платформа моніторингу стійкості – СРРС передбачають створення регіонально чутливої платформи, яка в режимі наближеному до реального часу агрегує дані від різних суб'єктів (державні служби, громади, бізнес, донори), візуалізує індикатори стійкості та підтримує спільне планування реагування. Інноваційність цієї компоненти – у поєднанні функцій моніторингу, аналітики, раннього попередження й координації дій в єдиному цифровому середовищі з архітектурою нульової довіри.

По-шосте, фокус на трансформаційній, а не лише відновлювальній стійкості. СРРС концептуально орієнтуються не стільки на повернення до «довоєнного стану» (bouncing back), скільки на використання криз як вікна можливостей для структурної модернізації регіонів (bouncing forward): переходу до розподіленої енергетики, переформатування економічних ланцюгів, розвитку нових кластерів (MilTech, логістика, креативні індустрії)

тощо.

«Регіональна чутливість» у нашому підході означає, що платформа не є універсальним національним дашбордом із «усередненими» показниками, а налаштовується під специфіку кожного регіону: тип загроз (прифронтовий, тилловий, транскордонний), структуру економіки, конфігурацію критичної інфраструктури, демографічні та соціокультурні характеристики. На рівні даних платформа акумулює інформацію з різних джерел: державних реєстрів, систем цивільного захисту, геоінформаційних сервісів, сенсорних мереж (IoT) на об'єктах інфраструктури, медичних та освітніх інформаційних систем, даних мобільності населення, а також зворотного зв'язку від громад (електронні платформи участі, чат-боти, звернення громадян). Ці дані не лише зберігаються, а й проходять попередню обробку, верифікацію та стандартизацію з урахуванням принципів архітектури нульової довіри, що мінімізує ризики маніпуляцій і кібервтручань.

На аналітичному рівні регіонально чутлива платформа формує систему індикаторів стійкості, адаптованих до конкретного регіону (навантаження на лікарні, запаси палива й енергії, пропускна спроможність транспортних коридорів, динаміка ВПО, рівень безробіття, стан об'єктів критичної інфраструктури тощо) та забезпечує їх візуалізацію у вигляді інтерактивних карт, «теплових» діаграм, сценарних панелей. Вбудовані алгоритми аналізу великих даних і машинного навчання дозволяють виявляти аномалії (раптове зростання навантаження на соціальні служби, пікові навантаження на мережі, зміни у потоках переміщення населення), будувати прогнози розвитку ситуації та моделювати варіанти реагування з оцінкою можливих наслідків.

На рівні підтримки управлінських рішень платформа надає інтерфейси для різних груп користувачів: центральних органів влади (оглядова картина по країні та міжрегіональні порівняння), регіональних адміністрацій і органів місцевого самоврядування (деталізовані дані по територіальних громадах, інструменти планування заходів реагування, матриці розподілу ресурсів), партнерських структур (бізнес, міжнародні донори, волонтерські мережі – у

форматі обмеженого, але достатнього доступу). Важливим елементом є можливість спільної роботи над планами реагування: платформа підтримує розроблення й оновлення карт ризиків, схем евакуації, планів резервування потужностей, міжрегіональних угод щодо підтримки у надзвичайних ситуаціях. У підсумку така регіонально чутлива платформа перетворює СРРС із статичного документу на живу, дано-керовану систему, що дозволяє не лише фіксувати стан стійкості, а й активно керувати її посиленням у режимі, максимально наближеному до реального часу.

Разом ці елементи дозволяють розглядати СРРС як інноваційну управлінсько-технологічну конструкцію, що якісно відрізняється від традиційних регіональних стратегій як за змістом, так і за способом розроблення та реалізації. Варто навести регіональні кейси запровадження СРРС:

1. Харків («Інтелектуальна фортеця») реалізує стратегію «наукового міста» під постійними обстрілами. Спільно з Н.Фостером розроблено Генеральний план, що включає створення «Наукового кварталу» (Science Quarter) на місці ринку Барабашово. Використання цифрових двійників (Digital Twin) дозволяє моделювати енергоспоживання та транспортні потоки для майбутньої відбудови [344].

2. Миколаїв («Водна безпека та інновації») – спільно з компанією One Works розробляється план, орієнтований на «блакитну економіку» (Блакитна економіка (blue economy) – важлива частина сталої світової економіки по попередженню негативних кліматичних змін, збереження морського та океанського просторів). Проєкти включають модернізацію водопостачання (у відповідь на руйнування водогону), виведення транзитного транспорту з центру та створення інноваційного району для R&D у морській галузі. Розроблена концепція розбудови морського індустріального парку, мета якого – створення індустріального парку для відновлення та розвитку промисловості в місті. Основні елементи парку включають індустріальні підприємства, бізнес-інкубатори, логістичні центри, інфраструктуру та

сервіси, а також зону інновацій. Також розроблено проєкт створення прибережного громадського простору Aqua Port, спрямованого на створення сучасного прибережного громадського простору для відпочинку та навчання. Основні елементи включають зони для літнього водного спорту, маломірного судноплавства та публічні простори для відпочинку та рекреації [345].

3. Буча (лабораторія Smart-відновлення). Буча стала пілотним майданчиком для концепції «Build Back Better». По-перше, Bucha Techno Garden – проєкт створення індустріального та технологічного парку для економічної самодостатності громади. По-друге, Green Recovery – відбудова шкіл та житла з використанням сонячних панелей та теплових насосів. По-третє, оцифрування руйнувань через ONOVA GIS HUB дозволило швидко оцінити збитки та залучити фінансування [346].

Важливо вказати на практичні кроки щодо створення індустріальних парків та релокації. У 2024 році релокація бізнесу стабілізувалася (11 тис. перереєстрацій), при цьому держава стимулює розвиток індустріальних парків (ІП) як точок зростання. Зареєстровано 77 ІП, але реальна ефективність поки низька (1,2 робочого місця на гектар). Слід також вказати на Дія.City як цифровий офшор. Правовий режим Дія.City продемонстрував високу резильєнтність. За 8 місяців 2024 року резиденти сплатили 19,5 млрд грн податків (+81% рік до року). Особливі умови для DefenseTech компаній дозволяють швидко масштабувати виробництво дронів та РЕБ [347].

Так само варто вказати на мілітарну складову реалізації СРРС. У контексті повномасштабної війни гуманітарне розмінування стає не просто технічною чи вузькосекторальною діяльністю, а одним з ключових вимірів регіональної стійкості. Забруднення територій мінами, нерозірваними боєприпасами й вибухонебезпечними залишками війни блокує: повернення населення й відновлення громад; відновлення аграрного виробництва та логістики; розвиток туризму, рекреації, інфраструктурних проєктів; реалізацію програм відбудови та залучення інвестицій. У пропонованій концепції гуманітарного розмінування СРРС розглядається як

інституціональна рамка, в межах якої гуманітарне розмінування інтегрується в ядро регіональної політики стійкості, а не існує паралельно у вигляді окремих проєктів. Саме на основі моделі СРРС є можливість визначити: просторову логіку пріоритезації розмінування; цифрову інфраструктуру для даних про забруднення; мережеву модель управління (держава – громади – міжнародні оператори – бізнес – донори); трансформаційний вектор: від «очищення заради безпеки» до «очищення як драйвера розвитку».

У площині гуманітарного розмінування індивідуалізація СРРС означає, що кожен регіон отримує окремий «профіль мінної резильєнтності», який стає невід’ємною частиною його смарт-резильєнтної стратегії. Такий профіль включає: 1) просторовий розподіл забруднених територій (с/г угіддя, лісові масиви, прифронтові зони, уздовж ліній електропередач, доріг, біля критичної інфраструктури; 2) функціональну важливість забруднених земель (аграрний потенціал; логістичне значення – ключові дороги, мости, залізниця); 3) цінність для життєзабезпечення – водозабори, лінії енергопостачання; 4) екосистемні послуги – ліси, заповідники, водно-болотні угіддя; 5) соціально-економічну чутливість – кількість населення, залежного від цих територій (фермери, працівники, місцеві громади); 6) наявність ВПО, що планують повернення або інтеграцію в регіон; 7) рівень бідності, безробіття, дефіцит альтернативних джерел доходу; 8) інституційну спроможність – наявність і спроможність місцевих координаційних органів з питань розмінування; 9) активність громадських ініціатив та місцевого бізнесу в цій сфері; 10) досвід співпраці з міжнародними операторами й донорами. На основі цього формується ієрархія пріоритетів гуманітарного розмінування в межах регіону, узгоджена із загальними цілями СРРС, отже, вирішується завдання не просто «де розмінувати в першу чергу», а «де розмінування забезпечить найбільший ефект для стійкості й трансформаційного розвитку» [348].

У концепції СРРС гуманітарне розмінування немислиме без цифрового ядра, яке забезпечує:

1. Регіональний цифровий двійник мінної ситуації:

- інтеграція геопросторових даних про підтверджені, підозрювані та очищені території;
- прив'язка до кадастру земель, об'єктів критичної інфраструктури, доріг, комунікацій;
- врахування економічних та соціальних показників (вартість врожаю, кількість домогосподарств, залежних від ділянки, роль у логістичних ланцюгах).

2. Інтеграція польових даних:

- результати обстежень операторів розмінування;
- звіти військових та ДСНС;
- звернення громадян, локальні повідомлення (краудсорсинг);
- супутникові й аерофото дані (дрони, супутники).

3. Аналітичні модулі та Big Data:

- моделювання ризику забруднення для ще необстежених ділянок (за характером бойових дій, типом застосованих боєприпасів, тактикою противника);
- оцінка економічного ефекту від розмінування (втрачені/потенційні доходи, вплив на зайнятість, податкову базу, харчову безпеку);
- пріоритезація ділянок: де співвідношення «вартість–ефект» (у термінах стійкості) є найкращим.

4. Практичні смарт-технології:

- використання безпілотних систем, сенсорів, роботизованих платформ;
- формування єдиних технічних стандартів даних, щоб результати роботи різних операторів були сумісними й автоматично потрапляли в регіональний цифровий двійник;
- інструменти мобільних додатків для інформування населення (карти небезпек, зміни статусу територій, можливість подати повідомлення про підозрілі об'єкти).

Таким чином, цифрова складова СРРС робить гуманітарне розмінування керованим, прозорим і підзвітним процесом, а не набором розрізнених проєктів. Водночас, у рамках СРРС гуманітарне розмінування організовується як поліцентрична мережа, де:

- 1) національний рівень формує нормативну базу, стандарти безпеки, протоколи обміну даними, загальні стратегічні пріоритети;
- 2) регіональний рівень (обласні військові адміністрації, регіональні координаційні платформи) відповідає за:
 - адаптацію національних пріоритетів до локального контексту;
 - координацію різних операторів розмінування;
 - інтеграцію розмінування в регіональну стратегію стійкості (СРРС) і стратегію економічного розвитку;
- 3) рівень громад забезпечує:
 - локалізацію потреб (де є найбільша соціальна й економічна чутливість);
 - комунікацію з населенням і залучення до превенції (MRE – mine risk education);
 - участь у пріоритезації ділянок через публічні консультації, інструменти е-демократії;
- 4) міжнародні та приватні структури (оператори розмінування, донори, бізнес-партнери) вбудовуються в цю мережу через:
 - прозорі регіональні «комплекси (портфелі) проєктів» у сфері розмінування;
 - єдині протоколи звітності й даних;
 - узгодження з профілем регіональної резильєнтності.

Інноваційність СРРС у цій площині полягає в тому, що розмінування з «галузевої» теми перетворюється на інтегральний елемент регіонального врядування, де рішення приймаються на перетині: безпекових міркувань; економічної доцільності; соціальної справедливості (чи не концентруються ресурси лише в «привабливих» регіонах/секторах).

У межах СРРС регіонально чутлива платформа моніторингу для гуманітарного розмінування виконує кілька функцій [349]:

1. Моніторинг стану забруднення та прогресу очищення: стан кожної ділянки (підозра / обстежено / очищено / введено в обіг); тип загрози (міни, касетні боєприпаси, НЗФБ); відповідальний оператор, терміни робіт, залучені ресурси.

2. Відображення «алгоритму стійкості»: як очищення конкретних ділянок впливає на відновлення агровиробництва, відновлення/запуск логістичних маршрутів; повернення населення й зростання зайнятості; реалізацію інфраструктурних проєктів; візуалізацію ефектів розмінування для стійкості (доходи, робочі місця, зменшення гуманітарних ризиків).

3. Підтримка прийняття рішень, перш за все дашборди для регіональних та національних органів влади з можливістю – змінювати пріоритети, перерозподіляти ресурси, моделювати варіанти співпраці з донорами/операторами; а також відкриті або частково відкриті інтерфейси для громад і бізнесу (розуміння, де вже безпечно працювати/інвестувати).

У концепції смарт-резильєнтних регіональних стратегій гуманітарне розмінування не обмежується поверненням до довоєнного статус-кво [349]. Воно розглядається як: по-перше, умова структурної перебудови економіки регіонів (перехід до більш високотехнологічного, екологічного та диверсифікованого використання земель після очищення); по-друге, поле для інновацій (розвиток українських технологій розмінування, робототехніки, аналізу даних, навчання персоналу, створення експортоспроможних компетенцій); по-третє, платформа для нових партнерств (державно-приватних, науково-технологічних, міжнародних), які посилюють резильєнтність не лише до мінної загрози, а й до майбутніх криз [349].

Таким чином, у площині гуманітарного розмінування СРРС виступають інтегральною рамкою, що просторово диференціює потреби й пріоритети розмінування; забезпечує цифрове, дано-кероване управління цим процесом; вбудовує його в поліцентричну систему врядування; перетворює очищення

територій на один із ключових механізмів трансформаційної стійкості регіонів України.

4.4. Компаративно-адаптаційні механізми розвитку НМС та формат «раціональної цифрової стабільності» в умовах гібридних загроз

У сучасному геополітичному цивілізаційному вимірі, що характеризується гібридними загрозами, кібернетичними атаками та повномасштабними військовими конфліктами, концепція національної безпеки зазнала фундаментальної трансформації. Традиційний підхід, що спирався виключно на військову міць та захист кордонів, поступився місцем концепції національної стійкості (resilience). Стійкість визначається не просто як здатність держави витримати удар, а як системна спроможність суспільства та інституцій адаптуватися до шоківих змін, забезпечувати безперервність життєво важливих функцій та відновлюватися на якісно новому рівні.

Для України, яка перебуває в епіцентрі найбільшого з часів Другої світової війни військового конфлікту в Європі, побудова ефективної національної системи стійкості є екзистенційним імперативом. Ухвалення Указу Президента України № 479/2021 «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» заклало нормативний фундамент для цього процесу. Водночас практична імплементація цієї концепції, деталізована в Розпорядженні Кабінету Міністрів № 1025-р від 10 листопада 2023 року «Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року», потребує ретельного вивчення та адаптації кращих світових практик [350].

Авторська дослідницька методологія базується на компаративному моделі стійкості Фінляндії, Ізраїлю, Великої Британії, Естонії та США. Кожна з цих країн розробила унікальні механізми реагування на кризи, які

можуть бути інтегровані в українську архітектуру безпеки: від фінської моделі «всеосяжної безпеки» та ізраїльської системи цивільного захисту до британської багаторівневої координації та естонської цифрової моделі. Аналіз зосереджено на виявленні конкретних законодавчих, технологічних та організаційних рішень, які дозволять Україні перейти від волонтерського героїзму до інституціоналізованої національної (державної) стійкості.

Модель Сполучених Штатів Америки є еталонним прикладом того, як масштабна федеративна система переходить від жорстких регуляторних мандатів до ризик-орієнтованого підходу, забезпечуючи при цьому уніфіковану реакцію на кризові ситуації через сувору стандартизацію обміну даними. Вона демонструє, що ключем до стійкості є не уніфікація програмного забезпечення чи централізований контроль, а поєднання гнучкості на рівні організацій із жорсткими вимогами до безпеки, даних та інтероперабельності.

Еволюція хмарної стратегії федерального уряду США від моделі «Cloud First» до «Cloud Smart» є показовою для розроблення та імплементації української політики у сфері хмарних послуг [351]. Початкова стратегія «Cloud First» (2011 р.) зобов'язувала федеральні агентства надавати пріоритет хмарним рішенням, що часто призводило до формального підходу типу «lift and shift» – прямого перенесення застарілих застосунків у хмарне середовище без їхньої архітектурної модернізації. Такий підхід у багатьох випадках не забезпечував ні очікуваних економічних вигід, ні підвищення рівня кібербезпеки, а іноді навіть відтворював наявні вразливості у новому середовищі. У відповідь на ці обмеження у 2019 р. Адміністративно-бюджетне управління (Office of Management and Budget, OMB) представило оновлену стратегію «Cloud Smart», яка базується на трьох взаємопов'язаних стовпах – безпека, закупівлі та кадровий потенціал. «Cloud Smart» відходить від догматичного принципу «хмара за будь-яку ціну», натомість пропонуючи прагматичний підхід, за якого кожне агентство оцінює доцільність хмарних рішень з огляду на свою місію, технічні вимоги, профіль ризиків та життєвий

цикл інформаційних систем. Такий підхід релевантний для України, де імплементація Закону «Про хмарні послуги» має уникнути як технологічного популізму, так і надмірної зарегульованості, натомість забезпечивши раціональну, ризик-орієнтовану міграцію до хмари [351].

Ключовим елементом американської моделі, який має безпосереднє значення для проєктування українського реєстру надавачів хмарних послуг, є програма FedRAMP (Federal Risk and Authorization Management Program). Вона стандартизує процеси оцінки безпеки, авторизації та безперервного моніторингу хмарних продуктів і сервісів у федеральному секторі. Засадовим принципом FedRAMP є взаємність (reciprocity): якщо провайдер хмарних послуг, наприклад Amazon Web Services або Microsoft Azure, отримує авторизацію для одного федерального агентства, відповідний пакет авторизації (Authority to Operate, ATO) стає доступним для повторного використання іншими установами. Це дозволяє усунути дублювання аудиторських зусиль, заощаджує значні фінансові та часові ресурси й формує єдину «мову безпеки» для держави та ринку [352].

Іншою інституційною інновацією є екосистема акредитованих сторонніх оцінювальних організацій (Third-Party Assessment Organizations, ЗРАО). Федеральний уряд не проводить усі аудити власними силами; натомість він встановлює стандарти та здійснює акредитацію незалежних аудиторів, які виконують оцінювання відповідності хмарних сервісів вимогам FedRAMP. Це створює ринковий механізм забезпечення відповідності (compliance), який дає змогу масштабувати сертифікацію набагато швидше, ніж за умов суто державного контролю, і водночас зберігати єдину нормативну рамку. Фундаментальним елементом FedRAMP є модель безперервного моніторингу (Continuous Monitoring, ConMon). Авторизація не розглядається як одноразовий акт із тривалим строком дії, а як процес, що потребує регулярного підтвердження. Провайдери зобов'язані щомісяця надавати звіти про результати сканування вразливостей, стан управління оновленнями (patch management), обробку інцидентів безпеки та

усунення виявлених недоліків. Порухення вимог ConMon може призвести до призупинення або відкликання авторизації, що стимулює провайдерів підтримувати постійно високий рівень кіберстійкості [352].

У контексті українського законодавства, зокрема Закону України «Про хмарні послуги», який покладає на Державну службу спеціального зв'язку та захисту інформації відповідальність за ведення переліку надавачів хмарних послуг, існує ризик перетворення цієї процедури на «вузьке горло» або формальну реєстраційну практику [353]. Адаптація принципів FedRAMP – насамперед моделі ЗРАО та безперервного моніторингу – дозволила б залучити приватний сектор до процесів аудиту та оцінювання, залишаючи за державою функції акредитації, встановлення стандартів і нагляд за їх дотриманням. Перехід від періодичної переатестації комплексних систем захисту інформації (КСЗІ) раз на декілька років до режиму постійного моніторингу відповідності є критичним з огляду на динаміку сучасних кіберзагроз і масштаб воєнних викликів, із якими стикається Україна.

Другим виміром, у якому модель США демонструє системний підхід до стійкості, є створення та розвиток Національної системи управління інцидентами (National Incident Management System, NIMS). NIMS забезпечує уніфікований організаційний та процедурний каркас для управління інцидентами будь-якого масштабу – від локальних пожеж до національних катастроф – і синхронізує дії різномірних суб'єктів (федеральних, штатних, місцевих органів влади, служб екстреного реагування, приватного сектору). Технічним фундаментом цієї системи виступає інтегрованість, досягнута не через запровадження єдиного програмного забезпечення для всіх, а через жорстку стандартизацію форматів обміну даними й протоколів взаємодії. У сфері обміну даними в надзвичайних ситуаціях США використовують набір спеціалізованих XML-стандартів EDXL (Emergency Data Exchange Language), розроблених консорціумом OASIS за підтримки Міністерства внутрішньої безпеки (Department of Homeland Security, DHS). Зокрема, стандарт EDXL-HAVE (Hospital Availability Exchange) дозволяє

лікарням автоматично публікувати інформацію про наявні ресурси: кількість вільних ліжок у відділеннях інтенсивної терапії, доступність спеціалізованого медичного персоналу, статус приймальних відділень (відкрито, обмежене приймання, переповнено). Під час подій із масовими ураженнями це дає змогу службам екстреної медичної допомоги оперативно маршрутизувати потік поранених до тих закладів, які реально спроможні їх прийняти, уникаючи перевантаження окремих лікарень. Інтеграція аналогічної функціональності до української системи eHealth у взаємодії з Державною службою України з надзвичайних ситуацій та Міністерством охорони здоров'я могла б суттєво підвищити ефективність реагування на ракетні удари та інші масові інциденти, замінивши фрагментарні телефонні комунікації автоматизованими процесами прийняття рішень [354].

При цьому стандарт EDXL-DE (Distribution Element) виступає універсальним контейнером для маршрутизації повідомлень. Він містить метадані про відправника, цільову географічну зону (наприклад, багатокутник геопросторових даних) та тип вмісту (ситуаційний звіт, запит на ресурси, попередження тощо). Мова обміну даними про надзвичайні ситуації (EDXL) – це набір стандартів обміну повідомленнями на основі XML, які сприяють обміну інформацією про надзвичайні ситуації між урядовими установами та всіма організаціями, пов'язаними з надзвичайними ситуаціями. EDXL стандартизує формати повідомлень для зв'язку між цими сторонами. EDXL був розроблений як безкоштовний стандарт Міжнародним консорціумом відкритих стандартів OASIS.

OASIS (англ. Organization for the Advancement of Structured Information Standards) є глобальним некомерційним консорціумом, який займається розробкою, конвергенцією й ухваленням відкритих стандартів у рамках міжнародної інформаційної спільноти. Цей консорціум є лідером за кількістю випущених стандартів, що належать до вебслужб. Окрім цього, він займається стандартизацією в області безпеки, електронної комерції; також зачіпається суспільний сектор і ринки вузькоспеціальної продукції. В OASIS

входить понад 5000 учасників, що представляють понад 600 різних організацій зі 100 країн світу. Спонується провідними корпораціями ІТ індустрії – IBM, Novell, Oracle, Microsoft, Sun [355].

У квітні 2013 року консорціум OASIS був акредитований Американським інститутом національних стандартів (ANSI). Отримання акредитації ANSI дозволить OASIS передавати свої стандарти в ANSI для затвердження їх як американських національних стандартів, а також безпосередньо представляти свої стандарти для прийняття організаціями ISO (Міжнародна організація зі стандартизації) і IEC (Міжнародна організація зі стандартизації), без проходження попередніх формальних процедур і затвердження в додаткових інстанціях. EDXL було розроблено для того, щоб забезпечити обмін інформацією про життєво важливі ресурси між місцевими, державними, племінними, національними та неурядовими організаціями. Впровадження стандартів EDXL має на меті покращити швидкість та якість скоординованих дій реагування, дозволяючи обмін інформацією в режимі реального часу [355].

Завдяки цьому досягається гарантована доставка релевантної інформації лише уповноваженим одержувачам, навіть у разі використання гетерогенних інформаційних систем та каналів зв'язку. У свою чергу, протокол Common Alerting Protocol (CAP) є основою інтегрованої системи сповіщення та попередження IPAWS (Integrated Public Alert and Warning System) [356]. CAP забезпечує можливість створення одного уніфікованого повідомлення про загрозу, яке система автоматично трансформує в повідомлення для різних каналів – радіо та телебачення (EAS), мобільних пристроїв (Wireless Emergency Alerts, WEA), сирен, інтернет-сервісів тощо. Для України, яка вже здійснила суттєвий прогрес у впровадженні технології Cell Broadcast, перехід до повноцінної реалізації стандарту CAP відкриває можливість глибшої інтеграції оповіщення в цифрову інфраструктуру: системи «розумного міста», цифрові вивіски, платформи «розумного дому», застосунки третіх сторін, що дозволило б значно розширити охоплення

населення та підвищити якість реагування [356].

Важливим інституційно-технологічним компонентом американської моделі кризового управління є платформа WebEOC, яку використовує Федеральне агентство з управління надзвичайними ситуаціями (Federal Emergency Management Agency, FEMA) та більшість штатів. WebEOC функціонує як веб-орієнтована інтеграційна платформа для управління оперативною інформацією та координації дій у кризових ситуаціях, виконуючи роль «віртуальної дошки оголошень» для штабів реагування. Її особливістю є наявність механізмів інтероперабельності через компонент Fusion Server, що дозволяє автономним інсталяціям WebEOC у різних штатах обмінюватися даними та координувати запити на ресурси. Таким чином, штат, який постраждав від масштабної події (наприклад, урагану), може в автоматизованому режимі звертатися за допомогою до сусідніх юрисдикцій, навіть якщо їхні внутрішні інформаційні системи, організаційні процедури та нормативні режими істотно відрізняються [357].

Архітектура WebEOC передбачає також можливість роботи локальних серверів в умовах обмеженого або відсутнього зовнішнього зв'язку з подальшою синхронізацією даних після його відновлення. Ця властивість є особливо релевантною для українських умов, які характеризуються ризиками тривалих блекаутів, пошкодженням телекомунікаційної інфраструктури та необхідністю забезпечення безперервності критичних управлінських процесів навіть у разі ізоляції окремих регіонів. Адаптація концептуальних рішень, закладених у WebEOC, може стати основою для побудови національної платформи управління надзвичайними ситуаціями в Україні, здатної інтегрувати дані від різних відомств, рівнів влади й партнерських структур у єдиному інформаційному полі.

Отже, формальна американська модель НМС демонструє, що стійкість сучасної держави базується на поєднанні ризик-орієнтованої хмарної стратегії (Cloud Smart і FedRAMP), поліцентричної системи управління інцидентами (NIMS), жорсткої стандартизації протоколів обміну даними

(EDXL, CAP) та використанні інтеграційних платформ типу WebEOC, здатних працювати в умовах фрагментованої інфраструктури. Для України ключовим завданням є не механічне копіювання цих інструментів, а осмислена адаптація їхніх принципів – взаємності, безперервного моніторингу, стандартизації даних та децентралізованої інтероперабельності – до власного правового, інституційного й безпекового контексту. Це створює підґрунтя для побудови національної системи цифрової стійкості, здатної функціонувати в умовах тривалої війни та післявоєнної відбудови.

У Сполучених Штатів Америки немає єдиного кодифікованого загальнонаціонального документу у вигляді «Національної моделі стійкості» (National Resilience Model). Останніми роками в США формується окремий документ – National Resilience Strategy, який задає загальні принципи й пріоритети підвищення стійкості держави, зокрема інфраструктури та управління ризиками. У документах зазначено, що стратегія має регулярно переглядатися (раз на 4 роки або за потреби), тобто розглядається як еволюційний, а не раз і назавжди «завершений» документ. Однак за змістом це стратегія (vision, principles, пріоритети), а не формалізована «модель» зі структурою рівнів, підсистем та єдиним нормативним описом [358].

Система національної готовності у США (National Preparedness System) і PPD-8 – Президентська директива PPD-8 «National Preparedness» визначає рамку національної готовності, яка включає поняття національної стійкості й реалізується через Національну ціль готовності, п'ять національних рамкових документів – пом'якшення (mitigation), захист, реагування, відновлення, запобігання тощо. Це фактично функціональна модель стійкості й готовності, але вона розподілена між кількома документами; не оформлена як один інтегрований «National Resilience Model». До формату стійкості також входять: Національні рамки та плани у сфері захисту та пом'якшення (National Mitigation Framework та пов'язані документи), окремі рамки/стратегії, наприклад, у сфері кліматичної стійкості (National climate resilience framework); документи щодо критичної інфраструктури,

кіберстійкості тощо. У сукупності вони формують де-факто модель, але не зведену в один «зобов'язальний» документ [359].

Варто вказати, що Федеральне агентство з надзвичайних ситуацій (FEMA) розробляє National Resilience Guidance – документ, який подається як «collaborative approach to national resilience» і має узгодити підходи до стійкості для «всієї спільноти» (whole community). На момент оприлюднення він був у статусі national engagement draft (проект для національного обговорення), а не затвердженого стандарту [360].

Ключові принципи та компоненти National Resilience Guidance:

1) спільний підхід – стійкість не формується одним сектором; вона вимагає спільної роботи окремих осіб, підприємств, неурядових організацій та всіх рівнів влади;

2) шоки та стресові фактори – визнає, що хронічні проблеми (стреси) послаблюють спільноти, роблячи їх більш вразливими до гострих подій (шоків);

3) взаємопов'язані системи – концепт National Resilience Guidance осереджується на шести основних системах: соціальній, економічній, екологічній, житловій, інфраструктурній та інституційній [360].

National Resilience Guidance надає моделі (наприклад, моделі стійкості) для планування та впровадження, переходячи від розуміння до дії. Це показує, що навіть тут США рухаються радше шляхом поступового формування рамки, ніж фіксації однієї остаточної «моделі». «Національна модель стійкості» США існує як поліцентрична, система, а не як один завершений кодифікований документ. Україна рухається до більш цілісного, «рамкового» документа, тоді як США будують модель через мережу стратегій і стандартів [360].

Модель НМС Великої Британії демонструє, як за допомогою інструментів цифрового врядування та фінансово-процедурних механізмів можна вибудовувати цілісну національну модель стійкості. Ключова особливість підходу у Великій Британії полягає в тому, що цифрові

платформи, стандарти сервісу та механізми контролю видатків розглядаються як інфраструктура загальнодержавної стійкості: вони забезпечують безперервність ключових публічних функцій, керованість державних інвестицій, узгодженість інституційної архітектури та здатність держави швидко адаптуватися до криз.

На відміну від багатьох країн, де «цифрові міністерства» мають переважно дорадчий статус, у Великій Британії Кабінет Міністрів (Cabinet Office) через Government Digital Service (GDS, створений у 2011 р.) [361] та Central Digital and Data Office (CDDO, сформований у 2021 р.) [362] володіє реальним інструментом впливу на формування національної стійкості – механізмом контролю видатків (spend controls). Цей механізм уперше був формалізований для ІКТ-проектів у 2010–2012 рр., а потім деталізований у керівництві Cabinet Office «Digital and Technology Spend Controls» (2014 р.; оновлені версії – 2017 і 2021 рр. під егідою CDDO). Відповідно до цих документів, будь-який центральний орган влади, який планує суттєві витрати на цифрові сервіси чи ІТ-інфраструктуру, зобов'язаний отримати попереднє схвалення від CDDO/GDS, якщо вартість перевищує встановлені пороги (орієнтовно 100 тис. фунтів стерлінгів для публічних цифрових сервісів і 1 млн фунтів для інфраструктурних та технологічних проектів) [363].

Це означає, що архітектура державних цифрових систем і структура державних витрат стають частиною єдиного управлінського поля національної стійкості: центральний орган не лише «радить», а й реально блокує або коригує проекти, якщо вони знижують системну стійкість (фрагментують дані, дублюють критичні функції, створюють залежність від закритих рішень, не мають планів безперервності діяльності). Така логіка закріплена, зокрема, в «Government Roadmap for Digital and Data 2022–2025» (Cabinet Office/CDDO, 2022 р.), де підкреслюється роль спільних стандартів та контролю інвестицій у зміцненні стійкості держави [364].

Ключем до такого підходу є випереджальне планування. Міністерства та агентства зобов'язані формувати «pipeline» запланованих цифрових та

ІТ-ініціатив на 15-18 місяців уперед та подавати його до CDDO/GDS відповідно до оновлених правил spend controls (версії 2014, 2017, 2021 рр.). Це дає змогу на національному рівні бачити сукупну картину майбутніх цифрових змін, виявляти дублювання (наприклад, спроби створити альтернативні системи ідентифікації замість участі в програмі *GOV.UK One Login*, 2021–2023 рр.) чи альтернативні платіжні системи замість використання GOV.UK Pay (запущено у бета-режимі з 2016 р.). Таким чином, превентивне управління цифровими інвестиціями безпосередньо працює на структурну стійкість держави, обмежуючи появу «островів» критично важливої інфраструктури, які важко підтримувати й інтегрувати в умовах кризи [365].

У межах spend controls проекти класифікуються за ризиковим профілем (Assured, Monitor, Control), що відображено в оновлених керівництвах Cabinet Office/CDDO 2017 та 2021 рр. Ця класифікація відбиває не лише технологічні, а й інституційні та операційні ризики: чи забезпечує проєкт безперервність виконання публічних функцій, чи не створює він надмірної залежності від одного постачальника, чи передбачені сценарії відновлення після інцидентів. Відповідно, фінансовий контроль перетворюється на інструмент управління національною стійкістю, а технічні стандарти з «м'яких рекомендацій» – на жорсткі порогові умови доступу до бюджетних ресурсів [365].

Центральним елементом інституціоналізації такої стійкості є Урядовий стандарт сервісу (Government Service Standard). Його перша версія була запроваджена GDS як Digital Service Standard у 2014 р., а оновлена та формалізована в ширшому форматі Government Service Standard у 2019 р. (14 пунктів; актуалізований у 2021 р.). Формально це набір критеріїв до проєктування та експлуатації цифрових послуг, але де-факто він виконує роль нормативної рамки національної стійкості у сфері публічних сервісів. Стандарт застосовується на різних етапах життєвого циклу послуги (Alpha, Beta, Live Assessment) і визначає не лише якість користувацького досвіду, а й

вимоги до безпеки, інклюзивності, доступності, управління ризиками та відновлення.

Особливо важливим у контексті НМС є пункт 14 «Operate a reliable service» (у версії 2019 р.), що вимагає від команд розробників і власників сервісів:

- встановлювати чіткі, вимірювані цілі щодо доступності (uptime) і максимально допустимого часу простою;
- розробляти та регулярно відпрацьовувати сценарії відновлення роботи після інцидентів у середовищах, наближених до продуктивного;
- впроваджувати методи розгортання, які мінімізують або усувають простої (blue-green deployment, canary-релізи тощо) [366].

Якщо сервіс не відповідає Стандарту сервісу (зокрема, вимогам до надійності та відновлюваності), він не може бути розгорнутий або масштабований на національній платформі GOV.UK (запущена GDS у 2012 р.), а його фінансування може бути обмежено відповідно до керівництв spend controls. Це означає, що безпека та стійкість окремих цифрових сервісів трансформуються у вимогу до стійкості всієї системи державного управління: держава свідомо не дозволяє вводити в експлуатацію сервіси, які можуть «провалитися» в момент кризи й паралізувати виконання базових функцій.

Ще одним стрижневим компонентом національної моделі стійкості є реалізація концепції «Уряд як платформа» (Government as a Platform, GaaP), яка системно оформлена в Government Transformation Strategy 2017–2020 (Cabinet Office, 2017 р.) та подальших програмних документах GDS/CDDO [367]. Йдеться про створення спільних, стандартизованих платформених сервісів, які виконують роль «критичної спільної інфраструктури» для всієї системи державного управління. До таких сервісів належать:

- GOV.UK Pay (бета з 2016 р., масштабування з 2017–2018 рр.) – єдина платформа для онлайн-платежів до державних органів [368];

- GOV.UK Notify (запущено в публічний бета-режим у 2016 р.) – сервіс масових сповіщень (SMS, email, листи) [369];
- платформи хостингу й інфраструктури (наприклад, GOV.UK Platform as a Service, розгорнута після 2016 р.) та, пізніше, єдина програма цифрової ідентифікації GOV.UK One Login (з 2021 р.) [370].

Ці сервіси розглядаються не лише як інструменти економії коштів, а як елементи національної критичної цифрової інфраструктури, надійність і масштабованість якої є умовою стійкості в умовах кризи. Завдяки наявності GOV.UK Pay, GOV.UK Notify та стандартизованих рішень хостингу місцеві органи влади змогли за лічені дні запустити сервіси підтримки вразливих груп (реєстрація на допомогу, організація доставки продуктів і ліків, локальні програми підтримки бізнесу). Національна інфраструктура платформ, закріплена в стратегіях 2017–2020 та дорожній карті 2022–2025 рр., фактично виступила каркасом стійкості всієї публічної системи, дозволивши швидко синхронізувати рішення різних рівнів влади, не жертвуючи безпекою, надійністю та прозорістю.

Узагальнюючи, практика Великої Британії показує, що національна модель стійкості може вибудовуватися не лише через окремий «документ про стійкість», а через комбінацію інституційних механізмів і політик:

- 1) централізований контроль цифрових та ІТ-видатків (керівництва spend controls 2014, 2017, 2021 рр.) як інструмент управління системними ризиками;
- 2) обов'язкові стандарти сервісу (Government Service Standard 2019/2021 рр.) як норми стійкості для всієї державної сервісної екосистеми;
- 3) спільні платформені сервіси (GOV.UK Pay, Notify, PaaS, One Login, розгорнуті з 2012–2016 рр. і далі) як елементи критичної національної інфраструктури, придатні для швидкого розгортання в умовах криз.

Для України це означає, що побудова НМС має передбачати інтеграцію стійкості в бюджетний процес, технічну архітектуру й стандарти сервісів, а не обмежуватися секторальними стратегіями чи лише «цифровим виміром».

Платформи на кшталт «Дія.Engine» можуть відігравати роль аналогічних «каркасів стійкості», за умови, що вони поєднані з реальними важелями контролю видатків, єдиними стандартами послуг та безперервністю виконання ключових державних функцій у кризових умовах (таблиця 4.6).

Таблиця 4.6

Концептуалізація досвіду Великої Британії у побудові НМС

Елемент моделі	Ключовий зміст (з роками й документами)	Досвід для НМС України
Загальний підхід Великої Британії до стійкості	Інтеграція цифрового врядування, фінансового контролю та стандартів сервісу в єдину рамку забезпечення стійкості, закріплену, зокрема, в Government Transformation Strategy 2017–2020 та Government Roadmap for Digital and Data 2022–2025 (Cabinet Office/CDDO)	Показує, як послідовні стратегії (2017–2020, 2022–2025) формують довгострокову Національну модель стійкості, де цифрова сфера – несучий елемент, а не ізольований сегмент
Spend Controls як інструмент стійкості	Механізм контролю видатків на ІКТ-проекти, запроваджений для центрального уряду у 2010–2012 рр. та формалізований у керівництві «Digital and Technology Spend Controls» (Cabinet Office, 2014; оновлення 2017, 2021). Пороги: ≈£100k для цифрових сервісів, ≈£1m для інфраструктурних	Фінансовий контроль, закріплений у формальних документах 2014–2021 рр., використовується як інструмент керування системними ризиками, що безпосередньо посилює національну стійкість
Пайплайн закупівель	Обов'язок органів влади подавати 15–18-місячний пайплайн цифрових/ІТ-закупівель відповідно до правил spend controls (редакції 2014, 2017, 2021 рр.), з можливістю зупинити дублюючі чи ризикові ініціативи до оголошення тендерів	Дає змогу будувати єдину архітектурну карту держави, уникати фрагментації критичної інфраструктури та закладати стійкість на стадії планування бюджетів
Категоризація ризиків (Assured / Monitor / Control)	У керівництвах Cabinet Office/CDDO щодо spend controls (2017, 2021 рр.) проекти класифікуються за ризиковими категоріями; високоризикові (Control) блокуються до усунення недоліків, що впливають на стійкість і безпеку	Перетворює технічні та процесні критерії на інструмент управління національними ризиками, пов'язаними з працездатністю та безперервністю критичних функцій
Government Service Standard (2014, 2019, 2021)	Перший Digital Service Standard запроваджений GDS у 2014 р., оновлений як Government Service Standard (14 пунктів) у 2019 р., з подальшими оновленнями 2021 р. Регламентує проєктування й експлуатацію сервісів (безпека, доступність, ризики, відновлення)	Може слугувати прототипом національного стандарту стійкості публічних сервісів в Україні, офіційно закріпленого в нормативних документах і пов'язаного з фінансуванням

Продовження таблиці 4.6

Елемент моделі	Ключовий зміст (з роками й документами)	Досвід для НМС України
Пункт 14 «Operate a reliable service» (2019)	Пункт 14 Government Service Standard (2019) фіксує вимоги до високого uptime, часу відновлення, регулярних тестів відмов та використання безперервних стратегій розгортання (blue-green тощо)	Створює практику resilience by design на рівні сервісів; аналогічні вимоги можуть бути інтегровані в українські технічні стандарти й типові ТЗ для державних ІТ-проектів
Оцінювання Alpha/Beta та доступ до GOV.UK (2012+)	З 2012 р. платформа GOV.UK використовується як єдиний фронт-енд держави; сервіси допускаються до домену лише після проходження Alpha/Beta/Live-оцінювання на відповідність Government Service Standard (редакції 2014, 2019, 2021 pp.)	Логіка «нема відповідності стандартам стійкості – нема запуску й фінансування» може бути вбудована в українську систему допуску сервісів до держреєстрів, порталів та платформ
Government as a Platform (GaaP) (з 2012–2016 pp.)	Концепція GaaP, системно зафіксована в Government Transformation Strategy 2017–2020, реалізується через спільні сервіси: GOV.UK Pay (beta з 2016 р.), GOV.UK Notify (beta з 2016 р.), GOV.UK PaaS (після 2016 р.), GOV.UK One Login (з 2021 р.). Платформи стали базою для швидкого розгортання сервісів у кризу COVID-19 (2020–2021 pp.)	Демонструє, як платформені компоненти, впроваджені й закріплені стратегіями 2017–2025 pp., перетворюються на інфраструктуру національної стійкості, що Україна може віддзеркалити через розвиток «Дія.Engine» та споріднених платформ

Джерело: узагальнено за [361-370]

Естонська модель цифрової держави є однією з найбільш наближених до української моделі (зокрема завдяки використанню технології X-Road у системі «Трембіта»), однак водночас вона демонструє значно глибшу інтеграцію цифрових рішень у національну модель стійкості. Для Естонії цифрова держава – це не лише зручність сервісів, а насамперед інфраструктура виживання й безперервності державності в умовах кібератак, гібридної війни та потенційної окупації.

Архітектура X-Road (X-tee) [371] була розгорнута на національному рівні у 2001 році як шар обміну даними між інформаційними системами держави. Вона реалізує принцип розподілених реєстрів – не існує єдиної «супербази», знищення якої паралізувало б державне управління. Кожен

реєстр (населення, податки, нерухомість, транспорт тощо) зберігається та адмініструється профільним відомством, а X-Road забезпечує захищений, автентифікований і шифрований обмін даними між ними в режимі реального часу [371].

Такий підхід безпосередньо працює на інфраструктурну стійкість:

1) відсутність єдиної точки відмови означає, що компрометація або вихід з ладу одного реєстру не блокує функціонування інших систем, а отже – не паралізує всю державу;

2) децентралізоване володіння даними поєднується з централізованими правилами інтероперабельності, що дозволяє одночасно зберігати інституційну автономію та підтримувати єдине інформаційне поле [371].

Ключовим нормативним елементом є принцип «once-only»: держава не має права повторно запитувати в громадянина або бізнесу дані, які вже збережені в будь-якому державному реєстрі. Цей принцип закріплений у правовій базі Естонії та підтримується європейськими ініціативами щодо інтегрованих публічних послуг. Юридична обов'язковість «once-only» змушує відомства не дублювати бази даних, а налагоджувати автоматизований обмін через X-Road, перетворюючи інтероперабельність із технічної опції на правовий імператив. У результаті цілісність, актуальність і узгодженість даних стають системною властивістю держави, а не «проектним досягненням» окремих органів [371].

У контексті національної стійкості X-Road виконує роль «цифрового хребта» держави: навіть за умов локальних відмов, атак або фізичного пошкодження окремих центрів обробки даних, розподіленість і дублювання функцій через цей шар дозволяють зберігати працездатність критично важливих процесів (оподаткування, реєстрація прав, виплати, ідентифікація). Після масованих кібератак 2007 року Естонія зробила акцент не лише на захисті доступності систем, а й на математично гарантованій цілісності даних, тобто на неможливості їх непомітної підміни заднім числом. Для

цього уряд у співпраці з компанією Guardtime почав у 2008 році розробляти та впроваджувати технологію KSI (Keyless Signature Infrastructure) Blockchain, яка з 2012 року використовується для захисту критичних державних реєстрів [372].

З точки зору національної стійкості, KSI виконує одразу декілька функцій: антифейк і антикорупція: унеможливорює непомітну зміну прав власності, судових рішень, реєстраційних даних, що критично важливо для постконфліктних і постокупаційних сценаріїв; стійкість до внутрішніх загроз: знижує ризик зловживань з боку інсайдерів у критичних системах; підвищення міжнародної довіри: дозволяє партнерам та інвесторам покладатися на правовий режим, підкріплений технічною незмінністю записів. Для України така модель особливо актуальна у зв'язку з ризиками маніпуляцій правами власності, реєстрами боргів, судових рішень на тимчасово окупованих територіях. Інтеграція подібних механізмів у національну модель стійкості дала б змогу математично доводити автентичність та історію державних записів після деокупації, незалежно від того, які дії з даними вчиняв окупант.

Третім ключовим виміром естонської моделі стійкості є концепція «цифрових посольств» (data embassies). Ідея полягає в тому, що критично важливі державні інформаційні системи та дані реплікуються в захищені дата-центри за кордоном, яким надається спеціальний міжнародно-правовий статус, подібний до статусу фізичного посольства. Перше таке цифрове посольство створено в Люксембурзі. Уряд Естонії схвалив відповідну угоду 15 червня 2017 року, а «Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems» було підписано 20 червня 2017 року; парламентську ратифікацію завершено у 2018 році. На основі цієї угоди ресурси дата-центру в Люксембурзі отримали договірний режим, близький до екстериторіальності: держава перебування не може самотійно отримувати доступ до розміщених там естонських систем і даних, а поводить з ними як з об'єктами, що

підлягають суверенітету Естонії [373].

Операційно модель виглядає таким чином: критично важливі реєстри (населення, бізнес, податки, реєстр нерухомості, ключові елементи е-сервісів) безперервно реплікуються в інфраструктуру цифрового посольства. У разі масштабної фізичної атаки, кібератаки, окупації частини території або руйнування національних дата-центрів держава може перезапустити ключові цифрові функції зі «запасного суверенного майданчика», не втрачаючи безперервності правовідносин (виплати, реєстрації, голосування, банківські операції, ідентифікація). Таким чином, естонська держава будує вищий рівень стійкості, й навіть у разі тимчасової втрати контролю над фізичною територією вона зберігає контроль над своєю цифровою інфраструктурою та правовими записами. Це підвищує не лише технологічну, а й конституційно-правову стійкість: існування держави як правопорядку й інформаційної системи стає менш залежним від ситуації. Для України, яка вже активно використовує хмарні платформи для резервного копіювання реєстрів, естонський досвід показує важливість формалізації міжнародно-правового статусу таких розміщень.

Розподілена архітектура обміну даними (X-Road, 2001 р.), математична гарантія цілісності (KSI Blockchain, з 2008/2012 рр.) та екстериторіальні цифрові посольства фоормують модель, яка мінімізує технічні єдині точки відмови, усуває можливість прихованої маніпуляції державними даними, забезпечує безперервність державних функцій навіть у разі втрати частини території. Для України цей досвід може слугувати орієнтиром для інтеграції розподілених реєстрових архітектур, криптографічних механізмів фіксації правових записів та міжнародно-правових інструментів захисту даних у єдину НМС, орієнтовану на довготривале протистояння агресії та післявоєнну відбудову (таблиця 4.7).

Таблиця 4.7

Ключові елементи національної моделі стійкості Естонії

Елемент моделі	Ключовий зміст (з роками й документами)	Значення / уроки для НМС України
Загальний підхід Естонії до стійкості	Стійкість держави через «цифрову державу» як інфраструктуру виживання: послідовні стратегії «Digital Agenda 2020 for Estonia» (2013), Digital Agenda 2030 (з 2021 р.), кілька Cyber Security Strategy (2008–2013, 2014–2017, 2019–2022) інтегрують безперервність публічних послуг, кіберзахист і цифровий суверенітет	Приклад того, як цифрову трансформацію формалізують як основу НМС, а не як окремий сектор; в українських стратегіях стійкість теж має бути детермінована через цифрову, кібер і правову політику
X-Road (X-tee) як «цифровий хребет» держави	Платформа обміну даними X-Road (X-tee) розгорнута на нац.рівні з 2001 р.; описана в технічних та урядових документах RIA (Information System Authority) як базовий формат міждержавних інформаційних систем. Реєстри залишаються у відомствах, а X-Road забезпечує захищений, автентифікований, шифрований обмін	Модель, де обмін даними, а не «супер-реєстр», є ядром стійкості, для України це аргумент на користь розвитку «Трембіти» як стратегічного елемента НМС (а не тільки як тех.проєкту)
Відсутність єдиної точки відмови та принцип «опсе-only»	X-Road з 2001 р. реалізує розподілену архітектуру: кожне міністерство/агентство зберігає «свій» реєстр, немає «супербази». Принцип «опсе-only», закріплений у національній е-політиці та підтриманий Tallinn Declaration on eGovernment (2017), забороняє повторний запит уже наявних у держави даних. Це юридично змушує відомства користуватися X-Road, а не дублювати дані	Законодавче закріплення інтероперабельності (аналог «опсе-only») може стати для України правовим хребтом стійкості реєстрової моделі, змушуючи органи влади інтегруватися через формати обміну (Трембіта, інші шини), а не будувати ізольовані бази
Уроки кібернападів 2007 р. і поява KSI Blockchain	Після масованих кібератак 2007 р. Естонія ухвалила Estonian Cyber Security Strategy 2008–2013 (оновлена стратегіями 2014–2017, 2019–2022), CyberSecurity Strategy 2024–2030 «Cyber-Conscious Estonia», де одним із фокусів стала гарантована цілісність державних даних. На цій основі з 2008 р. у співпраці з Guardtime розгортається технологія KSI (Keyless Signature Infrastructure) Blockchain, яка з 2012 р. використовуються для державних систем	Показує, як криза (кібератаки 2007 р.) може стати тригером для інституціоналізації криптографічних гарантій стійкості. Для України це прецедент: елементи KSI-подібних рішень мають бути частиною не лише кіберстратегії, а й Національної моделі стійкості

Продовження таблиці 4.7

Елемент моделі	Ключовий зміст (з роками й документами)	Значення / уроки для НМС України
KSI Blockchain як математична гарантія незмінності реєстрів	KSI створює хеш-дерева для транзакцій і станів систем; кореневі хеші періодично фіксуються в глобальному реєстрі, публічно верифікованому. Впровадження з 2012 р. реєстру нерухомості, комерційного реєстру, судових рішень, e-Health та інших ключових систем, на основі документів Мінекономіки/Мін'юсту	Для України це модель «антифейку» та «антикорупції» – криптографічне фіксування історії записів (земля, бізнес, судові рішення, борги) уможливорює математичний доказ їх автентичності після деокупації й зменшує ризики внутрішніх маніпуляцій
Стратегічний фокус на цілісності даних у держполітиці	У стратегіях Cyber Security Strategy 2014–2017, 2019–2022 та в е-урядових програмах Естонія прямо фокусується не лише на конфіденційності та доступності, а й на незмінності (integrity) державних даних, де KSI і X-Road згадані як ключові інфраструктурні компоненти.	Підкреслює, що Національна модель стійкості України має окремо артикулювати цілісність реєстрів (integrity) як стратегічну мету, з конкретними технічними інструментами, а не лише захист доступності.
«Цифрові посольства» (Data Embassies) та угода з Люксембургом	Перше «цифрове посольство» реалізоване через Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems, підписану 20.06.2017 р., ратифіковану у 2018 р. Угода надає дата-центру в Люксембурзі спеціальний режим, близький до екстериторіальності, для розміщення естонських критичних систем і даних	Для України це модель юридичної інтеграції хмарних/закордонних бекапів у Національну модель стійкості: потрібні не лише технічні копії за кордоном, а й двосторонні угоди, що гарантують їхній суверенний статус
Data Embassies як рівень безперервності державності	Згідно з урядовими рішеннями 2017–2018 рр., критично важливі реєстри (населення, бізнес, податки, нерухомість тощо) безперервно реплікуються до «цифрового посольства» в Люксембурзі. У випадку фізичної окупації або знищення націнфраструктури держава може перезапустити цифрові функції з екстериторіального майданчика	Дас модель екстериторіальної стійкості держави: Україна може закріпити в Національній моделі стійкості створення «цифрових посольств» у дружніх державах як гарантію безперервності правового порядку й публічних сервісів навіть у випадку тимчасової втрати контролю над територією

Джерело: узагальнено автором за [371–373].

Модель Фінляндії показує, як національна стійкість вибудовується не лише через технологічну інфраструктуру, а передусім через концепцію всеосяжної безпеки (Comprehensive Security / Kokonaisturvallisuus) [374],

інституційну співпрацю держави й бізнесу та високий рівень суспільної довіри. Концепт «comprehensive security» закріплений у Security Strategy for Society 2010 та оновленій версії 2017 року (Yhteiskunnan turvallisuusstrategia), де прямо зазначено, що за безпеку відповідають уряд, бізнес, органи місцевого самоврядування, НУО, церкви, ЗМІ та громадяни [374]. Це фактично є національною моделлю стійкості, у якій цифрова, економічна, військова, інформаційна та соціальна складові розглядаються разом.

Національне агентство постачання в надзвичайних ситуаціях (NESA, Huoltovarmuuskeskus) [375] діє з початку 1990-х років на основі Закону про безпеку постачання (National Emergency Supply Act, 1390/1992) [376] і підпорядковується Міністерству економіки та зайнятості. Його завдання – забезпечити стійкість постачання (security of supply) в умовах криз, включно з енергією, транспортом, продовольством, фінансами та цифровою інфраструктурою. Особливістю NESA є модель фінансування: ключовим фінансовим інструментом є Національний фонд безпеки постачання (National Emergency Supply Fund), який наповнюється за рахунок цільових зборів (levies) на споживання енергії, палива та деяких інших товарів, а не з річного держбюджету. Це зафіксовано в Законі 1390/1992 та наступних змінах, а також у рішеннях уряду щодо цілей безпеки постачання, зокрема Government Decision on the Objectives of Security of Supply 1048/2018 [377]. Така схема забезпечує стабільне, майже «квазіринкове» фінансування стійкості, менш залежне від політичних циклів і поточних бюджетних пріоритетів.

З часом NESA розширила розуміння «резервів» від традиційних запасів зерна й палива до цифрової інфраструктури та кіберстійкості. У стратегічних документах та на практиці до об'єктів security of supply віднесено банки, телеком-операторів, логістичні компанії, дата-центри, мережі зв'язку, а також критичні цифрові послуги. Агентство фінансує: підвищення кіберстійкості критично важливих операторів (аудити, модернізація, резервування); спільні проекти з посилення надійності дата-центрів і мереж; навчання та моделювання кризових сценаріїв у цифровому середовищі.

Організаційною «фішкою» фінської моделі є галузеві «пули» (pools) у структурі Національної організації безпеки постачання (National Emergency Supply Organisation, NESO) [378], які координуються NESO. Існують, зокрема:

- Digital Pool / ICT Pool – для ІКТ-інфраструктури, операторів зв'язку, дата-центрів;
- Media Pool – для ЗМІ, телерадіомовників, великих цифрових платформ;
- інші галузеві пули (енергія, логістика, харчова промисловість тощо).

Таким чином, NESO та NESO перетворюють приватний сектор на структурний елемент національної моделі стійкості, формалізуючи партнерство через законодавство, стабільне фінансування та інституційні платформи взаємодії. Для України це дає кілька безпосередніх уроків. По-перше, стійкість критичної інфраструктури (енергетика, банки, телеком, логістика) має власну, захищену та передбачувану систему фінансування (наприклад, через спеціальні збори/фонди), а не лише річні бюджетні програми; по-друге, інтеграція бізнесу в Національну модель стійкості потребує формалізованих механізмів координації (аналог «пулів»), а не ад-гос робочих груп.

Важливим елементом фінської НМС виступає формування суспільної довіри та медіаграмотності як частини національної безпеки. Фінляндія стабільно посідає перші місця в Media Literacy Index, який вимірює стійкість до дезінформації в європейських країнах. Це не випадковість, а результат багаторічної політики. Фінська освітня система ще з реформ 2000-х років інтегрує медіаграмотність і критичне мислення в Національний базовий навчальний план (National Core Curriculum for Basic Education, 2014, оновлення 2016) [379]. Медіаосвіта присутня не як окремий «факультатив», а як горизонтальна компетентність у різних предметах: історія – аналіз джерел, пропаганди, історичних маніпуляцій; математика – робота зі статистикою,

графіками, критика «цифрових доказів»; мистецтво та мова – аналіз візуальних і текстових наративів, реклами, мемів. Координаційну роль відіграє, зокрема, Фінський національний аудіовізуальний інститут (KAVI), який разом із Міністерством освіти й культури публікує національні лінії політики з медіаграмотності (наприклад, «Media Literacy in Finland» 2013, оновлення 2019). Особливе місце посідає довіра як показник стійкості. У фінських дослідженнях та державних документах простежується чітка ідея – високий рівень довіри до інституцій і медіа знижує вразливість до криз та дезінформації. Зниження цих показників розглядається як індикатор вразливості національної безпеки, оскільки в умовах низької довіри легше поширюються ворожі наративи, теорії змови, відмова від колективних заходів безпеки. Таким чином, соціальний капітал, медіаграмотність і довіра стають для Фінляндії такими ж важливими елементами національної стійкості, як енергетичні резерви чи кіберзахист.

Для України цей досвід вказує, що медіаграмотність і критичне мислення повинні бути інтегровані в базові навчальні плани, а не існувати як розрізнені проекти; довіра до інституцій має розглядатися як одна з ключових метрик Національної моделі стійкості, з відповідною системою моніторингу й реагування (комунікаційна політика, реформа медіа, підзвітність) (таблиця 4.8).

Таблиця 4.8

Ключові елементи фінської національної моделі стійкості

Елемент моделі	Ключовий зміст (з роками й документами)	Значення / уроки для НМС України
Концепція «Всеосяжної безпеки» (Comprehensive Security)	Концепт kokonaisturvallisuus закріплено в Security Strategy for Society 2010 та оновленій 2017: за безпеку відповідають держава, бізнес, НУО, муніципалітети, ЗМІ та громадяни; безпека постачання, кібербезпека, інформаційна стійкість і довіра розглядаються разом	Модель, де НМС є системою спів-відповідальності, а не лише функція силових структур. Для України це означає необхідність офіційно «прошити» бізнес, ЗМІ та громадянське суспільство в архітектуру стійкості

Продовження таблиці 4.8

Елемент моделі	Ключовий зміст (з роками й документами)	Значення / уроки для НМС України
NESA та Закон про безпеку постачання (1390/1992)	National Emergency Supply Agency (NESA) діє на основі National Emergency Supply Act 1390/1992, координується Міністерством економіки та зайнятості. Її мандат у забезпеченні security of supply в умовах криз (енергія, транспорт, цифрова інфраструктура тощо)	Для України це приклад окремого органу, який системно відповідає за стійкість постачання, у т.ч. цифрового, на правовій основі з чітко визначеним мандатом
Фінансування через Національний фонд безпеки постачання	Ключовий фінансовий інструмент, National Emergency Supply Fund, що поповнюється за рахунок цільових зборів (levies) на споживання енергії, пального тощо, закріплених у Законі 1390/1992 та деталізованих в урядових рішеннях, зокрема Government Decision 1048/2018	Показує можливість створення стабільного, надбюджетного фінансування стійкості, менш залежного від політичних циклів, важливий орієнтир для української моделі фінансування критичної інфраструктури
Пули (Pools) у структурі NESO	У межах National Emergency Supply Organisation (NESO) створено галузеві «пули» (енергетичний, транспортний, Digital/ICT Pool, Media Pool тощо), що об'єднують державних службовців і приватні компанії, які планують спільні дії,	Прототип інституційних платформ співпраці з бізнесом, для України це аргумент за створення постійних «пулів» при органах, відповідальних за стійкість,
Розширення «стратегічних запасів» до цифрової інфраструктури	У документах уряду та NESA 2010-х років (включно з Government Decision 1048/2018) до об'єктів security of supply віднесено не лише фізичні ресурси, а також банки, телеком-мережі, дата-центри, цифрові сервіси, NESA фінансує кібер- та інфраструктурну стійкість	Закріплює ідею, що цифрова інфраструктура – це офіційно частина національних резервів, а не просто «ринкові послуги»; аналогічний статус мають отримати критичні ІТ-системи в Україні
Системна медіаграмотність у школі	National Core Curriculum for Basic Education 2014/2016 та політика «Media Literacy in Finland» (KAVI, 2013, 2019) інтегрують медіаграмотність і критичне мислення в усі рівні освіти, від дитячого садка до старшої школи	Показує, що когнітивна стійкість не може будуватися короткими кампаніями; Україні потрібна інтеграція медіаграмотності в національні стандарти освіти як частини НМС
Індекси медіаграмотності та довіри	Фінляндія стабільно посідає перші місця в Media Literacy Index (наприклад, 2018–2022), що пов'язується з високим рівнем медіаосвіти й довіри до інституцій. Державні й наукові інституції регулярно вимірюють довіру до уряду, парламенту, ЗМІ, експертів	Для України це сигнал, що рівень довіри й медіаграмотності має стати офіційним індикатором стійкості, із включенням у національну систему моніторингу безпеки та ризиків

Джерело: узагальнено автором за [374-379]

Ізраїльська національна модель стійкості особливо цінна для України саме зараз, оскільки вона сформувалася та щоденно перевіряється в умовах постійної військової загрози та активних бойових дій. Ізраїль, який із моменту створення держави (1948) пережив вісім повномасштабних війн, десятиліття терористичних атак і зараз перебуває в активній фазі бойових дій із ХАМАС (з жовтня 2023 р.), вибудував модель, де цифрова й фізична стійкість є невід’ємними складовими державної системи виживання нації.

Ізраїль одним із перших офіційно визнав кіберпростір окремим доменом бойових дій і національної безпеки. Уже в 2011 році було створено Israel National Cyber Bureau (INCB) при Канцелярії Прем’єр-міністра (Government Resolution 3611/2011), а в 2017–2018 роках його об’єднано з Israel Cyber Security Authority в Israel National Cyber Directorate (INCD) на основі урядових рішень Government Resolutions 2443 (2015) та 2444 (2016) [380]. INCD підпорядкований напряму Офісу Прем’єр-міністра, що відображає критичну важливість цифрової стійкості для національної безпеки в умовах воєнного стану. У «Israel’s Cybersecurity Strategy» (INCB/INCD, 2017) [381], розроблений з урахуванням військових загроз та досвіду попередніх конфліктів, кіберрезильєнтність визначається як здатність держави «витримувати, виявляти, реагувати і відновлюватися» від атак на всіх рівнях – від окремих організацій до національних систем. Саме тут закладається перехід від пасивного регулювання (стандарти, нагляд) до активної оборони національного масштабу, де держава сама будує захисні платформи. Для України, яка воює з агресором, що активно використовує кіберзасоби для доповнення конвенційних атак, цей досвід активного, а не реактивного підходу має першочергове значення.

Держава Ізраїль будує цифрову політику не як «ІТ-сектор», а як інфраструктуру виживання держави в умовах постійної війни. Після хвилі кібератак 2000-х, а особливо на тлі загроз з боку Ірану, проіранських угруповань та масованої агресії ХАМАС 7 жовтня 2023 року, кіберпростір фактично закріплено як бойовий домен нарівні з сушею, морем, повітрям і

космосом. Через це кібербезпека та цифрові технології інтегровані безпосередньо в національну модель стійкості: держава не просто встановлює правила, а будує активні захисні системи національного рівня і пов'язує їх з обороною, розвідкою та інноваційною екосистемою.

Інституційним центром є Israel National Cyber Directorate (INCD), створений шляхом посилення повноважень і об'єднання структур, започаткованих урядовими рішеннями Government Resolution 3611 (2011), 2443 (2015) і 2444 (2016) [380]. INCD напряму підпорядкований Прем'єр-міністру й відповідає за цивільну кіберстійкість у зв'язці з силами оборони. На цьому фундаменті сформована концепція «Кіберкуполу» (Cyber Dome), публічно представлена INCD у 2022–2023 роках за аналогією з протиракетною системою Iron Dome (в експлуатації з 2011 р.). У воєнних умовах Ізраїлю Cyber Dome це:

- 1) національна платформа активного захисту, а не просто набір рекомендацій;
- 2) інструмент, який має запобігти паралічу критичної інфраструктури під час масованих кібератак, синхронізованих із ракетними ударами чи терактами;
- 3) ключовий компонент перебудови оборони після 7 жовтня 2023 р., коли стало очевидно, що атаки одночасно відбуваються і в фізичному, і в цифровому просторі [381].

Структурні елементи Cyber Dome: по-перше, централізована аналітика (Big Data Fusion), телеметрія з урядових систем і критичної інфраструктури (енергетика, вода, транспорт, фінанси, охорона здоров'я) інтегруються в єдину аналітичну платформу. Це дозволяє бачити національні патерни атак, які окрема організація не помітить; виявляти скоординовані операції супротивника у реальному часі; розгортати контрзаходи синхронно по всій країні. По-друге, Protective DNS (PDNS), Національний сервіс захищеного DNS, розгорнутий INCD у 2020-х роках, блокує звернення до відомих шкідливих доменів (фішинг, C2) на рівні DNS-запитів. При цьому уряд

декларує намір надавати PDNS як безкоштовну «парасольку» для всіх операторів критичної інфраструктури, адже їх кіберстійкість прямо впливає на здатність країни вести війну.

По-третє, AI-реагування – Cyber Dome використовує алгоритми ШІ для:

- 1) автоматичного виявлення аномалій у поведінці мереж;
- 2) кореляції подій між секторами й регіонами;
- 3) автоматичного генерування та розповсюдження правил блокування (оновлення фаєрволів, DNS-фільтрів, IDS/IPS) [382].

У стані війни, коли кібератаки можуть іти хвилями, швидкість реагування стає критичною: людські команди фізично не встигають, отже, машинне реагування – це не «опція інновацій», а умова виживання. Таким чином, «Кіберкупол» – це національний бар'єр цифрової сфери, без якого класична військова оборона стає вразливою до паралічу енергосистем, транспорту, фінансів. Після угод 2020 р. Ізраїль спільно з ОАЕ та іншими партнерами ініціював створення платформи «Crystal Ball» – спільної системи обміну даними про кіберзагрози [383]. У логіці національної стійкості Ізраїлю це:

- 1) продовження оборони за межі кордонів: атаки, зафіксовані на інфраструктурі партнера, одразу стають відомими Ізраїлю;
- 2) спосіб зменшити «ефект несподіванки» з боку таких акторів, як Іран чи транснаціональні хакерські угруповання;
- 3) інструмент закріплення Ізраїлю як центру кіберекосистеми регіону, що отримує і надає критичні розвіддані.

Постійна загроза військового конфлікту змусила Ізраїль сформувати унікальну модель, де національна безпека, інновації та економічний розвиток інтегровані в єдину екосистему. У місті Беер-Шева (Negev) було створено кластер CyberSpark, який об'єднав військових, дослідників та підприємців. Ключову роль тут відіграв досвід бойових дій, який показав, що швидкість трансформації досвіду в технології є критичним фактором стійкості.

Офіційно ініціатива CyberSpark Industry Initiative стартувала у 2014 році після військової операції «Непорушна скеля», яка продемонструвала зростаючу роль кібердомену в сучасній війні. Ця модель забезпечує безпрецедентно короткий цикл від «поля бою до інновації»: військові підрозділи виявляють нові методи атак противника під час реальних бойових дій; стартапи та лабораторії швидко створюють контрзаходи, часто за декілька тижнів чи навіть днів [383].

Для України цей досвід особливо цінний, оскільки він демонструє, як бойовий досвід може стати драйвером інновацій та національної стійкості. Україна має унікальну можливість розробити власну модель, що трансформує досвід реальної війни з Росією у технології, які: посилять оборонні спроможності України; стануть «експортним продуктом» для посилення міжнародної підтримки; сформують основу для повоєнного розвитку кібер- та оборонного секторів. Особливо важливим аспектом ізраїльської моделі, що сформований саме досвідом війни, є глибока інтеграція фізичної та цифрової стійкості. Під час останніх конфліктів із ХАМАС та Хезболлою (2021, 2023–2024) фізичні атаки майже завжди супроводжувалися кібератаками на критичну інфраструктуру, особливо на енергетику, водопостачання та систему оповіщення населення. Ізраїль відповів на ці виклики формуванням цілісної системи захисту, де цифрова стійкість розглядається як прямий елемент національної безпеки:

- 1) фізичні системи раннього попередження про ракетні атаки (Red Alert) інтегровані з цифровими платформами оповіщення;
- 2) системи управління критичною інфраструктурою мають підвищений рівень кіберзахисту та автономності;
- 3) населення тренується діяти за сценаріями, коли кібератаки ускладнюють фізичну евакуацію чи реагування.

Ключові елементи ізраїльської національної моделі стійкості в умовах війни узагальнено у таблиці 4.9.

Таблиця 4.9

Ключові елементи ізраїльської національної моделі стійкості в умовах війни

Елемент моделі	Ключовий зміст (з роками й документами)	Значення / уроки для Національної моделі стійкості України в умовах війни
Інституційна структура НМС з прямим підпорядкуванням вищому керівництву	Israel National Cyber Bureau (INCB) створено урядовим рішенням Government Resolution 3611/2011 при Офісі ПМ; у 2017–2018 рр. трансформовано в INCD (National Cyber Directorate), що забезпечило єдину координацію під час військових загроз	Необхідність стратегічного рівня управління стійкістю з прямим доступом до вищого керівництва держави – критично важливий елемент для України, де координація органів в умовах війни часто розмита між різними відомствами
Національна кіберстратегія як компонент воєнної доктрини	У «Israel's Cybersecurity Strategy» (2017), розроблений з урахуванням досвіду військових конфліктів (2012, 2014), цифрова стійкість визначена як невід'ємна складова національної безпеки і військового потенціалу	Демонструє необхідність явного включення цифрової стійкості у воєнну доктрину України, а не лише в окремі «цифрові» чи «кібер»-стратегії, що особливо актуально в умовах затяжної війни
«Кіберкупол» (Cyber Dome) як система активної оборони національного масштабу	INCD у 2022–2023 рр. розгорнув Cyber Dome як відповідь на комбіновані атаки під час військових операцій, аналогічно до ПРО Iron Dome, яка захищає від фізичних ракетних ударів	Для України це модель централізованої системи захисту, що поєднує фізичну та цифрову оборону, особливо актуальна в умовах, коли РФ синхронізує ракетні удари з кібератаками на критичну інфраструктуру
Інтеграція даних про загрози в умовах війни	Cyber Dome агрегує й аналізує в режимі реального часу телеметрію безпеки з військових і цивільних систем, що дозволяє прогнозувати нові атаки, особливо напередодні військових операцій, що підтвердилося під час конфлікту 2023–2024 рр.	Для України критично важливо розвивати національну систему збору та аналізу індикаторів кібератак, що допоможе завчасно виявляти підготовку нових наступальних операцій противника
AI-реагування та автоматизація захисту як елемент військової готовності	Після досвіду конфліктів 2014 та 2021 рр., де було виявлено критичну роль швидкості реакції, в Ізраїлі впроваджено системи, де AI автоматично блокує нові вектори атак без людського втручання	В умовах масованих і координованих російських атак Україна потребує аналогічних систем автоматичного реагування на кіберзагрози з мінімальною залежністю від людського фактору, особливо для захисту критичної інфраструктури
Міжнародні коаліції як посилення стійкості воюючої держави	Платформа «Crystal Ball», особливо активізована в контексті війни з ХАМАС (2023–2024), перетворює двостороннє та багатостороннє співробітництво в реальні механізми раннього попередження та колективного захисту	Для України, що протистоїть агресії, участь у подібних альянсах або створення власної коаліції цифрової стійкості дозволить поєднати захисні ресурси та отримувати ранню інформацію про нові тактики противника
CyberSpark: перетворення бойового досвіду на технологічні інновації	Кластер CyberSpark, створений після військових операцій 2012–2014 рр., об'єднує військових (Unit 8200), академічний сектор та індустрію для швидкої трансформації бойового досвіду в конкретні технології захисту	Україна може створити аналогічну екосистему, де унікальний досвід протидії російській агресії трансформується у технологічні рішення, що зміцнюють оборону, стають експортним продуктом і основою для повоєнного розвитку
Комплексна інтеграція фізичної та цифрової стійкості	Під час конфліктів з ХАМАС та Хезболлою (особливо 2021, 2023–2024) Ізраїль вибудував систему, дефізична безпека (оповіщення, укриття) інтегрована з цифровою, а населення тренується діяти в умовах комбінованих атак	Для України особливо важливо забезпечити інтегровану стійкість цивільного захисту та цифрових систем, зокрема системи оповіщення, координації рятувальних служб та управління критичною інфраструктурою в умовах комбінованих фізичних і кібератак

Джерело: узагальнено автором за [380–383]

Досвід Ізраїлю демонструє, що справді ефективна національна модель стійкості формується в умовах реальних загроз і постійно вдосконалюється на основі аналізу бойового досвіду. Для України, яка веде активну фазу війни з потужним противником, ізраїльський досвід не просто корисний – він критично необхідний для побудови такої моделі стійкості, яка забезпечить виживання держави і суспільства як у поточній війні, так і в умовах довгострокового протистояння.

Порівняння розвинених демократичних країн демонструє спільну тенденцію – жодна ефективна НМС не є ані суто централізованою, ані суто децентралізованою. Успішні кейси – це різні варіанти гібридних моделей, у межах яких держава створює центральні інституції, платформи й стандарти, але стійкість «реалізується» через децентралізовані виконавчі структури, регіони, громади, бізнес і громадян. Так, США демонструють сильний центр (CISA, FedRAMP, DHS), який задає стандарти, здійснює координацію й будує національні платформи (наприклад, FedRAMP, CISA Protective DNS, програми спільного реагування JCDC), але реалізація стійкості розгортається через штати, місцеві органи, приватних провайдерів, які зберігають автономію.

Велика Британія поєднує централізований контроль (Cabinet Office, GDS/CDDO, Government Service Standard, spend controls) з розгалуженою мережею департаментів та агенцій, які самостійно впроваджують сервіси, але змушені «вписуватися» у єдину архітектурну і фінансову рамку. Естонія побудувала розподілену архітектуру (X-Road, KSI, data embassies), де реєстри та функції децентралізовані між відомствами, але поєднані жорсткими правовими та технічними стандартами інтероперабельності – фактично це центральна логіка в децентралізованому виконанні. Фінляндія реалізує модель «всеосяжної безпеки» (Comprehensive Security), де держава створює рамкові стратегії (Security Strategy for Society), а NESO/NESO інституціоналізує співпрацю з бізнесом (галузеві «пули»), перетворюючи приватний сектор на структурний елемент національної стійкості.

Ізраїль, що живе в умовах перманентної війни, поєднує надцентралізоване стратегічне управління (INCD при офісі Прем'єр-міністра, Cyber Dome як національна захисна платформа) з високим рівнем децентралізованої інноваційної активності (кластер CyberSpark, стартап-екосистема, приватні R&D-центри), які постійно підживлюють оборонну й кіберстійкість новими рішеннями.

Цей порівняльний матеріал дозволяє посилити тезу про доцільність гібридної моделі управління в межах НМС для України. Вона має включати:

1) централізовані елементи: національні стандарти, єдині платформи (аналог британських spend controls, естонського X-Road, ізраїльського Cyber Dome), нормативне закріплення ролі цифрових платформ («Дія.Engine») як інфраструктури НМС;

2) децентралізовані елементи: стійкі громади, регіональні «сма́рт-резильє́нтні» стратегії, автономні (але взаємопов'язані) реєстри, локальні системи реагування;

3) крос-інституційну співпрацю: постійні платформи взаємодії з бізнесом і НУО (аналог фінських «пулів» чи ізраїльського CyberSpark);

4) розвиток цифрових компетентностей держслужбовців і цифрову інклюзію громад – як необхідну умову того, щоб гібридна модель працювала не лише «на папері», а в повсякденному управлінні.

На основі досвіду згаданих країн авторська концепція «раціональної інформаційної стабільності» логічно постає як інтегральний механізм НМС 3.0, що поєднує: когнітивну безпеку (захист свідомості, критичне мислення, стійкість до дезінформації); адаптацію до викликів цифровізації (управління ризиками ШІ, платформ, алгоритмів, кіберзагроз); збереження національної ідентичності (культурний, історичний та ціннісний вимір у цифровому середовищі).

Наведені у дисертації зарубіжні практики підтверджують, що інформаційна стабільність неможлива як «статичний стан»; вона завжди є результатом раціонально керованих процесів – від освіти й комунікацій до

технічної інфраструктури та міжнародної співпраці. Саме в цьому сенсі «раціональна інформаційна стабільність» виступає модулем НМС 3.0, який оперує «м'якими» (когнітивними, культурними) і «жорсткими» (технічними, правовими) інструментами одночасно.

На засадах аналізу зарубіжного досвіду у дисертації пропонується 5 ключових елементів моделі «раціональної інформаційної стабільності» НМС – 1) когнітивна діагностика, 2) управління інформаційними потоками, 3) освітня інтеграція, 4) соціально-культурна адаптація, 5) стратегічне управління ризиками – корелюють із практиками розглянутих країн і можуть розглядатися як інституціональний дизайн НМС 3.0. Очевидно, що у провідних державах когнітивний вимір безпеки стає предметом системного аналізу. Так, Фінляндія й низка країн Північної Європи регулярно оцінюють рівень довіри, стійкість до дезінформації, медіаграмотність населення як показники нацбезпеки. Велика Британія та США інституалізували підрозділи, що аналізують інформаційні операції, ворожі наративи, впливові кампанії. Ізраїль, у стані війни, безперервно моніторить інформаційне поле (традиційні й соціальні медіа) для виявлення як ворожих, так і панічних, деморалізуючих наративів. Отже, для України когнітивна діагностика має включати:

- постійний моніторинг національного та регіональних інформаційних середовищ;
- виявлення ключових вразливостей (тем страху, розколу, недовіри);
- оцінку впливу ворожих операцій на поведінку громад і службовців.

Це створює базу для раціональних (даних-орієнтованих) рішень щодо інформаційних інтервенцій і комунікаційних стратегій.

У контексті збройної агресії РФ проти України когнітивний вимір безпеки перестає бути другорядною темою і перетворюється на один із ключових фронтів війни. Україна стикається не лише з регулярними ракетними ударами та наземними операціями, а й з постійними інформаційно-психологічними атаками, спрямованими на деморалізацію

суспільства, посіяний розкол, підрив довіри до інституцій, дискредитацію Збройних Сил України, волонтерського руху та міжнародних партнерів. У цих умовах когнітивна діагностика має стати системною державною функцією, інтегрованою в загальну Національну модель стійкості, а не набором епізодичних реакцій на черговий «інформаційний привід».

Для України досвід Фінляндії, Великої Британії, США та Ізраїлю важливий не як «готові рецепти», а як підтвердження того, що провідні держави стабільно розглядають довіру, сприйняття загроз, стійкість до дезінформації та поведінкові реакції громадян як такі самі критичні показники безпеки, як стан ППО чи резервів енергоносіїв. Фінляндія послідовно вимірює рівень довіри до інституцій, медіаграмотність та здатність суспільства протистояти дезінформації, і трактує погіршення цих показників як фактор національної вразливості. Велика Британія та США інституціоналізували підрозділи, що постійно аналізують ворожі інформаційні операції та наративи, а Ізраїль у стані війни фактично веде безперервний оперативний моніторинг інформаційного поля, відстежуючи як відверто ворожі меседжі, так і хвилі паніки, втоми, розчарування. Для України, що воює з противником, чия доктрина системно спирається на інформаційно-психологічні операції, все це не теорія, а безпосередня практична необхідність.

Першим виміром когнітивної діагностики як ланки НМС в українських умовах є детермінація базових принципів. По-перше, принцип системності – сприйняття, емоції, наративи та поведінка людей мають вимірюватися не від випадку до випадку, а в режимі безперервного процесу, інтегрованого в цикл прийняття управлінських рішень. По-друге, принцип науковості й дано-орієнтованості – оцінка стану суспільних настроїв та впливу ворожих операцій має ґрунтуватися на поєднанні соціології, психології, лінгвістичного та мережевого аналізу, а не на інтуїції чи політичних враженнях. По-третє, принцип багаторівневості – важливо не лише бачити середньостатистичні показники, а й розуміти відмінності між фронтовими,

прифронтовими, деокупованими, тилowymi регіонами, між різними соціальними групами – військовими, родинами загиблих і поранених, ВПО, підприємцями, молоддю, старшими людьми. По-четверте, принцип інтеграції з безпековими та управлінськими контурами – результати когнітивної діагностики повинні безпосередньо впливати на рішення уряду, військово-політичного керівництва, місцевої влади, комунікаційних штабів, а не залишатися «звітами в шухляді».

У практичному вимірі це означає, що Україна потребує постійного моніторингу національного й регіональних інформаційних середовищ, який поєднував би автоматизований аналіз медіа та соцмереж, репрезентативні опитування і глибинні дослідження. Йдеться не лише про відстеження ключових наративів, що поширюються у телевізійному просторі чи великих онлайн-медіа, а й про системне спостереження за тим, що відбувається у регіональних медіа, локальних Telegram-каналах, Facebook-спільнотах, TikTok та інших платформах, де формується щоденний інформаційний фон мільйонів людей. Умовно кажучи, важливо не тільки знати, що пишуть «центральні» канали, а й розуміти, що насправді думають і обговорюють люди у невеликому місті на лінії фронту чи в деокупованому селі, де рівень тривоги, недовіри чи втоми може бути критично вищим.

Другий вимір когнітивної діагностики – виявлення ключових вразливостей, тобто «нервів», на які найсильніше тиснуть ворожі інформаційні операції. В українському контексті такими вразливостями є, зокрема, теми страху (масовані обстріли, загроза ядерної ескалації, енергетичний колапс), розколу (протиставлення «фронту» і «тилу», «влади» і «волонтерів», різних регіонів і соціальних груп), недовіри (до рішень військово-політичного керівництва, до використання міжнародної допомоги, до судової та правоохоронної систем). Систематичний аналіз інформаційного поля та результатів опитувань має дозволити будувати своєрідну карту цих вразливостей: де і з яких причин накопичується недовіра, які саме події й наративи запускають хвилі паніки чи агресії, які групи населення є найбільш

чутливими до певних типів повідомлень. Це дає змогу не лише вчасно фіксувати точку напруження, а й розуміти її структурні причини – від реальних управлінських помилок до цілеспрямованих ворожих кампаній.

Третій критичний компонент – оцінка впливу ворожих інформаційних операцій на поведінку громад і службовців. Для країни, що воює, важливо не просто знати, що «зросла кількість негативних коментарів у соцмережах», а розуміти, як це відбивається на конкретних діях людей.

1. Чи впливають інформаційні кампанії противника на готовність громадян дотримуватися правил безпеки, йти в укриття, виконувати вимоги евакуації, платити податки, підтримувати мобілізаційні заходи, працювати в критичних сферах?

2. Чи призводить систематична дискредитація органів влади до саботажу чи пасивного опору серед держслужбовців на центральному й місцевому рівнях?

3. Чи мають таргетовані операції проти військових і їхніх родин помітний ефект на боєздатність підрозділів, повернення резервістів, моральний стан фронту? Відповіді на ці питання мають ґрунтуватися не лише на враженнях командирів чи чиновників, а й на зіставленні даних моніторингу інформаційного поля, соціології, внутрішніх управлінських індикаторів і «жорстких» показників (рівень явки, дисциплінарні порушення, виконання планів тощо).

Когнітивна діагностика в умовах протидії російській агресії повинна також мати низку властивостей, без яких вона перетворюється на формальність. Вона має бути безперервною, а не акційною, чутливою до регіональних та соціокультурних відмінностей, здатною швидко оновлювати свої моделі з урахуванням нових тактик противника. Вона повинна бути мультисекторальною: до її здійснення мають бути залучені не лише державні органи, а й наукові установи, професійні соціологічні служби, незалежні медіа-аналітичні центри. Водночас критично важливою є етичність: аналіз когнітивного виміру не може використовуватися як інструмент політичних

переслідувань чи придушення легітимної критики, інакше це саме по собі стає джерелом недовіри та вразливості.

У результаті саме налагоджена когнітивна діагностика створює базу для раціональних, дано-орієнтованих рішень у сфері інформаційної політики та стратегічних комунікацій. Вона дозволяє переходити від інтуїтивних, реактивних кроків – «дати спростування», «оголосити кампанію», «змінити тональність» – до виважених інтервенцій, побудованих на чіткому розумінні того, де саме і чому система є вразливою, як виглядає «нормальний» і «критичний» стан суспільних настроїв, які саме заходи (зміна комунікацій, управлінські рішення, підтримка конкретних груп) реально знижують ризики, а які – ні. Для України, що одночасно воює, проходить глибоку цифрову трансформацію та готується до повоєнного відновлення, така когнітивна діагностика є не додатковим «аналітичним сервісом», а обов'язковим елементом Національної моделі стійкості, без якого неможливо ні утримати довіру й суб'єктність суспільства в умовах тривалої війни, ні забезпечити легітимність і ефективність майбутніх рішень у період відбудови.

Коли когнітивна діагностика побудована за тими принципами, які застосовують Фінляндія, Велика Британія, США чи Ізраїль, вона перетворює суб'єктивні враження на керовані показники. Йдеться не про те, що «здається, люди панікують», а про те, що на основі вимірювань зафіксовано: у конкретних регіонах рівень тривоги, недовіри чи втоми зріс на певний відсоток. Така об'єктивація стану суспільних настроїв дозволяє дивитися на інформацію так само раціонально, як на економічні чи військові показники.

За наявності якісної когнітивної діагностики держава отримує змогу пріоритезувати інформаційні інтервенції там, де вони справді потрібні. Це дає підстави обґрунтовано змінювати тональність, формат або зміст офіційних комунікацій, виходячи з реальної картини настроїв, а не з політичних міркувань чи ситуативного тиску. Водночас стає можливим оцінювати ефективність уже проведених кампаній: що саме спрацювало, які групи населення відреагували очікуваним чином, де комунікації не досягли

мети або навіть мали побічні негативні ефекти.

Ще одна ключова функція полягає в тому, що когнітивна діагностика забезпечує чіткий зв'язок між інформаційною політикою та реальною поведінкою населення й службовців. Аналітика дає змогу простежити, як зміна наративів, повідомлень і каналів комунікації впливає на готовність людей дотримуватися правил безпеки, виконувати рішення органів влади, підтримувати оборонні зусилля. На цій основі стає можливою побудова сценарного планування: моделювання того, як можуть змінитися настрої та поведінка різних груп у разі тих чи інших подій, рішень чи інформаційних атак. У такому розумінні когнітивна діагностика перестає бути простим «моніторингом медіа» і перетворюється на повноцінну аналітичну підсистему НМС. Без неї будь-які комунікаційні стратегії залишаються здебільшого інтуїтивними й реактивними, тоді як завдання воюючої держави – діяти на основі даних, передбачення й проактивного управління суспільними настроями.

2. *Управління інформаційними потоками як складник НМС* в умовах війни є питанням виживання держави, збереження довіри й керованості суспільства. управління інформаційними потоками відповідає на запитання, яку саме інформацію, в якій формі, у якій послідовності й від кого отримують громадяни, військові, бізнес, місцева влада та міжнародні партнери. Цей складник визначає, чи сприйматимуться рішення держави як зрозумілі й легітимні, чи інформаційний простір буде заповнений чутками, ворожими вкидами та взаємовиключними повідомленнями.

Досвід Фінляндії, Великої Британії, США й Ізраїлю показує, що ефективне управління інформаційними потоками не «піар» і не хаотичні пресрелізи, а окрема, добре організована підсистема національної безпеки. Фінляндія, спираючись на концепцію всеосяжної безпеки, підтримує стабільну екосистему публічних комунікацій: сильний суспільний мовник, чіткі протоколи кризового інформування, довгострокове формування культури прозорості влади. Велика Британія через урядову комунікаційну

службу й стандарти (Government Communication Service, Government Service Standard) забезпечує узгодженість послань різних відомств і чіткі правила поведінки в кризах: хто, коли і що говорить громадянам, як коригуються повідомлення з урахуванням нових даних. У США структури на кшталт FEMA, DHS, CDC використовують стандартизовані протоколи кризових повідомлень, єдині платформи оповіщення, механізми Joint Information Center для узгодження меседжів між різними органами влади. Ізраїль у стані постійної війни показує, наскільки критичною є оперативна, точна й синхронізована комунікація між Армією оборони Ізраїлю, урядом, Службою тилу (Home Front Command) та місцевими органами влади: від повітряних тривог і вказівок населенню до пояснення ходу операцій і помилок.

4.5. Модель «раціональної інформаційної стабільності» як інтегральний механізм забезпечення НМС 3.0

Для України, яка перебуває в умовах повномасштабної агресії та постійних комбінованих ударів (ракетних, дронів, інформаційно-психологічних), управління інформаційними потоками має стати структурованою функцією НМС, а не розпорошеною активністю окремих відомств і каналів. Ключова проблема нині є фрагментарність, коли паралельні й часом суперечливі заяви різних посадовців; затримки з офіційним підтвердженням подій, які вже кілька годин розміщені у Telegram; перевантаження людей негативними новинами без пояснення контексту й дій; недостатня координація між центральними й місцевими комунікаціями.

Ключовою рамкою для розуміння цього складника є триада: прозорість, об'єктивність і своєчасність інформації.

Прозорість означає, що держава не просто повідомляє сухі факти, а пояснює логіку власних рішень, критерії пріоритетів, можливі ризики й обмеження. В українському контексті це, зокрема, стосується питань мобілізації, відбудови, розподілу міжнародної допомоги, енергетичної

безпеки. Коли рішення виглядають для людей як «несподівані накази згори» без пояснення, чому вони потрібні і які альтернативи розглядалися, виникає ґрунт для підозр, чуток і конспірологічних версій, які противник охоче підхоплює та підсилює. Натомість прозорість, навіть якщо йдеться про непопулярні кроки, створює відчуття поваги до громадян і зменшує «інформаційний вакуум».

Об'єктивність інформаційних потоків означає опору на перевірені дані, чітке розмежування фактів, оцінок і припущень, а також узгодженість повідомлень між різними державними інституціями. Для воюючої України це особливо чутливе питання. Тому стандарти об'єктивності мають включати уніфіковані формати статистичної звітності (для того, щоб МОУ, Офіс Президента України, обласні військові адміністрації не публікували взаємовиключних цифр), процедури верифікації інформації перед публікацією, встановлені правила виправлення помилок (коли початкові дані виявились неточними через стрес чи хаос першої години). Важливо також, щоб офіційні спікери чітко позначали, де вони говорять про підтверджені факти, а де висловлюють оціночні судження чи прогнози.

Своєчасність є третьою невід'ємною складовою. В українських реаліях вона часто виявляється критичнішою за формальну повноту інформації. Управління інформаційними потоками має будуватися на принципі: оперативне базове повідомлення – із чіткою вказівкою, що інформація попередня й буде уточнюватися, – а потім регулярні оновлення з конкретними часовими рамками. Так діють, наприклад, американські служби під час природних катастроф, а ізраїльські структури – під час масованих обстрілів: спочатку – короткий сигнал «це сталося, такі дії безпеки, чого очікувати далі», згодом – розгорнуте пояснення. Управління інформаційними потоками в рамках НМС має спиратися на низку принципів, які роблять прозорість, об'єктивність і своєчасність не деклараціями, а практикою.

Головний з таких принципів – *єдність інформаційної рамки*. Це не означає цензуру чи уніфікацію всіх висловлювань, але означає, що щодо

базових питань (цілі війни, пріоритети оборони, стратегія відбудови) публічні сигнали від різних органів влади не можуть бути взаємовиключними. Для цього необхідна координація на найвищому рівні – умовно, «центр тяжіння» комунікацій, який узгоджує ключові меседжі між Офісом Президента України, урядом, парламентом, сектором безпеки й оборони.

Другий принцип – *проактивність*. Держава не повинна чекати, поки противник запусить чергову кампанію, щоб «спростовувати фейки». Значна частина того, що сьогодні використовується у ворожих операціях, – це не вигадані з нуля історії, а реальні проблеми й прогалини, які просто інтерпретуються максимально руйнівно. Проактивне управління інформаційними потоками означає, що влада заздалегідь інформує про складні рішення, визнає вразливі місця, пояснює, що робиться для їх усунення, демонструє проміжні результати. У такому разі ворожим вкиданням складніше закріпитися, адже вони не потрапляють у повний вакуум інформації.

Третій принцип – *багаторівневість і локальна адаптація*. Загальнонаціональні повідомлення мають транслюватися не як універсальний шаблон, а з урахуванням специфіки регіонів, громад і цільових груп. Для цього потрібні налагоджені інформаційні потоки не лише «зверху вниз» (із центру до регіонів), а й «знизу вгору» – коли місцева влада, волонтерські мережі, лідери думок передають у центр інформацію про те, як насправді сприймаються загальнонаціональні меседжі й які додаткові роз'яснення потрібні.

Четвертий принцип – *інклюзивність і доступність*. В умовах війни особливо вразливими є люди з інвалідністю, літні, внутрішньо переміщені особи, мешканці сільських територій із поганим інтернетом. Інформаційні потоки мають бути налаштовані так, щоб критична інформація (тривоги, інструкції, зміни правил) доходила до них не лише через сучасні цифрові канали, а й через традиційні: радіо, локальні газети, оголошення, громади,

церковні структури тощо. Це потребує технічного й організаційного резервування каналів: одночасне використання кількох незалежних шляхів доставки повідомлень, щоб у разі руйнування частини інфраструктури інформаційний зв'язок не переривався.

П'ятий принцип – *вимірюваність і зворотний зв'язок*. Як і когнітивна діагностика, управління інформаційними потоками має спиратися на дані: наскільки швидко й повно повідомлення досягають аудиторій, як вони розуміються, чи відповідають їм реальні дії людей. Це означає регулярне відстеження охоплення (але не лише «лайків»), аналіз помилкових інтерпретацій, проведення опитувань щодо того, чи знають люди про ті чи інші рішення та як вони їх сприймають. На основі цього зворотного зв'язку мають коригуватися як зміст, так і формати комунікацій.

Якщо ці принципи реалізовані, управління інформаційними потоками поступово набуває властивостей повноцінної системної підсистеми НМС. Воно стає безперервним, а не епізодичним; координованим, а не хаотичним; підзвітним і керованим, а не розмитим між «усі говорять про все». Усередині держави це означає налагоджені канали обміну інформацією між міністерствами, силовими структурами, органами місцевого самоврядування, які дозволяють приймати рішення, ґрунтуючись на актуальних даних, а не на здогадках або медіашумах. У відносинах «державна – суспільство» це означає сталі відчуття в громадян, що їх інформують чесно, своєчасно й шанобливо, навіть коли новини важкі. У тісному зв'язку з когнітивною діагностикою така система управління інформаційними потоками створює основу для раціонального, даними підкріпленого управління суспільними настроями.

Важливим напрямом аналізу є *освітня інтеграція в межах моделі «раціональної інформаційної стабільності»* як наскрізна інтеграція процесу формування інформаційної грамотності й критичного мислення в усі рівні й формати освіти та підготовки професійних кадрів. Завдання освітньої інтеграції – перетворити суспільство з пасивного споживача інформації на спільноту громадян, здатних усвідомлено сприймати, перевіряти,

інтерпретувати й використовувати інформацію, особливо в умовах війни, масованої дезінформації та швидкої цифрової трансформації. У контексті НМС освітня інтеграція виконує подвійну функцію. З одного боку, вона формує індивідуальний «когнітивний імунітет» – здатність кожної людини розпізнавати маніпуляції, відрізняти факти від оціночних суджень, не піддаватися паніці й конспірології. З іншого – створює культурну норму суспільства у сфері національної стійкості, у якій критичне ставлення до інформації, відповідальність за її поширення й повага до фактів стають звичними, а не елітарними практиками. Це безпосередньо посилює когнітивну безпеку та підтримує інші елементи моделі НМС – когнітивну діагностику й управління інформаційними потоками, робить їх більш ефективними.

У межах авторської дослідницької моделі НМС варто виділити кілька ключових вимірів освітньої інтеграції. По-перше, це *системна інтеграція в формальну освіту* – від школи до університету. На шкільному рівні йдеться не лише про вставлення тем з медіаграмотності в один із предметів, а про наскрізний підхід: уміння працювати з джерелами інформації, розуміння базових принципів роботи медіа, соціальних мереж, алгоритмів рекомендацій має формуватися на уроках мови й літератури, історії, громадянської освіти, інформатики. У закладах професійної й вищої освіти це доповнюється розумінням інформаційних операцій, механізмів пропаганди, етичних аспектів створення й поширення контенту, основ цифрової безпеки. По-друге, критичний блок освітньої інтеграції – *це підготовка та перенавчання державних службовців і посадових осіб місцевого самоврядування*. У межах моделі стійкості вони не можуть залишатися «звичайними користувачами» інформації, а виступають вже як суб'єкти управлінських і комунікаційних рішень, і від їхньої здатності розуміти інформаційні ризики, відрізняти ворожі вкидання від легітимної критики, правильно реагувати на інформаційні кризи залежить як ефективність державного управління, так і рівень довіри до інституцій. По-третє, освітня інтеграція *виходить за межі*

формальної системи освіти й апарату управління, охоплюючи неформальну й інформальну освіту дорослих. У країні, яка протидіє агресії, значна частина населення вже завершила формальне навчання, але щоденно перебуває в зоні інформаційного ураження: у стрічках соцмереж, месенджерах, локальних спільнотах. Тому важливим завданням є створення доступних форматів навчання для широких груп – онлайн-курсів, інтерактивних тренінгів, інформаційних кампаній. Окремо можна виділити роботу з вразливими групами – старшими людьми, внутрішньо переміщеними особами, мешканцями деокупованих територій, для яких базові навички роботи з цифровими сервісами та критичного сприйняття онлайн-контенту стають елементом безпеки, а не лише «комфорту».

Четвертий важливий компонент – *методична та кадрова база освітньої інтеграції.* Неможливо сформувати інформаційну грамотність і критичне мислення «на папері», якщо вчителі, викладачі, тренери самі не володіють цими навичками, не розуміють поточних інформаційних загроз або відчують страх працювати з «чутливими темами». Тому в межах моделі необхідні програми підготовки педагогів і тренерів, розробка якісних навчальних матеріалів, кейсів, симуляцій, які відображають реальний український досвід – від теми пропаганди до етичних дилем публічних комунікацій у воєнний час. Освітня інтеграція тут виступає не лише як зміст, а й як інституційна інфраструктура: мережі шкіл, університетів, центрів підвищення кваліфікації, громадських організацій, що спільно формують компетентності.

П'ятим виміром є *змістовний баланс між критичністю й відповідальністю.* Освітня інтеграція не має на меті виховати тотальний цинізм або автоматичну недовіру до будь-яких джерел. Її завдання – формувати зріле, а не руйнівне критичне мислення: готовність ставити запитання, вимагати доказів, співставляти джерела, але водночас усвідомлювати, що в умовах війни абсолютна відкритість даних неможлива, що існують безпекові обмеження, що відповідальність за поширення

інформації (навіть «для друзів» у закритому чаті) є реальною. У цьому сенсі освітня інтеграція слугує містком між когнітивною безпекою та збереженням національної ідентичності: вона вчить одночасно не вірити ворогові й уміти конструктивно критикувати своїх, не впадаючи в патерни «все брехня» чи «всі зрадники».

У структурі концепції *«раціональної інформаційної стабільності»* освітня інтеграція тісно взаємодіє з іншими елементами. Дані когнітивної діагностики показують, які саме групи населення є найбільш уразливими до певних наративів, де відбувається провал критичного мислення, які теми викликають найбільші емоційні реакції. Це дозволяє адаптувати освітні програми до реальних ризиків, а не до абстрактних уявлень. Управління інформаційними потоками, у свою чергу, задає практичний контекст для навчання: коли офіційні комунікації демонструють приклад прозорості, об'єктивності й своєчасності, освітні ініціативи можуть опиратися на них як на позитивні кейси, а не лише розбирати помилки й провали.

Загалом, освітня інтеграція в моделі *«раціональної інформаційної стабільності»* – це довгостроковий інвестиційний компонент НМС, який працює повільніше, ніж кризові комунікації чи оперативні інформаційні відповіді, але забезпечує набагато глибший ефект. Вона формує покоління громадян і управлінців, які сприймають інформаційні ризики як нормальну частину сучасного середовища, володіють інструментами їх розпізнавання й мінімізації, здатні підтримувати стійкість суспільства не лише завдяки зовнішньому захисту, а й завдяки внутрішній когнітивній і культурній готовності.

Слід також вказати на феномен соціально-культурної адаптації в межах моделі *«раціональної інформаційної стабільності»* – як системне цифрове відтворення, захист і популяризація національних цінностей, мови, історичної пам'яті й культурних практик. Адже завдання адаптації – зробити так, щоб українська ідентичність була живою й присутньою в цифровому середовищі, а не витіснялася агресивнішими або «зручнішими» чужими

наративами. В умовах війни та цифрової трансформації соціально-культурна адаптація виконує щонайменше три критичні функції: внутрішню згуртованість – закріплює відчуття «ми» як політичної й культурної спільноти, знижує уразливість до наративів про «штучність» чи «неспроможність» України; когнітивну безпеку – створює позитивне, стійке «тло» для сприйняття інформації: цінності, смисли та символи стають опорою, яка ускладнює маніпуляції страхом, ненавистю чи зневірою; зовнішню суб'єктність (soft power) – демонструє світу, що Україна – не лише територія війни, а повноцінна культура, яка має що запропонувати й чому заслуговує на підтримку (таблиця 4.10).

Таблиця 4.10

Порівняльний аналіз підходів до соціально-культурної адаптації

Параметр	Традиційний підхід	Цифровий підхід	Інтегрована модель в НМС 3.0
Відтворення історичної пам'яті	Фізичні музеї, архіви, монументи; обмежений доступ	Оцифрування матеріалів, віртуальні музеї, онлайн-архіви	Гібридний формат: цифрові двійники + фізичні об'єкти; дані захищені в розподіленій системі
Мовна політика	Регулювання вживання мови в офіційних документах та ЗМІ	Українізація інтерфейсів,	Розвиток "цифрової екосистеми української мови": штучний інтелект, контент-платформи, спільноти
Культурний контент	Професійні виробники; висока вартість; обмежена дистрибуція	Демократизація створення; нижча вартість; доступність будь-де	Стирання меж між професійним та аматорським; співтворчість; адаптивний контент
Робота з травматичним досвідом	Офіційні наративи; монументи; обмежені формати	Персональні історії; інтерактивні проекти; різноманітність форматів	«Мережа пам'яті» – поєднання офіційних і особистих наративів; інструменти колективного осмислення травми
Залучення громадян	Пасивне споживання; участь через формальні інституції	Активна співтворчість; низький поріг входу; зворотний зв'язок	Керована співтворчість: громадяни як співавтори національного наративу з інституційною підтримкою
Міжнародна репрезентація	Дипломатичні канали; культурні центри; обмежене охоплення	Глобальні платформи; мультимовність; масштабоване охоплення	Стратегічна цифрова дипломатія: таргетовані наративи для різних аудиторій; вимірюваний вплив
Інституційне забезпечення	Централізовані установи; повільні процеси; обмежені ресурси	Децентралізовані мережі; швидкість; масштабованість	Гібридна модель: інституційний каркас + мережеві спільноти; спільне фінансування; гнучке управління

Джерело: розроблено автором

Перший вимір соціально-культурної адаптації у межах НМС – це оцифрування та систематизація національної спадщини: архівів, музейних колекцій, усної історії, місцевої нематеріальної культури, традицій і практик різних регіонів. Це важливо не лише як «культурний проєкт», а як елемент стійкості, адже у разі фізичного знищення об'єктів цифрові копії зберігають пам'ять і можливість відновлення, а також стають базою для освітніх і комунікаційних проєктів.

Другий вимір – активна присутність українського культурного змісту в цифрових медіа та платформах, де люди щодня споживають інформацію. У межах моделі стійкості це не просто «розвиток культури», а створення альтернативи токсичному чи ворожому контенту. Коли у просторі є потужний пласт якісного українського продукту, людям менше потрібно «добирати» сенси з чужих (у т.ч. ворожих) джерел.

Для ефективного функціонування соціально-культурної адаптації в рамках моделі «раціональної інформаційної стабільності» необхідно дотримуватися системи принципів, які забезпечують її інтегрованість у загальну архітектуру National E-Resilience:

1) *принцип автентичності й достовірності* – культурний зміст, історія та традиції мають представлятися без викривлення, спрощення чи політичної кон'юнктури;

2) *принцип технологічної суверенності* – зберігання і поширення культурного контенту має спиратися на інфраструктуру, що не залежить повністю від закордонних платформ і може функціонувати автономно в умовах обмежень чи блокування;

3) *принцип інклюзивності та різноманітності* – цифрове відтворення культури має враховувати регіональні, етнічні та інші особливості української ідентичності, не зводячи її до спрощеної версії, але при цьому формуючи спільну рамку загальнонаціональної єдності;

4) *принцип діалогічності* – культурні наративи мають формуватися не як монолог держави, а як діалог між різними голосами та перспективами

всередині суспільства, створюючи простір для осмислення складних питань, а не нав'язування єдиної інтерпретації;

5) *принцип проактивної адаптації* – соціально-культурні практики повинні випереджати технологічні зміни, а не наздоганяти їх, своєчасно адаптуючи українську ідентичність до нових форматів і платформ, де формуються суспільні сенси;

6) *принцип резильєнтності культурної пам'яті* – ключові елементи національної пам'яті мають бути захищені через множинне резервне копіювання, розподілене зберігання та можливість відновлення навіть за умов знищення фізичних носіїв;

7) *принцип синергії між традицією та інновацією* – національні цінності й традиції мають не протиставлятися цифровому середовищу, а органічно інтегруватися в нього, створюючи нові культурні форми, що поєднують історичну тяглисть із сучасною креативністю.

Третій вимір соціально-культурної адаптації – повсякденні практики людей у соціальних мережах і онлайн-спільнотах. Це допомагає зняти відчуття «культурного споживача» і перетворити людей на співавторів цифрової української культури, що підвищує відчуття причетності й відповідальності. Окремий, дуже важливий блок – цифрове осмислення складних і травматичних тем. Соціально-культурна адаптація означає, що ці теми не замовчуються і не спрощуються до пропагандистських штампів, а осмислюються через численні формати з увагою до складності.

П'ятий вимір соціально-культурної адаптації – представлення української культури й ідентичності назовні, у глобальному цифровому просторі. У моделі стійкості це працює як зовнішній контур захисту від російських наративів. Чим більше світ знає й цінує українську культуру, тим складніше легітимізувати будь-які форми заперечення нашої суб'єктності.

Соціально-культурна адаптація в моделі «раціональної інформаційної стабільності» не існує окремо, а переплетена з іншими елементами: когнітивною діагностикою, яка виявляє вразливі зони; управлінням

інформаційними потоками, що забезпечує узгодженість наративів; освітньою інтеграцією, яка вбудовує культурну пам'ять в освіту; стратегічним управлінням ризиками, що готує сценарії реагування на кризи, пов'язані з атаками на символи й цінності.

Як наслідок, соціально-культурна адаптація стає опорною платформою НМС, задає базову систему координат екзистенційного розвитку (*«хто ми»*, *«що для нас важливо»*, *«чому ми боремося»*), у межах якої вже працюють інші інструменти забезпечення стійкості. У цьому сенсі соціально-культурна адаптація не є «галузевим» компонентом, відповідальність за який несе лише профільне міністерство, а інтегральною частиною National E-Resilience, що потребує координації зусиль держави, громадянського суспільства, креативних індустрій, технологічних компаній та освітніх інституцій.

Стратегічне управління ризиками в межах моделі «раціональної інформаційної стабільності» – це систематичний підхід до передбачення, оцінювання та підготовки до інформаційних криз і загроз, що включає сценарне прогнозування, розробку планів реагування, резервування комунікаційних каналів і створення гнучких протоколів дій. Цей елемент забезпечує перехід від реактивної до проактивної позиції в протидії інформаційним загрозам, що критично важливо для України в умовах тривалої російської агресії, гібридних атак і масштабної цифрової трансформації.

У контексті НМС стратегічне управління ризиками виконує три ключові функції: 1) прогностична функція – виявлення потенційних загроз і вразливостей до їхньої активації, що дозволяє спрямувати ресурси на запобігання, а не лише на подолання наслідків; 2) превентивна функція – створення багаторівневих систем захисту від інформаційних впливів, щоб мінімізувати їхній потенційний вплив на суспільство, економіку та безпеку; 3) відновлювальна функція – забезпечення швидкого відновлення інформаційних потоків і довіри після криз, зменшення «часу простою» управлінських систем і критичної інфраструктури (таблиця 4.11).

Таблиця 4.11

Порівняльний аналіз підходів до стратегічного управління
інформаційними ризиками

Параметр	Реактивний підхід	Тактичний підхід	Стратегічний підхід в НМС 3.0
Часовий вимір	Миттєве реагування на вже активні кризи; дії постфактум	Середньострокове планування (3-6 місяців); обмежене прогнозування	Довгострокове прогнозування (1-5 років); раннє виявлення; проактивне моделювання
Охоплення ризиків	Фокус на очевидних, публічних загрозах; пропускання латентних ризиків	Аналіз галузевих і видимих ризиків; обмежена увага до взаємозв'язків	Системний аналіз взаємопов'язаних ризиків; каскадні ефекти; трансграничні загрози
Координація дій	Ситуативна, часто неузгоджена; дублювання функцій	Координація в межах інституцій; обмежена між-відомча взаємодія	Інтегрована система: спільні протоколи, єдині центри прийняття рішень, чітка субординація
Підготовка ресурсів	Екстрене мобілізування ресурсів під час кризи; відсутність резервування	Базовий рівень резервування; недостатня гнучкість розподілу	Динамічне резервування ресурсів; контингентні плани; швидке перенаправлення
Навчання персоналу	Загальні інструктажі; відсутність планової підготовки	Періодичні навчання для відповідальних осіб	Систематичні симуляції; міжвідомчі тренування; оцінювання стійкості персоналу
Зворотний зв'язок	Обмежений аналіз уроків; повторення помилок	Внутрішні розбори після криз; обмежене впровадження змін	Систематичний аналіз досвіду; активна адаптація стратегій; інституціоналізоване навчання
Технологічна інтеграція	Мінімальне використання аналітичних інструментів	Часткова автоматизація моніторингу; обмежена аналітика	Інтегровані системи раннього попередження; ШІ-аналітика; «цифрові близнюки» для моделювання

Джерело: розроблено автором

У структурі стратегічного управління ризиками можна виділити кілька ключових екзистенційних вимірів реалізації НМС 3.0, що забезпечують повноцінне функціонування цього елемента в моделі «раціональної інформаційної стабільності».

Перший вимір – **системна ідентифікація та аналіз інформаційних ризиків в межах НМС**, комплексне виявлення потенційних загроз та вразливостей інформаційного простору, що включає: по-перше, створення

загальнодержавної таксономії інформаційних ризиків із деталізацією за джерелами (зовнішні/внутрішні), механізмами поширення (соціальні мережі, ЗМІ, месенджери), цільовими аудиторіями, потенційними наслідками; по-друге, міжвідомчу аналітику й аналіз нових тактик і технологій, що можуть бути використані для інформаційних атак (зокрема, *deepfakes*, алгоритмічні маніпуляції, таргетовані атаки); по-третє, секторальний аналіз вразливостей підсистем (оборона, енергетика, фінансова система, громадське здоров'я) до різних типів інформаційного впливу; по-четверте, з'ясування впливу інформаційних загроз на фізичну безпеку, критичну інфраструктуру, економічну й політичну стабільність. Отже, ідентифікація ризиків орієнтована на майбутні загрози та системні вразливості.

Другий вимір – **розробка й аналіз різноманітних сценаріїв розвитку інформаційних ситуацій**, серед яких: по-перше, найгірші сценарії (*worst-case scenarios*) – масштабні кібератаки з одночасною дезінформаційною кампанією; підробки стратегічних рішень, що можуть викликати паніку; по-друге, каскадні сценарії, що передбачали аналіз, як локальна інформаційна криза в одному секторі може поширитися на інші; по-третє, регіональні та локальні сценарії, які передбачають, як інформаційні атаки можуть бути адаптовані до особливостей різних регіонів України (прикордонні території, деокуповані райони, міста-мільйонники, сільські громади); по-четверте, темпоральні сценарії: прогнозування інформаційних загроз у різних часових горизонтах – від миттєвих криз до довгострокових кампаній з підриву довіри та національної ідентичності.

Важливо навести систему принципів стратегічного управління інформаційними ризиками

- 1) *принцип випереджувального реагування* – прогнозування та підготовка до інформаційних загроз до їх матеріалізації;
- 2) *принцип інституційної пам'яті* – систематичне документування досвіду подолання попередніх криз, збереження й доступність цих знань для нових управлінських команд;

3) *принцип гнучкої ієрархії* – чіткий розподіл відповідальності в умовах кризи, з можливістю прийняття рішень на нижчих рівнях, якщо вищі рівні недоступні або неспроможні діяти;

4) *принцип багаторівневого резервування* – створення резервних каналів зв'язку, джерел інформації, керівних структур, що можуть активуватися;

5) *принцип крос-секторальної координації* – узгодження планів реагування для уникнення суперечливих дій або дублювання функцій;

6) *принцип постійного навчання й адаптації*;

7) *принцип пропорційності* як відповідність заходів реагування масштабу та природі загрози, уникнення як недостатніх, так і надмірних реакцій.

Третій вимір стратегічного управління ризиками – **перетворення сценарних прогнозів на конкретні, операціоналізовані плани дій**, що включають: протоколи раннього реагування (ідентифікація початкових ознак інформаційної атаки), кризові комунікаційні плани для різних типів загроз; протоколи координації між різними органами державної влади, місцевого самоврядування, силовими структурами, бізнесом, медіа та громадянським суспільством у разі інформаційних криз; плани безперервності інформаційної діяльності (Information Continuity Plans).

Четвертий вимір – **створення резервних можливостей, які забезпечать стійкість інформаційних потоків під час криз**:

1) технічне резервування комунікаційних каналів, через використання альтернативних платформ для поширення офіційної інформації в разі недоступності основних, незалежні від інтернету засоби комунікації (радіо, друковані матеріали, SMS-оповіщення);

2) кадрове резервування на основі підготовки «другої лінії» спікерів, аналітиків, операторів комунікаційних систем, які можуть замінити основний склад у разі його недоступності;

3) контентне резервування на основі попередньої підготовки базових інформаційних матеріалів для типових кризових сценаріїв, шаблонів повідомлень, відеозвернень, інструкцій для населення;

4) міжнародне резервування через налагоджені канали комунікації із закордонними партнерами та медіа, які можуть бути задіяні для поширення правдивої інформації в разі блокування внутрішніх каналів.

П'ятий вимір стратегічного управління ризиками – **регулярна перевірка й удосконалення підготовлених планів**, що включає:

1) кросфункціональні симуляції інформаційних криз із залученням представників різних відомств, медіа, бізнесу та громадянського суспільства для відпрацювання спільних дій;

2) формування «red teaming» – груп експертів, які спеціально намагаються знайти слабкі місця в наявних планах захисту та протоколах реагування;

3) tabletop exercises для керівного складу з моделювання прийняття рішень у різних сценаріях інформаційних криз, а також технічні тестування резервних систем комунікації та інформування, включаючи перевірку їх доступності, потужності та захищеності.

При цьому важливо визначити ключові суперечності у стратегічному управлінні інформаційними ризиками:

1) *суперечність між централізацією та розподілом управління*, при цьому виклик полягає в побудові системи, де існує чіткий баланс між централізованим стратегічним управлінням і достатньою автономією локальних структур для прийняття рішень у кризових умовах;

2) *суперечність між прозорістю та безпекою*, що потребує диференційованого підходу до відкритості інформації, коли публічні версії загальних принципів для широкого використання, але захищені деталі конкретних процедур і технічних механізмів;

3) *суперечність між алгоритмізацією та креативною адаптацією*, адже баланс між детальними інструкціями та простором для адаптивних,

креативних рішень на місцях є одним із найскладніших викликів у стратегічному управлінні ризиками;

4) *суперечність між технократичним і соціальним підходами*. При цьому застосування методології НМС вказує, що існує тенденція зосереджуватися на технічних аспектах інформаційної безпеки (системи моніторингу, алгоритми виявлення фейків), недооцінюючи соціально-психологічні чинники поширення дезінформації та паніки. Водночас суто соціальний підхід може ігнорувати технологічну природу багатьох сучасних інформаційних загроз. Інтеграція технічних і соціальних компетенцій у командах з управління ризиками є ключем до подолання цієї суперечності;

5) *суперечність між підготовкою до відомих і невідомих загроз*. Більшість ресурсів спрямовується на захист від уже відомих типів інформаційних атак, тоді як найнебезпечнішими часто стають непередбачені, нові форми впливу. Надмірний акцент на підготовку до конкретних сценаріїв може призвести до відсутності загальної адаптивності системи. НМС дозволяє Вирішення полягає в розвитку не лише специфічних протоколів для відомих загроз, але й загальних принципів та інструментів гнучкого реагування на непередбачувані виклики.

Шостий вимір стратегічного управління ризиками – це **створення стійких інституціональних механізмів для активації компонентів НМС**, що забезпечується:

1) національними центрами оцінювання інформаційних ризиків і загроз, які здійснюють системний моніторинг, аналіз і прогнозування ситуації в інформаційному просторі;

2) міжвідомчими координаційними радами з управління інформаційними кризами, які забезпечують узгоджену роботу різних структур під час загроз;

3) регіональними та секторальними підрозділами, які адаптують загальнонаціональні плани до специфіки конкретних регіонів і галузей;

4) міжнародним партнерством з обміну інформацією про загрози, транскордонні інформаційні атаки та взаємну підтримки під час криз.

Узагальнення підходів до НМС 3.0 показано на рис. 4.3.

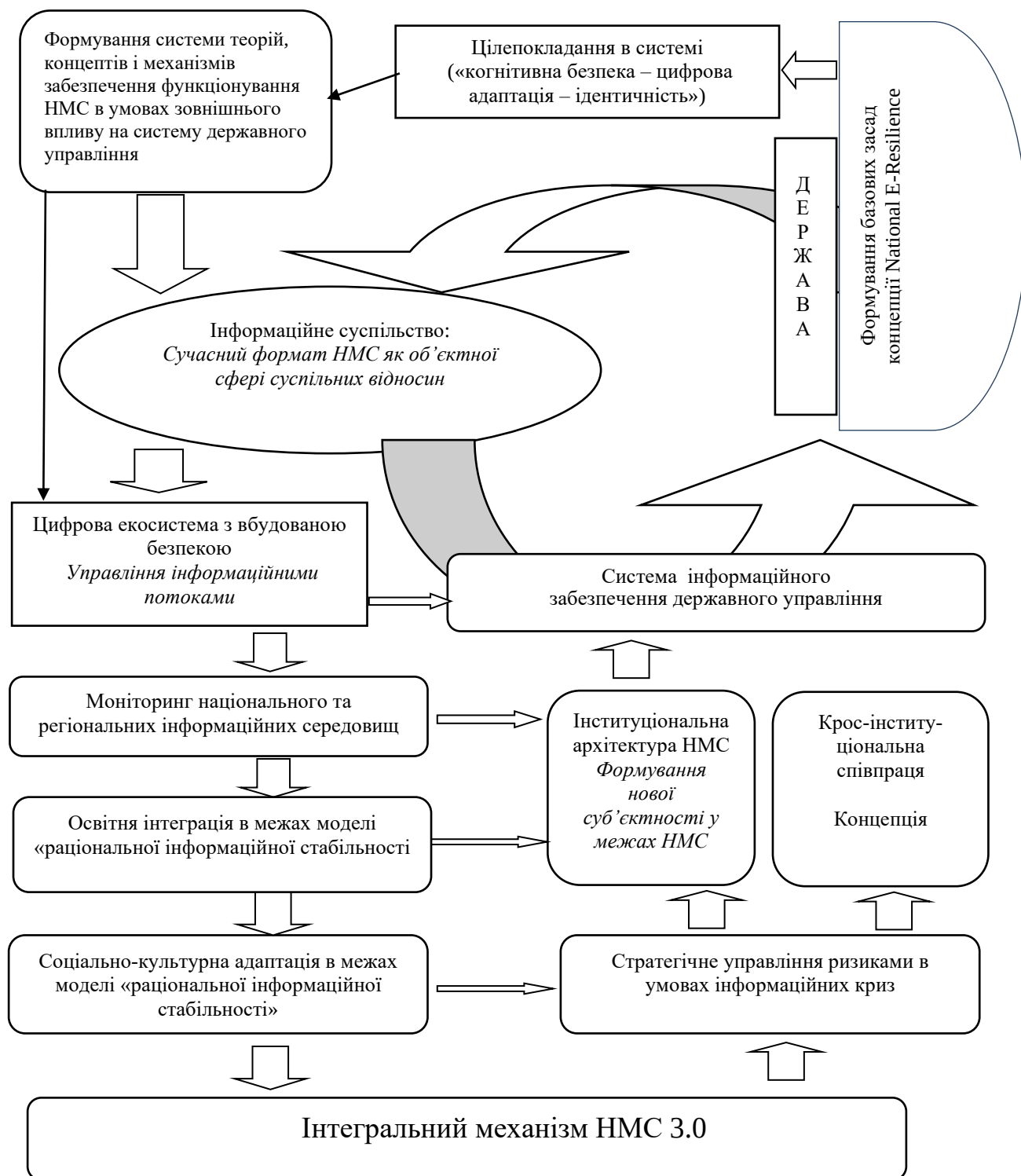


Рис. 4.3. Інтегральна гібридна модель управління стійкістю в межах National E-Resilience (НМС 3.0) на основі авторської концепції ««раціональної інформаційної стабільності»»

Проведене дослідження компонентів моделі «раціональної інформаційної стабільності» – когнітивної діагностики, управління інформаційними потоками, освітньої інтеграції, соціально-культурної адаптації та стратегічного управління ризикам – демонструє формування цілісної архітектури протидії інформаційним загрозам, яка виходить далеко за межі тактичних контрзаходів і становить фундаментальний елемент Національної моделі стійкості України.

Кожен із п'яти компонентів моделі відповідає за власний функціональний вимір: когнітивна діагностика забезпечує аналіз і моніторинг інформаційного середовища; управління інформаційними потоками гарантує прозорість, об'єктивність і своєчасність офіційної інформації; освітня інтеграція формує індивідуальний і суспільний «когнітивний імунітет»; соціально-культурна адаптація створює стійкі ціннісні та ідентичнісні опори; а стратегічне управління ризиками забезпечує готовність до майбутніх викликів. Водночас ці компоненти функціонують не ізольовано, а утворюють синергетичну систему з численними взаємопідсиленнями: діагностика скеровує інформаційні потоки; освітня інтеграція посилює ефективність культурної адаптації; стратегічне управління ризиками використовує дані всіх інших компонентів для прогнозування викликів.

Принципова цінність запропонованої моделі полягає в тому, що вона одночасно працює на трьох рівнях: індивідуальному (формуючи стійкість кожного громадянина до маніпуляцій), інституційному (вибудовуючи координовані механізми державно-приватної взаємодії) та загальносуспільному (створюючи спільний фундамент цінностей і критичного мислення). Така багаторівнева структура забезпечує не лише реактивну, але й проактивну відповідь на інформаційні загрози, трансформуючи вразливості на потенціал розвитку.

Для України в умовах російської агресії та одночасної цифрової трансформації модель «раціональної інформаційної стабільності» стає не

теоретичним конструктом, а практичним інструментом збереження державності та суб'єктності. Вона дозволяє протистояти не лише тактичним інформаційним атакам, а й стратегічним кампаніям з підриву національної ідентичності, довіри до інституцій і суспільної єдності. Імплементация цієї моделі в межах National E-Resilience створює передумови для сталого функціонування управлінських систем у воєнний час і забезпечує фундамент для когнітивної безпеки в процесі повоєнного відновлення.

Інтегральна гібридна модель управління стійкістю в межах National E-Resilience (НМС 3.0) на основі авторської концепції ««раціональної інформаційної стабільності» перетворює когнітивну діагностику, освітню інтеграцію, соціально-культурну адаптацію, управління потоками й стратегічне управління ризиками з декларативних функцій на динамічні, даними керовані процеси. Разом з тим, дана модель забезпечує проактивний характер стійкості: система не лише реагує на фактичні кризи, а завчасно спрямовує інформаційні, освітні та культурні ресурси в точки найбільшої потенційної уразливості. Загалом, це створює інтелектуальну інфраструктуру National E-Resilience, у якій кожен інформаційний сигнал, запит чи ризик потрапляє «правильною дорогою» – до відповідного адресата, каналу й рішення.

Висновки до розділу 4

1. НМС – це не сума окремих політик, а складна соціотехнічна «система систем». У розділі показано, що без цілісного архітектурного розуміння – як саме поєднуються цифрові платформи, інститути, нормативні механізми, когнітивні й інформаційні інструменти – будь-які точкові рішення дають лише фрагментарний ефект. НМС має проєктуватися й оцінюватися в логіці складної адаптивної системи, де кожен елемент впливає на інші й водночас постійно адаптується до змін середовища. Основою реалізації НМС є інтегрована національна цифрова платформа моніторингу. У авторській

концепції саме інтегрована національна цифрова платформа моніторингу є основою National E-Resilience. Саме ця платформа об'єднує дані від органів влади, сектору безпеки й оборони, місцевого самоврядування, громадянського суспільства та міжнародних партнерів, забезпечуючи обмін інформацією в режимі реального часу. Важливо не лише те, що вона збирає дані, а те, що її інструменти дозволяють оцінювати структурну готовність до криз, ступінь адаптації систем, ефективність відновлення й оперативно змінювати управлінські рішення. Так ідея National E-Resilience зі сфери концептів переведена у площину конкретної цифрової інфраструктури.

2. У розділі формалізовано раціональний алгоритм динамічного моніторингу НМС як послідовність чітко пов'язаних етапів. Принципово, що моніторинг не зводиться до «звітування», а працює як безперервний цикл. На першому етапі діагностуються загрози й виклики – війна, суспільна дестабілізація, інформаційна війна, руйнування інфраструктури. На другому здійснюються інтегрований збір та аналіз даних із використанням big data та мультиканальних джерел. Далі визначаються критичні індикатори стійкості: обороноздатність, соціальна довіра, доступ до критичної інфраструктури, стан інформаційної безпеки, обороноздатність, соціальна довіра, доступ до критичної інфраструктури, стан інформаційної безпеки. На цій основі здійснюється сценарне прогнозування та коригування стратегій. Таким чином, в умовах війни життєво необхідний єдиний, логічно вибудований підхід до моніторингу, який не лише фіксує проблеми, а й забезпечує адаптацію інституцій.

3. Запропоновано зміст «смарт резильєнтних регіональних стратегій» як ключового інструменту просторової диференціації НМС. Обґрунтовано, що стійкість неможливо забезпечити узагальненими показниками. Тому для кожного регіону запропоновано формувати окремий профіль ризиків і можливостей, враховуючи структуру економіки, демографію, природні загрози, культурний контекст. визначено, як цифрові моделі розвитку, геоінформаційні системи й смарт-технології управління інфраструктурою

дозволяють проєктувати сценарії криз і реагування саме на регіональному рівні. СРРС – це спосіб поєднати децентралізовану ініціативу регіонів із вертикальною координацією та горизонтальною співпрацею, а інтегрована регіонально чутлива платформа моніторингу виступає практичним інструментом такої взаємодії.

4. Структуровано механізми НМС у логіці компаративно-адаптаційної парадигми й на цій основі обґрунтовують модель «раціональної інформаційної стабільності» як інтегральний механізм НМС 3.0. На цій основі досліджено підходи у США, Великої Британії, Естонії, Фінляндії та Ізраїлю щодо «раціональної інформаційної стабільності», та виявлено структурні елементи, які можна адаптувати з огляду на українські воєнні реалії, гібридні загрози, цифрову нерівність і кризу довіри. На цій основі сформовано гібридну модель управління стійкістю, де централізовані й децентралізовані механізми доповнюють один одного. У межах цієї моделі концептуалізовано «раціональну інформаційну стабільність» із п'ятьма ключовими елементами – когнітивною діагностикою, управлінням інформаційними потоками, освітньою інтеграцією, соціально-культурною адаптацією та стратегічним управлінням ризиками – і показано, що саме їх синергія забезпечує не лише здатність протидіяти деструктивним впливам, а й основу для сталого функціонування й відновлення управлінських систем України в умовах війни та цифрової трансформації.

Основні результати дослідження, що наведені у цьому розділі, були опубліковані у фахових наукових виданнях галузі знань «Публічне управління і адміністрування» та включені до списку публікацій автора [2-4; 26-28; 43-45]

РОЗДІЛ 5

ЦИФРОВА РЕЗИЛЬЄНТНІСТЬ ДЕРЖАВИ Й СУСПІЛЬСТВА: КОНЦЕПЦІЇ,
УПРАВЛІНСЬКІ СТАНДАРТИ ТА ІНСТИТУЦІЙНІ МОДЕЛІ

5.1. Концептуалізація НМС в умовах війни та цифрової трансформації

Ефективна НМС в умовах війни та цифрової трансформації можлива лише за наявності інтегрованої цифрової інфраструктури моніторингу, смарт-резильєнтних регіональних стратегій і когнітивно-інформаційних механізмів стійкості, закріплених інституційно. На основі раціонального алгоритму моніторингу, архітектури єдиної національної платформи є можливість створити модель «раціональної інформаційної стабільності» як інтегрального механізму НМС 3.0. Однак на цьому етапі дослідження очевидним стає, що йдеться вже не лише про окремі інструменти чи підсистеми, а про нову якість стійкості, зумовлену цифровою природою сучасного державного управління, безпеки й суспільного розвитку.

Стрімкий розвиток цифрових технологій та інформаційного середовища зумовлює виникнення нових викликів для суспільної стійкості. Зростання обсягів інформаційного потоку підвищує значущість розробки ефективних моделей управління, здатних забезпечити когнітивну безпеку та адаптацію до змін. У цьому контексті модель «раціональної інформаційної стабільності» пропонує інноваційний підхід, що враховує вплив цифровізації на індивідуальне та колективне мислення.

Саме тому важливо перейти від аналізу окремих механізмів (моніторинг, інформаційна стабільність, смарт-резильєнтні регіональні стратегії) до узагальнення їх у глобальній рамці цифрової резильєнтності держави й суспільства. Якщо НМС описує загальну архітектуру стійкості, НМС 3.0 фокусує увагу на тому, як саме цифрові технології, дані та мережеві інститути змінюють природу вразливостей і можливостей, і які управлінські стандарти мають забезпечити не лише захищеність, а й адаптивний розвиток

у цьому середовищі. Такий підхід передбачає вирішення спеціальних завдань.

1. Необхідність концептуального узагальнення, адже цифрові платформи, алгоритмічний моніторинг, інформаційні механізми, смарт-стратегії регіонів стають критичними елементами стійкості, й тому виникає потреба узагальнити ці напрацювання у вигляді цілісної концепції цифрової резильєнтності, окреслити її категоріальний апарат, відмінність від класичних підходів до безпеки й стійкості, а також її місце в структурі НМС 3.0.

2. Потреба у формалізації управлінських стандартів – алгоритм моніторингу, модель Digital Resilience Assessment і концепція інтегрованої платформи вказують на те, що без узгоджених управлінських стандартів і процедур (як на національному, так і на регіональному рівнях) цифрова резильєнтність залишиться фрагментарною. Тому важливо визначити, які стандарти управління (принципи, протоколи, метрики, регламенти) є необхідними, щоб цифрова складова не просто підтримувала НМС, а стала її системоутворюючим елементом.

3. Інституційний вимір цифрової резильєнтності. Запропонована модель «раціональної інформаційної стабільності» та смарт-резильєнтні регіональні стратегії показують, що стійкість неможливо забезпечити винятково через технології – потрібні спеціалізовані інституційні моделі, здатні працювати в умовах гібридних загроз, високої невизначеності й швидкої зміни цифрового середовища. Отже, виникає завдання описати та порівняти можливі інституційні конфігурації цифрової резильєнтності: від національних центрів даних і кіберрезильєнтності до регіональних хабів стійкості, механізмів державно-приватного партнерства та участі громад.

Актуальність дослідження зумовлена необхідністю систематизації унікального українського досвіду, який демонструє перехід від статичних моделей захисту інформації (зокрема, застарілої системи КСЗІ) до динамічних екосистем National E-Resilience. Ця екосистема характеризується

здатністю державних інституцій не лише витримувати деструктивний вплив кінетичних та кібернетичних атак, але й адаптуватися до кризових умов, забезпечуючи безперервність надання публічних послуг та функціонування критичної інфраструктури. Розуміння природи цифрової стійкості в українському контексті вимагає чіткого розмежування між традиційним захистом інформації та комплексним поняттям резильєнтності, яке охоплює соціальні, управлінські та технологічні виміри.

Екосистема National E-Resilience розглядається як інтегроване середовище, що забезпечує циркуляцію даних між рівнями та секторами управління, перетворення цих даних на управлінські рішення та інституціоналізацію зворотного зв'язку між державою, суспільством і бізнесом. На відміну від класичної кібербезпеки, яка фокусується на периметрах захисту, екосистема E-Resilience орієнтована на безперервність процесів. Навіть за умови компрометації окремих вузлів чи фізичного знищення інфраструктури (дата-центрів), система повинна продовжувати виконувати критичні функції для громадян та сил оборони.

Сучасні безпекові виклики, з якими стикається Україна, демонструють принципову недостатність традиційних підходів до забезпечення стійкості держави та суспільства. Повномасштабне російське вторгнення, гібридні атаки на критичну інфраструктуру, масштабні кібероперації та інформаційно-психологічні кампанії, спрямовані на дезорганізацію управлінських процесів, відбуваються паралельно з прискореною цифровою трансформацією всіх сфер життєдіяльності. В цих умовах формується фундаментальне протиріччя: з одного боку, цифрові технології створюють нові вразливості й залежності, з іншого – саме вони стають ключовим інструментом підтримання функціональної безперервності держави та адаптивного управління кризами.

Наукова проблема полягає у відсутності цілісної концептуальної рамки, яка б дозволила інтегрувати розрізнені цифрові ініціативи в єдину архітектуру національної стійкості, що враховує багатовимірність взаємодій

між інфраструктурними, інституційними, когнітивними та соціальними компонентами в умовах високої невизначеності. Існуючі моделі переважно фокусуються або на кібербезпеці (захист цифрової інфраструктури від атак), або на цифровізації публічних послуг (підвищення їх доступності та якості), або на розвитку цифрової економіки (трансформація бізнес-моделей, підвищення конкурентоспроможності). Однак жоден з цих підходів не дає відповіді на ключове питання: як саме спроектувати та реалізувати таку цифрову екосистему, яка б забезпечувала не просто роботу окремих сервісів, а стійкість держави як системи в цілому – її здатність підтримувати критичні функції, відновлюватися після шоків і адаптуватися до нових загроз.

У межах даного дисертаційного дослідження (розділи 1-4) ми встановили, що National E-Resilience визначається як інтегрована національна модель управління, спрямована на забезпечення стійкості держави й суспільства в умовах цифровізації шляхом ефективного використання інформаційних технологій для об'єднання ресурсів, політик і процесів у єдину адаптивну систему, здатну передбачати загрози, витримувати шоки, відновлюватися після криз і трансформуватися для відповіді на нові виклики.

Ключові концептуальні відмінності пропонованої моделі National E-Resilience від наявних у науці державного управління підходів є розуміння таких властивостей: *інтегративності*, коли замість розрізнених секторальних підходів (кібербезпека, цифрове урядування, цифрова економіка) пропонується єдина архітектура, де ці елементи є взаємодоповнюючими компонентами спільної системи; *проактивності* – фокус не лише на реагуванні на кризи, а на формуванні передумов для завчасного виявлення загроз, сценарного планування та адаптивного управління; *соціотехнічному балансі* – коли однакова увага як до технологічної інфраструктури, так і до соціальних, культурних, інституційних факторів визначають ефективність використання моделі; *динамічності* як розумінні стійкості не лише у вигляді статичної характеристики, а і як безперервного процесу адаптації та навчання системи;

а також *децентралізованій відповідальності при стратегічній координації* – поєднанні вертикальних механізмів координації з горизонтальними мережами співпраці та локальною автономією.

Головним компонентом моделі National E-Resilience у дослідженні визначено централізовану цифрову управлінську платформу державного управління (C-eGovPro). Це не просто технологічне рішення, а інституціональний механізм, що забезпечує «єдину версію правди» для прийняття стратегічних рішень. Архітектура платформи базується на трьох функціональних рівнях, виявлених у ході дослідження: 1) рівні стратегічної обізнаності (Decision-Making Core), і в рамках National E-Resilience цей компонент відповідає за предиктивну аналітику та оперативне управління кризами; 2) рівні прозорого відновлення та управління ресурсами – екосистема DREAM (Digital Restoration Ecosystem for Accountable Management), яка інтегрує управління інвестиціями, забезпечує підзвітність та довіру донорів, що є критичним для економічної стійкості; 3) рівня інтероперабельності. Фундаментом централізації є не фізичне злиття баз даних (що небезпечно), а логічна інтеграція, що забезпечує безпечний обмін даними між реєстрами без створення єдиної точки відмови, що відповідає принципам стійкості.

В авторській доктрині National E-Resilience національна стійкість розглядається як керована екосистема, у якій усі ключові елементи державного управління, цифрової інфраструктури, інформаційних потоків та суспільної взаємодії об'єднані в єдиний динамічний контур. Йдеться не лише про опис статичної структури, а про побудову такої конфігурації держави й суспільства, де критичні функції здатні підтримуватися, відновлюватися й посилюватися завдяки безперервним циклам спостереження, оцінювання, корекції та адаптації. У цьому розумінні National E-Resilience задає цільову «архітектуру поведінки» держави в умовах війни, гібридних загроз і глибокої цифрової трансформації: держава має бачити свій стан і зовнішнє середовище, вимірювати відхилення від бажаних параметрів стійкості,

обираючи керуючі дії, перевіряти їх наслідки й постійно переналаштовувати власні механізми реагування.

Центральну роль у цій екосистемі відіграє інтегрована цифрова платформа державного управління, яку доцільно розглядати як операційну «нервову систему» та «центр керування» всієї моделі. Через неї здійснюється збір сигналів про стан різних підсистем держави – від оборонного сектору, енергетики й транспорту до соціальної сфери, інформаційного простору та локальної інфраструктури громад. Усі ці сигнали уніфікуються, нормалізуються та порівнюються з еталонними профілями функціонування, що дозволяє виявляти як різкі аномалії, так і повільні тренди деградації чи накопичення напруги в системі державного управління. Функціональну конфігурацію National E-Resilience можна узагальнити у вигляді матриці (табл. 5.1), де для кожного домену визначені ключові вхідні сигнали, типові керуючі дії й очікувані ефекти з погляду стійкості.

Таблиця 5.1

Матриця функціональних доменів National E-Resilience

Функціональний домен	Вхідні сигнали	Типові керуючі дії	Очікуваний ефект для стійкості
Документообіг та управлінські процеси	Запити, проекти рішень, погодження, доручення	Маршрутизація, прискорені процедури, визначення пріоритетів	Скорочення часу ухвалення рішень, прозорість трасування
Дані та реєстри	Оновлення записів, запити доступу, помилки	Валідація, синхронізація, обмеження/надання доступів	Цілісність і доступність критичних даних
Моніторинг та аналітика	Показники секторів, сенсори, звіти	Налаштування порогів, запуск аналітичних сценаріїв	Раннє виявлення відхилень і загроз
Кризове управління	Інциденти, сигнали тривоги, звернення регіонів	Активація планів, координація відомств, перерозподіл ресурсів	Синхронізоване реагування без конфлікту повноважень
Комунікація з населенням і бізнесом	Звернення громадян, реакції, зворотний зв'язок	Масові й таргетовані повідомлення, уточнення інструкцій	Зниження паніки, підвищення виконавчої дисципліни
Підзвітність та аудит	Логи, звіти, скарги, результати перевірок	Розслідування, коригувальні плани, оновлення регламентів	Попередження повторення помилок, підвищення довіри

Джерело: дослідження автора

Функціональна специфіка National E-Resilience полягає в тому, що вона від початку проєктується з урахуванням режимів кризового перевантаження, часткових відмов та агресивних впливів. Критичні сервіси й дані розміщуються у розподіленій архітектурі з дублюванням ключових вузлів, що дозволяє зберігати працездатність навіть у разі втрати окремих елементів. Умовно кажучи, система має бути здатною переходити в «режим обмеженої функціональності» без втрати базових можливостей управління державою. Для цього в платформі закладаються сценарії деградації з пріоритезацією найважливіших процесів: наприклад, у разі перевантаження або атак відбувається автоматичне обмеження другорядних функцій на користь підтримки каналів кризової координації, масового оповіщення населення, доступу до критичних реєстрів. Вбудовані механізми аналізу помилок, журналювання подій і тестових «прогонів» сценаріїв дозволяють після кожної кризової події уточнювати порогові значення спрацювання, коригувати налаштування пріоритетів, виявляти «вузькі місця» архітектури й усувати їх у плановому режимі.

Інституціональна архітектура адаптивного управління в межах National E-Resilience вибудовується так, щоби кожен важливий контур ухвалення рішень мав визначеного «власника», зрозумілі входи й виходи, а також формалізований зворотний зв'язок. Національний центр цифрової резильєнтності задає стратегічні орієнтири, формує еталонні моделі бажаного стану стійкості за основними напрямками, розробляє методики вимірювання й координує коригувальні дії. Галузеві центри цифрової трансформації, регіональні хаби стійкості та спеціалізовані команди швидкого реагування працюють як взаємопов'язані регулятори нижчого рівня, які отримують сигнали про відхилення в відповідній сфері, оцінюють локальні умови й застосовують доступні керуючі впливи – зміну режимів роботи об'єктів, активацію резервних планів, перерозподіл ресурсів, корекцію процедур тощо. Для забезпечення узгодженості дій такі регулятори розгортаються на різних часових горизонтах, формуючи багаторівневу систему реагування (табл. 5.2).

Таблиця 5.2

Багаторівнева система реагування у межах National E-Resilience

Рівень реагування	Орієнтовний часовий горизонт	Типові завдання	Основні відповідальні суб'єкти
Миттєвий	Секунди – хвилини	Відбиття атак, перемикавання каналів, аварійне вимкнення	Технічні команди, SOC, оператори інфраструктур
Оперативний	Години	Запуск планів реагування, локалізація інциденту	Штаби кризового реагування, галузеві центри
Тактичний	Дні	Перерозподіл ресурсів, тимчасові регулювання	Урядові структури, регіональні хаби стійкості
Стратегічний	Тижні – місяці	Корекція політик, оновлення пріоритетів	Національний центр, профільні міністерства
Структурний	Роки	Реформи інституцій, зміна архітектури систем	Парламент, уряд, вищі органи виконавчої влади
Культурно-ціннісний	Десятиліття, покоління	Зміна норм поведінки, укорінення культури стійкості	Освітні інституції, медіа, громадянське суспільство

Джерело: розроблено автором

Ключовим складником National E-Resilience є те, що вертикальні взаємозв'язки (від національного до локального рівня) і горизонтальні мережі співпраці (між регіонами, відомствами, секторами) не розглядаються як конкуренти, а як різні рівні єдиної системи. Замість жорсткої централізації чи повної децентралізації вводяться механізми, за яких загальнодержавні цілі та обмеження визначають межі для прийняття рішень, а регіональні та секторні структури мають простір для самостійного налаштування в цих межах. Особливе місце в доктрині резильєнтності займають когнітивно-інформаційні механізми стійкості, які забезпечують стабільність суспільства й інституцій. На рівні функціонування це означає наявність сталі діючих контурів спостереження за інформаційним простором, оцінки напруги, панічних настроїв, довіри до інститутів, поширення дезінформації, а також відповідних механізмів коригувального впливу через комунікацію, освіту, контрнаративи й прозоре пояснення рішень. Суспільство отримує сигнали про стан безпеки, ризиків, ресурсів, а держава – сигнали про довіру, задоволеність, рівень тривоги. Доктрина National E-Resilience передбачає, що такі відхилення не замовчуються, а виявляються через системний моніторинг

і перетворюються на привід для адаптації як змісту політик, так і їхнього комунікаційного супроводу. Масштабна інформаційна атака, спрямована на дискредитацію сектору оборони, відстежується не тільки за кількістю ворожих повідомлень, а й за зміною індикаторів довіри до відповідних інституцій, готовністю громадян виконувати вимоги безпеки, динамікою намірів мігрувати чи брати участь у волонтерських ініціативах. Якщо система фіксує критичне розходження між бажаним і фактичним рівнем цих показників, автоматично вмикаються сценарії стратегічних комунікацій, посилюється присутність відповідальних акторів у ключових каналах, оновлюються меседжі, запускаються освітні й пояснювальні кампанії.

Важливо, що когнітивно-інформаційні механізми стійкості не обмежуються реакцією на зовнішні впливи, а розгортаються як довгостроковий процес формування критичного мислення, цифрової грамотності й готовності громадян взаємодіяти з державою в осмислений спосіб. Це означає поступове зміщення акценту з “гасіння пожеж” на зменшення вразливості до деструктивних впливів як такої: через інтеграцію відповідних модулів у систему освіти, постійні практики фактчекінгу, участь громадян у моніторингу загроз, розвиток суспільного діалогу щодо складних питань державної політики. Сталі програми підвищення компетентностей, регулярні інформаційні тренування, симуляції криз із залученням громад і місцевих спільнот дозволяють перетворювати потенційно дестабілізуючі інформаційні події на керовані ситуації навчання.

Сутнісною рисою National E-Resilience є те, що всі описані компоненти не живуть окремим життям, а з’єднані у спільні цикли моніторингу, ухвалення рішень і корекції. Інформація про відхилення в технічному стані інфраструктури впливає на управлінські рішення щодо пріоритезації інвестицій і резервування потужностей; дані про зміну суспільних настроїв коригують стратегії комунікацій і зміст соціальних політик; результати аналізу кризових інцидентів зумовлюють оновлення нормативно-правових актів, стандартів безпеки, навчальних програм для держслужбовців. Кожна

така петля зворотного зв'язку має свою тривалість, “чутливість” до відхилень і набір допустимих керуючих дій. Там, де спостереження й реакція надто повільні, система ризикує впасти в затяжну кризу; там, де вони надто імпульсивні, виникає небезпека надмірних або неадекватних рішень, що породжують нові проблеми.

Саме тому авторська парадигма National E-Resilience передбачає поетапне налаштування цих контурів: від визначення цільових показників стійкості в різних сферах до встановлення допустимих меж коливань і частоти коригуючих втручань. У деяких сферах (наприклад, енергетика чи кібербезпека) важлива висока швидкість реакції на аномалії, в інших (соціальна політика, реформа інститутів) потрібні більш “інерційні” механізми, що працюють на довших горизонтах. У сукупності це формує багаторівневу систему, де швидкі контури стабілізують миттєві збурення, а повільні – спрямовують еволюцію системи в цілому, не допускаючи накопичення структурних дефектів. Отже, National E-Resilience описує не просто набір цифрових рішень чи інституційних реформ, а цілісну, багатопланову систему керованої стійкості, у якій спостереження, аналіз, ухвалення рішень, виконання й навчання з'єднані в безперервні та взаємопов'язані цикли. Завдяки цьому держава й суспільство набувають здатності не тільки витримувати удари, а й перетворювати кризи на імпульси для свідомої адаптації та розвитку, зменшуючи розрив між бажаними цілями й реальною поведінкою системи в умовах гібридних загроз і цифрової невизначеності.

Водночас, у дисертації розглядається можливість варіативного підходу до National E-Resilience, що передбачає можливість розвитку НМС в межах переходу від централізованої цифрової платформи та ієрархічної інституціональної архітектури може стати модель, у якій резильєнтність вибудовується не стільки навколо єдиного центру, скільки навколо високого рівня інтероперабельності між множиною розподілених суб'єктів, систем та процесів. National E-Resilience у такому випадку – це здатність величезної

кількості різнорідних елементів НМС швидко й надійно узгоджувати дії завдяки сумісності даних, сервісів, процедур і норм.

У класичній моделі National E-Resilience, наданих для формування НМС, у 2-4 розділах дисертації, робиться акцент на єдиній інтегрованій цифровій платформі як ядрі моделі; національному центрі координації; стандартизованих вертикальних контурах управління. Очевидно, що розвиток такої моделі на власних засадах передбачає (у контексті змісту принципу інтероперабельності передбачає зміщує акценту: по-перше, від «єдиної платформи» – до «єдиного цифрового простору взаємодії»; по-друге, від монолітної архітектури – до інтеграції систем і суб'єктів, пов'язаних через узгоджені стандарти; по-третє. від централізації функцій – до взаємозамінності й взаємодоповнюваності компонентів моделі. У такому форматі держава вже не буде один «універсальний цифровий центр», а створює рамкові умови та протоколи, за якими будь-яка система, що виконує суспільно важливу функцію, може бути підключена, зрозуміла й використана іншими – у тому числі в кризовому режимі.

National E-Resilience забезпечує здатність національної цифрової екосистеми забезпечувати безперервність і адаптивність критичних функцій завдяки високому рівню технічної, семантичної, організаційної та правової інтероперабельності між державними, приватними та громадськими системами й інститутами. Ключовими є три фактори:

- по-перше, резильєнтність виступає як функція зв'язків, а не лише потужності окремих підсистем НМС;
- по-друге, стійкість забезпечується тим, що будь-який збій в одному компоненті може бути компенсований іншими, оскільки: дані доступні за уніфікованими інтерфейсами; сервіси можуть бути викликані ззовні; організації розуміють формати, процедури й повноваження одна одної;
- по-третє, національна цифрова екосистема яка виступає як множина рівноправних суб'єктів., при цьому суб'єкти (органи влади, громади, бізнес, громадські організації, міжнародні партнери) не вбудовуються жорстко в

одну ієрархію, а під'єднуються до спільного інтероперабельнісного простору, поділяючи: технічні стандарти; моделі даних; протоколи обміну й реагування;

– по-четверте, акцент на «здатності взаємодіяти в кризі» як ключовому індикатору.

Отже, не критично важливо, наскільки розвинена окрема система, якщо вона не здатна швидко обмінюватися критичною інформацією й синхронізувати дії з іншими системами. При цьому важливо зробити наголос на зміні інституціонального дизайну, коли розуміння National E-Resilience можна побудувати навколо чотирьох взаємопов'язаних рівнів інтероперабельності:

1) технічна інтероперабельність – узгоджені протоколи передачі даних і повідомлень; стандартні API для державних і квазідержавних сервісів; єдині вимоги до безпеки каналів;

2) семантична інтероперабельність – спільні словники та онтології (як визначаються «інцидент», «об'єкт критичної інфраструктури», «ризик» тощо); уніфіковані моделі даних, класифікатори, кодові схеми; механізми трансформації даних між різними доменами (наприклад, безпека – енергетика – транспорт);

3) організаційна інтероперабельність – взаємно узгоджені ролі й повноваження між суб'єктами; регламентовані процедури спільного реагування (хто, за який сигнал, що робить); інституціональні мости» (спільні центри, контактні точки, кризові штаби);

4) правова та політична інтероперабельність – сумісні правові режими для обміну даними й спільних операцій; угоди про взаємне визнання цифрових підписів, реєстрів, статусів; відповідність міжнародним стандартам для транскордонної взаємодії.

У класичній моделі НМС такі підходи можуть розглядатися як «допоміжні» для роботи єдиної платформи. В інтероперабельній моделі – вони самі стають ядром резильєнтності, адже якщо кожен рівень

структурований і працює, система загалом здатна перетікати в нові конфігурації, навіть якщо окремі вузли виходять з ладу.

Фактично, ми пропонуємо в розвиток нашої концепції НМС розглядати концепт National E-Resilience як такий, що здатний до самоналаштування. Отже, коли виникає нова загроза (наприклад, комбінована кібератака й фізичний удар по енергетичній інфраструктурі), не потрібно створювати «ад-hoc» тимчасову систему обміну даними, адже різні оператори на основі мережевого підходу вже здатні: ділитися телеметрією за стандартними форматами; отримувати пріоритетні сигнали про критичні стани; надавати один одному резервні потужності.

Очевидно, що формування (реорганізація) органу влади, або запровадження нового цифрового сервісу потребує його інтеграції в екосистему НМС, що відбувається шляхом: підключення до національних реєстрів; імплементації стандартних API; прийняття спільних політик безпеки й реагування. Таким чином, нова структура НМС від початку є інтероперабельною, що зменшує проблеми при взаємодії та підвищує готовність системи до майбутніх, ще невідомих сценаріїв.

На цій основі у дисертації пропонується виділити чотири інтероперабельні рівні у межах концепту National E-Resilience, кожен з яких інтегрує різні сектори й інститути в системі державного управління та може стати окремим об'єктом діагностики в емпіричному дослідженні:

- 1) рівень спільних стандартів і профілів сумісності;
- 2) рівень інтероперабельних сервісів;
- 3) рівень спільних процедур реагування;
- 4) рівень довіри та сертифікації.

Такий підхід дозволяє узгодити теоретичну модель National E-Resilience з методикою вимірювання зрілості цифрової резильєнтності, що є ключовим завданням прикладного аналізу НМС. Реалізація моделі National E-Resilience у контексті проблематики державного управління вимагає, *по-перше*, наближення чотирьох рівнів інтероперабельності до реальних

суб'єктів публічної влади – центральних органів виконавчої влади, органів місцевого самоврядування, державних підприємств, регуляторів, органів секторної безпеки. *По-друге*, потребують чіткої кореляції з принципами National E-Resilience наявні інформаційні системи, нормативно-правові акти, результати реформ децентралізації, цифрової трансформації, антикризових рішень у період повномасштабної агресії РФ. Саме в цьому контексті чотири рівні інтеперабельності можна розглядати як практичний інструмент аналізу зрілості системи державного управління щодо здатності працювати в умовах кризи, війни та гібридних загроз.

Перший рівень – *рівень спільних стандартів і профілів сумісності* – у сфері державного управління проявляється насамперед через наявність (і реальне застосування) загальнообов'язкових вимог до інформаційних систем органів влади. Йдеться про нормативні акти Кабінету Міністрів України, накази Мінцифри, Держспецзв'язку, НБУ, які визначають: формати електронних документів та електронного підпису; вимоги до інтеграції через систему «Трембіта»; стандарти інформаційної безпеки та криптографічного захисту; мінімальні вимоги до відмовостійкості ІТ-інфраструктури. Емпірично цей рівень можна спостерігати, аналізуючи, чи використовуються єдині формати ідентифікації (ID-дані з реєстрів, Єдиний демографічний реєстр), чи дотримуються органи влади єдиних технічних умов під час закупівель інформаційних систем, чи прописуються у міжвідомчих угодах уніфіковані вимоги до безпеки й обміну даними. Наприклад, впровадження міжвідомчого електронного документообігу в більшості міністерств стало можливим саме тому, що були уніфіковані формати підпису (кваліфікований електронний підпис, КЕП), шифрування та протоколи обміну повідомленнями з системою електронної взаємодії органів виконавчої влади.

На практиці, однак, ступінь реального впровадження таких стандартів істотно різниться, адже частина центральних органів влади (насамперед у сферах безпеки, фінансів, цифрової трансформації) активно підтримує стандарти і закладає їх у технічні завдання, тоді як окремі регіональні органи

та малі громади продовжують розгортати локальні системи, орієнтовані лише на внутрішні потреби. Саме тому рівень спільних стандартів доцільно оцінювати через ключові індикатори: наявність у стратегічних і програмних документах згадок про конкретні національні профілі стандартів; ступінь їх формалізації у внутрішніх регламентах органів влади; частку ІТ-проектів, що прямо посилаються на ці стандарти в технічних завданнях; наявність механізмів моніторингу дотримання (аудити, перевірки Держспецзв'язку, внутрішній ІТ-контроль).

Другий рівень – *рівень інтероперабельних сервісів* – у системі державного управління в Україні уже частково матеріалізувався через впровадження спільних державних сервісів: системи «Трембіта» як шини обміну даними між реєстрами; платформу «Дія» як єдиний фронт-офіс для громадян і бізнесу; національні сервіси електронної ідентифікації (id.gov.ua, BankID НБУ), електронного підпису й печатки. Для органів державної влади ці сервіси є композиційними складниками – вони дозволяють будь-якому ЦОВВ, ОМС чи державному підприємству не створювати власні замкнені механізми автентифікації чи обміну даними, а підключатися до спільної інфраструктури, автоматично отримуючи можливість інтегруватися з іншими учасниками.

Саме завдяки розвитку таких інтероперабельних сервісів вдалося різко прискорити надання адміністративних послуг в електронній формі, забезпечити безперервність ключових сервісів (реєстрація ФОП, отримання довідок, соціальні виплати) навіть під час масованих ракетних ударів і блекаутів 2022–2024 років. У той же час спостерігаються значні відмінності: великі міста та «цифрові» міністерства (Мінцифра, Мін'юст, МВС) набагато краще інтегровані у спільні сервіси, ніж невеликі громади чи окремі галузеві органи (зокрема в охороні здоров'я та житлово-комунальному господарстві). Для державного управління це означає, що загальна резильєнтність залежить не тільки від наявності таких сервісів, а й від рівня охоплення ними різних ланок влади.

Щоб зробити оцінку більш системною, доцільно застосувати матрицю зрілості, у якій кожен із чотирьох рівнів інтероперабельності описується п'ятьма стадіями розвитку – від початкової до оптимізованої. Така матриця може слугувати основою як для самодіагностики органів влади, так і для міжсекторального порівняння (таблиця 5.3).

Таблиця 5.3

Матриця зрілості інтероперабельних рівнів у моделі National E-Resilience

Рівень інтер-операбельності	Початковий (1)	Базовий (2)	Стандартизований (3)	Керований (4)	Оптимізований (5)
Стандарти і профілі	Кожен орган використовує власні ІТ-вимоги, взаємодія – переважно через папір або ad hoc інтеграції	Ухвалено окремі стандарти (КЕП, обмін даними), але впровадження фрагментарне	Затверджені профілі стандартів обов'язкові для ЦОВВ, рекомендовані для ОМС; використовуються в ТЗ	Стандарти системно моніторяться, порушення виявляються аудитами, є плани усунення	Стандарти проактивно оновлюються за результатами інцидентів, навчань, узгоджуються з ЄС/НАТО
Інтер-операбельні сервіси	Локальні системи без підключення до Трембіти, власні механізми доступу	Використання окремих державних сервісів (КЕП, id.gov.ua), але без глибокої інтеграції	Переважна більшість органів підключені до Трембіти, застосовують спільні сервіси для ключових процесів	Забезпечено гарантований рівень доступності, резервування, тестування DR-сценаріїв	Існує набір взаємо-доповнюючих сервісів з можливістю динамічного перерозподілу навантаження
Спільні процедури	Формальні ПЛЛАСА/ПРНС є, але не враховують цифрову взаємодію	Є загальні інструкції реагування, проте без чітких цифрових сценаріїв	Розроблено та відпрацьовано цифрові сценарії для типових криз (кібератаки, блекауту, міграційні хвилі)	За підсумками реальних подій процедури коригуються, проводяться регулярні тренування	Адаптивні процедури, що автоматично оновлюються з урахуванням аналітики та прогностичних моделей
Довіра і сертифікація	Відсутні загальні критерії надійності ІТ-систем органів влади	Є мінімальні вимоги (атестати відповідності КСЗІ), але контроль нерегулярний	Діє формалізована процедура сертифікації й реєстр надійних систем та учасників	Застосовується багаторівнева модель доступу, постійний моніторинг, позапланові перевірки	Впроваджено ризик-орієнтовані моделі довіри з прогнозуванням і автоматизованими обмеженнями доступу

Джерело: розроблено автором

ПЛЛАСА – план локалізації і ліквідації аварійних ситуацій та аварій, більш «об'єктові» і конкретні (для підприємств, критичних об'єктів)

ПРНС – плани реагування/дій на надзвичайні ситуації, рамкові/узагальнені документи для органів влади й системи цивільного захисту.

Третій рівень – *рівень спільних процедур реагування* – у державному управлінні безпосередньо пов'язаний із практикою міжвідомчої координації в кризових ситуаціях. Під час масованих ракетних обстрілів енергетичної інфраструктури у 2022–2023 роках стало очевидно, що наявність навіть добре розгорнутих інформаційних систем не гарантує ефективного реагування без чітко прописаних і протестованих цифрових сценаріїв взаємодії. Там, де такі сценарії були – наприклад, у роботі Національного банку України з банківською системою щодо забезпечення безперервності платежів, або в координації Мінцифри, Держспецзв'язку та операторів мобільного зв'язку щодо розгортання мережі «Пунктів незламності» – вдалося відносно швидко налагодити обмін інформацією, пріоритизувати ресурси, мінімізувати соціальні наслідки. Натомість у сфері охорони здоров'я чи соціального захисту неодноразово фіксувалися затримки в оновленні даних, неузгодженість інтерпретацій показників, суперечливі сигнали для громадян через відсутність уніфікованих процедур і форматів міжвідомчих запитів.

Цей рівень може бути наповнений емпіричним змістом через аналіз реальних кризових кейсів: COVID-19, масове внутрішнє переміщення населення, евакуації, кібератаки на державні реєстри, масовані ракетні удари по об'єктах енергетики чи місцевого самоврядування. У більшості таких ситуацій очевидно, що формально затверджені «плани реагування» часто не містили деталізованих цифрових сценаріїв: не було визначено, які саме системи мають обмінятися якими саме даними, у які терміни, хто є відповідальним за валідацію інформації та прийняття рішень. Саме емпіричні уроки цих подій створюють підстави для посилення третього рівня – формування не тільки планів, а й «цифрових протоколів взаємодії», регулярних навчань, міжвідомчих тренувань із моделюванням кібератак та комбінованих загроз.

Четвертий рівень – *рівень довіри та сертифікації* – у сфері державного управління має дуальний характер. З одного боку, йдеться про технічну довіру до інформаційних систем органів влади (наявність атестатів КСЗІ,

проходження аудитів за стандартами ISO, участь у програмах bug bounty тощо). З іншого боку – про інституційну довіру між різними суб'єктами публічної влади та між державою й приватними постачальниками послуг (хмарні провайдери, оператори зв'язку, розробники програмного забезпечення). На основі аналізу відкритих урядових звітів, нормативних актів та експертних оцінок доцільно побудувати умовну програму розвитку чотирьох рівнів інтероперабельності (ІО) для різних груп суб'єктів державного управління, демонструє характерні диспропорції, з якими стикається українська система державного управління (таблиця 5.4).

Таблиця 5.4

Орієнтовні профілі ІО резильєнтності основних груп суб'єктів публічного управління (5-бальна шкала)

Рівень ІО	ЦОВВ у сфері безпеки та оборони	Економічні та фінансові ЦОВВ	Соціальна політика та охорона здоров'я (ЦОВВ)	ОМС великих міст	Малі громади (ОМС)
Стандарти і профілі	4 (керований)	3 (стандартизований)	2 (базовий)	3 (стандартизований)	1–2 (початковий/ базовий)
ІО сервіси	3 (стандартизований)	4 (керований)	2 (базовий)	3–4 (стандартизований/ керований)	2 (базовий)
Спільні процедури	4 (керований)	3 (стандартизований)	2 (базовий)	2–3 (базовий/ стандартизований)	1–2 (початковий/ базовий)
Довіра і сертифікація	4 (керований)	3 (стандартизований)	2 (базовий)	2–3 (базовий/ стандартизований)	1–2 (початковий/ базовий)

Джерело: розроблено автором

Прогнозні оцінки в таблиці 5.4 відображають кілька важливих емпіричних закономірностей. По-перше, органи безпеки та оборони (Міноборони, СБУ, ДПСУ, частково МВС) за рахунок багаторічної інтеграції з партнерами по НАТО, участі в міжнародних навчаннях і високих вимог до захищеності демонструють порівняно високий рівень за всіма чотирма рівнями ІО. Вони мають усталені стандарти, підключені до спільних сервісів, відпрацьовують процедури реагування на реальних кейсах, проходять регулярні перевірки та сертифікації.

По-друге, економічні та фінансові ЦОВВ (Мінфін, Мінекономіки, НБУ,

ДПС) значною мірою просунуті в частині ІО сервісів і стандартів завдяки вимогам до обслуговування великої кількості транзакцій, міжнародній звітності, інтеграції з банківським сектором та донорами. У них також краще, ніж у багатьох інших, розвинені механізми моніторингу й аудиту, хоча спільні кризові процедури часом залишаються недостатньо деталізованими (що проявлялося, зокрема, в перші місяці повномасштабної війни під час екстреного перегляду бюджетних програм і фінансових пріоритетів).

По-третє, сектор соціальної політики та охорони здоров'я, попри значний прогрес (eHealth, Єдина інформаційна система соціальної сфери, «ЄМалятко» тощо), усе ще має низькі показники як щодо впровадження єдиних стандартів, так і щодо сформованих спільних процедур реагування. Під час пандемії COVID-19 та на початку повномасштабної війни фіксувалися труднощі зі своєчасною передачею даних між медичними закладами, НСЗУ, органами соціального захисту, що безпосередньо впливало на швидкість прийняття управлінських рішень (карантинні обмеження, перерозподіл ліжко-місць, призначення виплат).

По-четверте, великі міські ОМС (Київ, обласні центри) завдяки наявності власних ІТ-команд, залученню донорської допомоги, участі в проєктах «Смарт-сіті» та програмі «Дія.Цифрова громада» значно краще інтегровані у спільні сервіси й стандарти, ніж малі громади. Однак навіть у них спостерігається фрагментарність спільних процедур: цифрова взаємодія з ЦОВВ у кризових сценаріях часто залежить від неформальних контактів, а не від чітко прописаних протоколів. Малі громади ж часто знаходяться на початкових або базових рівнях: мають поодинокі цифрові рішення (сайт, система документообігу), але не інтегровані системно в національний інтероперабельний простір.

Інтероперабельна модель National E-Resilience, адаптована до системи державного управління України, демонструє, що НМС держави в умовах війни й гібридних загроз визначається не стільки наявністю окремих передових ІТ-рішень, скільки узгодженістю чотирьох взаємопов'язаних

рівнів: стандартів і профілів, спільних сервісів, процедур реагування та довіри/сертифікації. Там, де ці рівні розвинені комплексно (перш за все в секторі безпеки, фінансів, у великих містах), система виявляє значно вищу здатність до безперервності управлінських функцій і швидкого відновлення після ударів. Там, де спостерігаються дисбаланси (наявні сервіси без процедур, стандарти без контролю, взаємодія без довіри), кризи оголюють вразливості й призводять до затримок, інформаційного хаосу та фрагментованих рішень.

5.2. Integrated Open Governance Framework як нова концепція державного управління в цифрову епоху

Збройна агресія проти України, цифрові трансформаційні процес, деформація відносин у моделі «держава – людина» потребують переосмислення інтегрованого відкритого управління не лише як парадигми прозорості та участі, а як архітектури керованої адаптації державної системи до екзистенційних викликів. Класичний підхід до Integrated Open Governance (IOG) акцентував увагу на розширенні доступу до публічної інформації, цифрових сервісах взаємодії «держава – громадянин» та інклюзивних механізмах участі. У концептуальній архітектурі дисертації такі підходи розглядаються як функціональні компоненти єдиного контуру управління стійкістю, де відкритість і інтегрованість виконують роль не тільки демократичного, а й антикризового ресурсу. Адже проведені у розділах дисертації дослідження показали, що традиційні моделі управління (навіть відносно інноваційні) не завжди відповідають сучасному змісту НМС. Ми акцентуємо на важливості переосмислення інтегрованого відкритого управління не лише як парадигми прозорості та участі, а як архітектури керованої адаптації державної системи до шоків. Класичний підхід до Integrated Open Governance Framework (IOGF) міг би (за наявності розробленої методології) акцентувати увагу на розширенні доступу до

публічної інформації, цифрових сервісах суспільної взаємодії та інклюзивних механізмах участі. У запропонованій авторській інтерпретації ці елементи розглядаються як функціональні компоненти єдиного контуру управління стійкістю, де відкритість і інтегрованість виконують роль не тільки демократичного, а й антикризового ресурсу.

Якщо розглядати НМС як складну соціально-технічну систему, вона виявляється підпорядкованою загальним законам управління складними динамічними об'єктами, коли для підтримання функціонування в умовах різких зрушень система потребує дієвих механізмів «спостереження—оцінювання—реакції—навчання». У цьому контексті IOGF інтерпретується як:

- інституціонально-правова рамка, що визначає правила циркуляції інформації про загрози, ресурси та вразливості між акторами;
- цифрова інфраструктура, яка забезпечує оперативний збір, агрегацію, аналіз і візуалізацію даних про стан критичних сфер;
- організаційний механізм, який задає формати координації рішень між секторами, рівнями влади та недержавними учасниками.

У системно-кібернетичній термінології IOGF виконує функції «керуючої підсистеми» для НМС, перетворює потоки даних із середовища та підсистем (енергетика, оборона, соціальна сфера, економіка, цифрова інфраструктура) на узгоджені управлінські дії, зворотно впливаючи на конфігурацію національної системи в напрямі відновлення або трансформації. Принципово важливо, що в такій інтерпретації відкритість набуває нової ролі – це не лише умова демократичного контролю, а й спосіб збільшення «інформаційної розмірності» регулюючого контуру, тобто здатності держави бачити більше й точніше щодо стану суспільства, ресурсів, настроїв, ризиків.

Згідно із законом необхідної різноманітності Ешбі, система управління повинна мати різноманітність не меншу, ніж система, якою вона керує: «Для ефективного управління складною системою (об'єктом управління) система управління повинна мати не меншу або більшу різноманітність (кількість

можливих станів/дій), ніж різноманітність самого об'єкта управління, інакше керування не буде ефективним; іншими словами, тільки «різноманітність може знищити різноманітність», що означає, що для подолання зовнішнього різноманіття керуюча підсистема повинна мати достатній спектр відповідей, щоб протидіяти кожному з них. Отже, інтегроване відкрите управління, що оперує широкими масивами даних і спирається на різні групи акторів, підвищує цю різноманітність, а отже, підсилює спроможність до резильєнтності.

При цьому визначальним об'єктом поглибленого аналізу стають цифрові інструменти, що реалізують зворотні зв'язки між середовищем, суспільством і державою. У такому випадку системи DRA (Digital Resilience Assessment) можуть поєднувати у межах НМС:

- 1) автоматизований збір індикаторів стану критичних секторів (навантаження на енергосистему, доступність цифрових сервісів, міграційні потоки, динаміка цін);
- 2) опрацювання сигналів «знизу» (скарги, петиції, звернення, дані волонтерських і громадських ініціатив);
- 3) аналітичні модулі, які виявляють аномалії та можливі «точки зламу» задовго до того, як вони перетворяться на повномасштабні кризи.

У термінах управління складними системами DRA виступає самостійним сенсорно-аналітичним модулем – трансформує розрізнені, часто фрагментовані сигнали в осмислені управлінські «тригери», що запускають відповідні сценарії реагування. Аналітична складова DRA полягає в тому, що зібрані сигнали проходять послідовну обробку, очищення від несистемної інформації й помилок, нормалізацію форматів, агрегування за територіями, секторами, часовими інтервалами, зіставлення між собою. На цьому етапі з'являються не просто окремі показники, а індикатори стану резильєнтності – інтегральні оцінки навантаження на системи, рівня вразливості, стійкості ключових процесів. Виявляються як різкі відхилення від норми (аномалії), так і повільні, але стабільні тренди деградації чи покращення. Іншими

словами, хаотичний потік подій перетворюється на впорядковану картину, придатну для ухвалення рішень в системі державного управління.

Критичним є те, що DRA не зупиняється на рівні діагностики, а містить у собі вбудовані правила інтерпретації, які переводять аналітичні висновки в управлінські тригери. Для цього визначаються порогові значення індикаторів, комбінації подій і просторово-часові патерни, за яких ситуація класифікується як така, що потребує втручання. Наприклад, як ми вже вказували у попередніх розділах, одночасне зростання технічних збоїв, кількості скарг від користувачів та падіння обсягів транзакцій у певному регіоні може бути формалізовано як сигнал про кризу соціально-критичної важливості. У такому разі DRA не лише «фіксує проблему», а й генерує чіткий тригер для керуючих структур: автоматичне сповіщення відповідальних органів, запуск заздалегідь визначених сценаріїв реагування, активацію резервних каналів, а також формування публічного повідомлення для населення.

Таким чином, DRA виступає не пасивною панеллю моніторингу, а активним елементом керуючого контуру: воно скорочує відстань між появою відхилення у системі та управлінською реакцією на нього. Завдяки перетворенню фрагментованих сигналів на осмислені тригери DRA мінімізує ризик управлінських помилок, зменшує час інтерпретації ситуації людьми та дозволяє вбудувати в архітектуру інтегрованого відкритого управління механізми реагування, наближені до режиму реального часу. Це і є зміст твердження про DRA як сенсорно-аналітичний модуль: він не тільки «бачить» і «розуміє» стан складної системи, а й безпосередньо ініціює запуск відповідних сценаріїв реагування в межах Національної моделі стійкості.

Єдині простори даних, у яких поєднуються відомчі, регіональні, громадські та комерційні джерела, створюють спільну картину ситуації для різних органів влади. З погляду резильєнтності це означає:

- зниження ризику інформаційних «сліпих зон»;
- можливість порівнювати дані різної природи (статистика,

транзакції, сигнал з соціальних мереж, оперативні звіти) для більш надійного виявлення загроз;

- підтримку комплексної оцінки наслідків управлінських рішень (наприклад, впливу обмежень на енергоспоживання на економічну активність і соціальну напругу).

При цьому електронні канали зворотного зв'язку (онлайн-звернення, інцидент-репортинг, опитування в кризових умовах) набувають нового змісту – вони перетворюються на мережу «людських сенсорів», які доповнюють формальні вимірювання. Для резильєнтності особливо важливо, що такі канали дозволяють:

- швидко виявляти «локальні проблеми» у роботі систем управління (відсутність послуги в конкретному населеному пункті, недоліки у логістиці гуманітарної допомоги, проблеми доступності інформації для вразливих груп);

- тестувати прийнятність запропонованих рішень для різних соціальних груп до їх широкомасштабного впровадження;

- коригувати політику в режимі, близькому до реального часу.

Отже, цифрові засоби у межах IOGF не зводяться до фасилітаторів сервісів – вони формують структуру зворотних зв'язків, без яких неможливо досягти ані швидкої реакції, ані навчання системи державного управління на власному досвіді.

Класичне розуміння «відкритого урядування» як сукупності принципів прозорості, доступу до інформації та підзвітності сформувалося в умовах відносної стабільності суспільних відносин й було зорієнтоване насамперед на розширення демократичної участі та протидію корупції. Проте повномасштабна агресія проти України продемонструвала, що цього виміру відкритості недостатньо, коли йдеться про виживання й стійкість держави як системи. Екзистенційна загроза висуває до публічного управління інші вимоги: здатність діяти швидко за умов радикальної невизначеності, працювати з фрагментарною інформацією, узгоджувати рішення в режимі

«тут і тепер», зберігаючи при цьому легітимність і довіру суспільства. Саме в цих умовах виникає потреба в переході від лінійної моделі «відкритого уряду» до інтегрованої рамки Integrated Open Governance Framework (IOGF), яка розуміється вже не лише як механізм демократизації, а як модель робастного управління. Емпіричним підтвердженням такого переходу став кейс національної платформи «єДопомога», яка за перші місяці повномасштабного вторгнення опрацювала понад 14 мільйонів запитів щодо гуманітарної допомоги.

Ця система еволюціонувала з простого державного порталу у справжній інтеграційний хаб, де державні органи (Мінсоцполітики, ОВА, військові адміністрації), міжнародні донори (Червоний Хрест, UNICEF, UNDP), волонтерські організації та бізнес співпрацювали в єдиному цифровому середовищі. За даними Мінцифри, час від фіксації запиту до надання допомоги скоротився з 12-14 днів до 3-5 днів саме завдяки інтегрованій архітектурі, де обмін даними відбувався в режимі реального часу. У такій інтерпретації IOGF розгортається як замкнений контур управління, де відкритість і інтегрованість виконують функцію інформаційного «каркасу» для стійкості, а не лишаються декларативними цінностями. На «вході» цього контуру перебувають різноманітні сигнали – від формалізованих даних систем безпеки (кіберінциденти, пошкодження інфраструктури, показники роботи критичних систем) до соціальних запитів і скарг, зафіксованих через цифрові канали взаємодії з громадянами, бізнесом, волонтерськими мережами. Важливо, що ці потоки надходять не з одного, а з множини джерел: державні сенсори, приватні платформи, громадські ініціативи, міжнародні партнери.

Яскравим прикладом став український застосунок «Повітряна тривога», інтегрований з «Дією», який акумулював дані з військових систем раннього попередження, сенсорів у регіонах та волонтерських мереж спостереження. Лише за 2022 рік цією системою скористалося понад 18 мільйонів громадян. Анонімізовані дані про реакцію користувачів під час

тривог стали цінним зворотним зв'язком для ДСНС та ЗСУ щодо ефективності системи оповіщення. Іншим прикладом є платформа ВПО.інфо, яка поєднала дані з Реєстру ВПО, картографічні дані Мінрегіону, інформацію від місцевих громад та зворотний зв'язок від самих переселенців. Це дозволило оперативно виявляти «гарячі точки» з надмірною концентрацією ВПО та критичним навантаженням на інфраструктуру (за даними Мінреінтеграції, в 14 територіальних громадах кількість ВПО перевищила 40% від довоєнного населення). Усередині керуючого контуру відбувається обробка цих сигналів. Саме тут IOGF проявляє себе як інтегрований «процесор» – сукупність інституцій, правил, алгоритмів і цифрових платформ, які перетворюють розрізнену інформацію на керуючі рішення. Аналітичні модулі, що спираються на технології обробки великих даних, машинного навчання, геоаналітики, дозволяють поєднувати в єдиній рамці дані з різних секторів і рівнів управління, виявляти аномалії, моделювати сценарії розвитку подій.

Емпірично це простежується у функціонуванні Центру протидії дезінформації при РНБО України, який за 2022-2024 роки проаналізував понад 1,8 мільйона інформаційних повідомлень, ідентифікувавши та розвінчавши понад 12 000 дезінформаційних наративів. При цьому ЦПД використовує унікальну інтегровану систему, що поєднує дані з соціальних мереж (через API-інтеграції), повідомлення з державних систем моніторингу, сигнали від громадських «інфомедиків» (понад 8000 верифікованих волонтерів-дослідників дезінформації) та технічні дані про аномалії в інформаційному просторі. Іншим прикладом «процесора» стала система «eПідтримка», через яку держава надала допомогу 8,7 мільйонам громадян, інтегрувавши дані з 15 реєстрів та систем (податкова, соціальне страхування, банківська верифікація, реєстри підтверджених руйнувань та ін.). Кросс-верифікація даних та аналітика великих масивів дозволила на 42% знизити кількість помилкових виплат порівняно з класичними «паперовими» процесами [384].

При цьому сама структура інституцій змінюється: вертикальні ієрархії поступово доповнюються або частково заміщуються мережевими конфігураціями, де міжвідомчі команди, кризові штаби, спільні центри даних можуть приймати рішення, спираючись на спільну інформаційну картину. Таким чином, «процесор» у межах IOGF – це не окреме міністерство чи агентство, а інтегрована сукупність акторів, пов’язана спільними цифровими інструментами та правилами використання даних. Ця тенденція особливо виразно проявилася в функціонуванні Координаційного штабу з гуманітарних та соціальних питань при Офісі Президента України. Згідно зі звітом НАДС за 2022 рік, час прийняття міжвідомчих рішень скоротився в середньому на 68% порівняно з «домілітарними» форматами координації. Штаб, що мав доступ до інтегрованої системи «Гуманітарна карта України», міг у режимі близькому до реального часу бачити розподіл потреб, ресурсів та логістичних можливостей по країні. При цьому доступ до цифрової платформи штабу мали не лише державні органи, але й міжнародні партнери та акредитовані гуманітарні організації (237 організацій-партнерів на кінець 2023 року), що створювало безпрецедентну для українського урядування «екосистему спільного реагування».

Управлінський керуючий вплив, тобто вихід цього замкненого контуру, матеріалізується в конкретних діях: перерозподілі бюджетних ресурсів на користь критично важливих напрямів, організації евакуаційних заходів, зміні маршрутів постачання, пріоритизації відбудови окремих об’єктів, модифікації регуляторних вимог для бізнесу чи громад. Структурна стабільність (або ще «робастність») IOGF виявляється саме в тому, наскільки ці рішення є одночасно швидкими, обґрунтованими й адаптивними: система не просто виконує заздалегідь написаний план, а коригує його, виходячи з динаміки середовища. Конкретний вимір цього можна спостерігати в кейсі розгортання пунктів незламності, коли інтегрований аналіз даних про електропостачання, температурні режими, щільність населення та соціальне навантаження у громадах дозволив за лічені дні (з 23 по 28 листопада 2022

року) розгорнути понад 4500 таких пунктів у пріоритетних локаціях. Згідно зі звітом ДСНС, завдяки алгоритмам інтегрованого планування, ресурси (генератори, Starlink-станції, обігрівачі) розподілялися не рівномірно за областями, а за комбінованими критеріями потреби та вразливості. Подальші коригування розміщення відбувалися на основі даних про завантаженість та запитів громад, що надходили через єдину цифрову платформу «Пункти незламності». Інший приклад – переорієнтація програми «Доступні ліки» в перші місяці війни, коли на основі даних від аптек, медичних закладів та зворотного зв'язку від громадян через застосунок «Ліки.Контроль» (спільний проєкт МОЗ та громадської організації «Пацієнти України») було за 14 днів змінено перелік препаратів та змінено принцип дистрибуції для забезпечення потреб внутрішньо переміщених осіб.

Для вирішення таких завдань у межах IOGF вбудовується механізм постійного зворотного зв'язку: цифрові платформи, статистичні панелі, сервіси зворотного зв'язку з громадянами фіксують наслідки ухвалених рішень, виявляють побічні ефекти, відкривають додаткові вразливості. Отримані дані повертаються в «процесор», де переосмислюються параметри політики, уточнюються алгоритми розподілу ресурсів, модифікуються протоколи реагування. Яскравим прикладом такого зворотного зв'язку став «Індекс сприйняття безпеки» – спільний проєкт МВС, МОЗ, ДСНС та НУО «Центр безпечних громад», який через постійні мікроопитування (в середньому 8700 респондентів на місяць) вимірює реакцію громадян на безпекові заходи та зміни в системі цивільного захисту. За даними МВС, саме на основі аналізу цього індексу у вересні 2022 року було суттєво скориговано протоколи оповіщення про повітряну тривогу – введено диференціацію повідомлень за типами загроз, що дозволило знизити «тривожну втому» серед населення (показник «ігнорування тривог» знизився з 32% до 18%). Інший масштабний кейс – використання зворотного зв'язку з «Дії» для коригування програм компенсацій за зруйноване житло. Аналіз понад 147000 заявок (станом на серпень 2023 року) не лише виявив «вузькі

місця» в процесі верифікації, а й дозволив уточнити критерії «часткового руйнування», які виявилися неадекватними в реальних умовах [385].

Саме завдяки такій циклічній архітектурі IOGF виконує роль цифрового дизайну Національної моделі стійкості. Держава перестає бути винятково ієрархічною системою, в якій інформація рухається повільно й односторонньо, а рішення ухвалюються в умовах дефіциту зворотного зв'язку. Натомість вона набуває рис мережевого адаптивного організму: численні «сенсори» в різних частинах соціального й інфраструктурного тіла фіксують зміни; центральні й периферійні функціональні логи (органи влади різного рівня, партнерські структури) опрацьовують інформацію; керуючі імпульси швидко повертаються у вигляді рішень, які одразу ж оцінюються через новий виток зворотного зв'язку.

Ефективність такого підходу проявилася в результатах опитування керівників ЦОВВ та ОДА щодо швидкості прийняття складних рішень, проведеного у межах дисертаційного дослідження в НТУ «Дніпровська політехніка» у жовтні 2022-2024 рр. Підрозділи, які мали високий рівень цифрової інтеграції (спільний доступ до даних, інтероперабельні системи, автоматизовані канали зворотного зв'язку) демонстрували на 72% вищу швидкість реакції на кризові ситуації порівняно з тими, що працювали у традиційній моделі «послідовної бюрократії». При цьому показники якості рішень (відсутність необхідності подальшого перегляду, позитивна оцінка бенефіціарами) були вищими на 41% саме у «інтегрованих» підрозділах (аналіз опитування у додатку Д2).

У цій логіці класичні цілі відкритого уряду, прозорість і підзвітність, не зникають, але вбудовуються в ширшу архітектуру керованої адаптації, де відкритість слугує умовою не лише довіри, а й виживання складної державної системи в умовах тривалої війни та багатовимірних криз. Емпіричним підтвердженням цього стала позитивна кореляція ($r=0,68$) між рівнем відкритості даних місцевих органів влади (за методологією Open Data Maturity Model) та показниками їх адаптивності під час кризових ситуацій у

2022-2023 роках. Ті громади та області, які ще до повномасштабного вторгнення впровадили практики відкритих даних, публічного бюджету та цифрових консультацій, змогли значно швидше перебудувати систему управління під воєнні потреби та забезпечити більш ефективну взаємодію з вимушеними переселенцями, волонтерами та міжнародними партнерами.

Функціонування Integrated Open Governance Framework (IOGF) у системі державного управління доцільно розглядати також на основі сучасних кризових викликів. У цьому підході держава постає як складна керована система, яка постійно піддається впливу зовнішніх і внутрішніх факторів – військових, економічних, інформаційних, соціальних. Завдання IOGF полягає не лише в тому, щоб забезпечити прозорість та участь, а насамперед у тому, щоб перетворити ці принципи на робочі механізми підтримання стійкості НМС. Ключовими тут виступають три управлінські принципи, що визначають логіку роботи такого інтегрованого контуру: мінімізація латентності, компенсація девіацій і обов’язковий зворотний зв’язок.

1. Принцип *мінімізації латентності* спрямований на подолання хронічної проблеми класичної бюрократії – надмірних часових розривів між появою проблеми і реакцією на неї. У традиційній моделі сигнал про кризу або потребу (наприклад, нестача гуманітарної допомоги, руйнування об’єктів критичної інфраструктури, сплеск міграції) проходить через декілька рівнів погоджень, формальних запитів, міжвідомчих узгоджень і нерідко «застрягає» на проміжних етапах. У результаті час від виникнення девіації до управлінського рішення може вимірюватися тижнями чи місяцями, що в умовах війни або масштабної кризи фактично нівелює ефект будь-якого, навіть формально правильного рішення. IOGF націлений на переведення цієї логіки в режим, максимально наближений до реального часу, спираючись на розбудовану цифрову інфраструктуру. Такі інструменти, як система електронної взаємодії «Трембіта», цифрові сервіси податкової звітності («СОТА» та інші), портали оперативної звітності органів влади,

забезпечують можливість моментального захоплення, передачі та агрегації даних із різних точок системи управління – від окремої громади або військової адміністрації до центральних органів виконавчої влади. Управлінський зміст цього принципу полягає в усвідомленні часу як критичного ресурсу, адже кожна зайва година затримки між сигналом від об'єкта управління (фронт, громада, сектор економіки) та реакцією суб'єкта управління (Кабінет Міністрів, РНБО, профільне міністерство) зменшує шанси на стабілізацію ситуації та збільшує масштаб потенційних втрат. Мінімізація латентності означає не лише технічне прискорення документообігу, а й перегляд процедур, делегування повноважень, спрощення маршрутів ухвалення рішень за рахунок інтегрованих цифрових платформ.

2. Принцип *компенсації девіацій* відображає відхід від уявлення про державу як «кам'яну стіну», що протистоїть ударам середовища винятково за рахунок жорсткості. У парадигмі IOGF система державного управління розглядається як динамічна структура, здатна змінювати власні конфігурації каналів, процедур і сервісів у відповідь на кризові зміни, зберігаючи при цьому ключові вихідні параметри: безперервність базових послуг, керованість територій, захист прав людини. Це означає наявність вбудованих механізмів резервування та перерозподілу навантаження – якщо один канал управління або надання послуг блокується, система автоматично або напів автоматично переводить функції на альтернативний канал. Типовим прикладом є ситуація, коли через обстріли чи окупацію втрачається доступ до Центру надання адміністративних послуг у певній громаді. У класичній моделі це означало б фактичну зупинку доступу громадян до адміністративних процедур. В умовах же інтегрованого відкритого управління частина критичних послуг дублюється через портали та мобільні додатки, насамперед через екосистему «Дія», інша частина передається до найближчих доступних пунктів або активізуються виїзні мобільні офіси. Аналогічна логіка застосовується до інформаційних потоків, коли у разі

зупинки у роботі окремих відомчих інформаційних систем інтеграційні платформи дозволяють тимчасово перейти на альтернативні джерела даних, зберігаючи керованість. Управлінський сенс принципу компенсації девіацій полягає в тому, що держава відмовляється від ідеалу «раз і назавжди оптимальної» структури й натомість вибудовує множину резервних маршрутів, сценаріїв і конфігурацій, які можуть бути оперативно активовані під тиском зовнішніх або внутрішніх шоків.

3. *Принцип обов'язкового зворотного зв'язку* переводить IOGF у площину самокорекції й навчання. Адже у класичній бюрократичній логіці рішення вважається виконаним у момент формального звіту або закриття документа. Натомість у моделі інтегрованого відкритого управління управлінський цикл не завершується до того часу, поки система не отримає достовірної інформації про фактичний ефект реалізованого рішення. Для цього інструменти електронної демократії, системи публічного моніторингу та реєстри проєктів розбудови (зокрема, система DREAM у сфері відновлення) використовуються не як «вітрина» для демонстрації досягнень, а як повноцінні «показники помилок». Публічні панелі, інтерактивні карти, реєстри контрактів і виконаних робіт дозволяють як громадськості, так і самим органам влади фіксувати розриви між запланованим і фактичним станом справ, виявляти затримки, дублювання, неефективні витрати. Зворотний зв'язок доповнюється каналами прямої участі: електронними петиціями, консультаціями, механізмами повідомлень про порушення, які дозволяють швидко «зняти показники» суспільного сприйняття тих чи інших рішень. Управлінський сенс цього принципу полягає в інституціоналізації права системи на помилку за умови наявності вбудованого механізму її виявлення й виправлення. Якщо суспільство, професійні спільноти або локальні стейкхолдери послідовно сигналізують про неефективність певного інструменту, політики чи проєкту, IOGF має містити процедурні та цифрові засоби для перегляду відповідних рішень без надмірних бар'єрів і втрати обличчя владою.

Сукупність цих трьох принципів формує операційну логіку IOGF як керуючого контуру НМС. Мінімізація латентності забезпечує своєчасність реагування; компенсація збурень гарантує збереження ключових функцій попри руйнування окремих елементів системи; обов'язковий зворотний зв'язок перетворює помилки на ресурс навчання, а не на джерело накопичення структурної вразливості. У такій конфігурації інтегроване відкрите управління постає не як декоративна надбудова над традиційною бюрократією, а як ядро адаптивної, цифрово опосередкованої державної системи, здатної підтримувати національну стійкість у середовищі тривалих криз і високої невизначеності. Якщо перейти від концептуального опису IOGF до практичної реалізації в умовах Національної моделі стійкості, важливо чітко показати, що змінюється не лише набір інструментів, а сама логіка функціонування системи управління. Наведена нижче таблиця узагальнює цю трансформацію, демонструючи, як класична модель IOGF поступово переростає у резильєнтний, мережевий формат НМС.

Таблиця 5.5

Трансформація моделі Integrated Open Governance

Характеристика	IOGF 1.0 (класична «відкритість»)	IOGF 2.0 (модель НМС / резильєнтна)	Практика реалізації
Цільова функція	Фокус на прозорості, антикорупції, сервісності; відкриті дані та зручні е-сервіси як головні результати	Фокус на виживанні системи, безперервності критичних функцій, безпеці населення й інфраструктури; відкритість інтегрована в контур стійкості	Кількість е-послуг у «Дії» зросла до 100+; при цьому ключові виплати (пенсії, соц.допомога, виплати ВПО) у розпал атак на енергосистему зберігали рівень виплат >90–95% від довоєнних обсягів навіть у постраждалих регіонах
Роль інформації	Дані здебільшого як об'єкт публікації та звітності (портالي відкритих даних, відкриті бюджети, аналітичні звіти)	Дані як керуючі сигнали в режимі, наближеному до реального часу (дашборди для уряду, оперативні карти, кризові панелі)	Портал відкритих даних містить тисячі наборів, але під час війни з'являються оперативні панелі Міноборони, МВС, Мінреінтеграції: час оновлення критичних показників (ВПО, пошкоджена інфраструктура тощо) скорочується з місяців/кварталів до днів/годин
Реакція на кризу	Реактивна: штаби і комісії створюються <i>постфактум</i> , рішення узгоджуються вручну, цикл реагування затяжний	Проактивна – моделювання сценаріїв, раннє виявлення загроз, запуск превентивних заходів	Час розгортання мережі «Пунктів незламності» – кілька днів після масованих ударів по енергосистемі; рішення щодо евакуації окремих громад ухвалюються на підставі щоденних даних про обстріли, логістику й гуманітарний стан

Продовження таблиці 5.5

Характеристика	IOGF 1.0 (класична «відкритість»)	IOGF 2.0 (модель НМС / резильєнтна)	Практика реалізації
Структура зв'язків	Переважно вертикальна ієрархія з окремими епізодами горизонтальної координації (робочі групи, міжвідомчі наради)	Мережева, розподілена, відмовостійка: кілька центрів прийняття рішень, об'єднаних через інтегровані платформи та спільні дата-хаби	У міжвідомчих кризових штабах (гуманітарний, енергетичний тощо) одночасно працюють десятки ЦОВВ, ОВА, міжнародних партнерів; кількість підключених до «Трембіта» інформаційних систем і реєстрів зростає до сотень, що зменшує залежність від окремих відомчих IT-систем
Тип управлінського циклу	Цикл «планування – виконання – звітування» з великими лагами; корекція політик часто відбувається раз на рік/квартал	Безперервний цикл «виявлення – дія – оцінка – корекція» з опорою на постійний цифровий моніторинг	У системах типу DREAM (проекти відновлення) та цифрових дашбордах міністерств статус проектів, тендерів, будівельних робіт оновлюється у форматі «онлайн / раз на добу», що дозволяє переглядати рішення щотижнево, а не раз на рік
Критерій ефективності	Основний KPI – задоволеність користувача (зручність е-послуг, кількість зареєстрованих користувачів, кількість послуг онлайн)	Основний KPI – час відновлення керованості (Recovery Time Objective), мінімізація втрат і тривалості перерв у наданні	Кількість користувачів «Дії» зростає до 15–20 млн, але в резильєнтній логіці вимірюється також середній час відновлення доступу до послуг після атак (наприклад, відновлення роботи е-сервісів протягом годин/однієї доби після масованих кібератак або відключень енергії)
Механізм формування довіри	Довіра базується на прозорості: відкриті дані, публічні звіти, участь у консультаціях, громадський контроль	Довіра формується через доведену дієвість: здатність системи захищати, забезпечувати безперервність послуг і швидко адаптуватися до загроз. Прозорість – підтримуючий, але не єдиний чинник	Соціологічні опитування фіксують стійко високий рівень довіри до ЗСУ й значне зростання довіри до окремих інституцій влади саме після успішних хвиль евакуації, відновлення критичної інфраструктури, швидкого запуску програм компенсацій через цифрові сервіси
Роль громадян і стейкхолдерів	Громадяни – користувачі послуг і учасники консультацій (петиції, публічні обговорення, наглядові ради)	Громадяни, громади, бізнес, волонтери – елементи сенсорної мережі: їхні дані й сигнали інтегруються у прийняття рішень у режимі близькому до реального часу	Мільйони повідомлень через «Дію», гарячі лінії, боти (руйнування, потреби ВПО, відключення світла) стають інпутами для рішень КМУ, ОВА, служб порятунку; волонтерські карти (укриттів, черг, аптек) інтегруються у планування на місцевому рівні
Управлінські технології та дані	Е-уряд здебільшого як сервісність і звітність: електронні кабінети, публічні реєстри, базова аналітика; дані роз'єднані між відомствами	Інтегровані платформи, міжвідомчі дата-хаби, аналітика великих даних, алгоритми підтримки рішень; інтероперабельність та автоматизовані потоки даних по всій системі	Зростає кількість інтегрованих реєстрів у «Трембіта»; аналітичні центри РНБО, Міноборони, Мінфіну, Мінсоцполітики працюють з мільйонами записів у реальному чи близькому до реального часу (перехресна верифікація даних про ВПО, виплати, руйнування, гуманітарні вантажі)

Джерело: розроблено автором

Еволюція від IOGF 1.0 до IOGF 2.0 означає перехід від «класичного» відкритого уряду, орієнтованого передусім на прозорість і сервісність, до резильєнтної архітектури, де відкритість інтегрується в механізми виживання, безпеки та безперервності критичних функцій держави. Щоб структуровано зафіксувати ці відмінності, доцільно порівняти дві моделі за ключовими параметрами: цільовою функцією, роллю інформації, характером реакції на кризу, типом зв'язків у системі, критеріями ефективності та механізмами формування довіри. Адже перехід IOGF від 1.0 до 2.0 – це не просто посилення наявних практик прозорості, а глибинна зміна цільової функції та операційної логіки державного управління. У класичній моделі відкритий уряд зосереджений головню на нормативних цінностях – прозорість, підзвітність, участь, сервісність. Вона успішно працює в умовах відносної стабільності, коли основний виклик – підвищити якість послуг та знизити корупційні ризики.

Натомість, резильєнтна модель IOGF 2.0 виходить із припущення постійної присутності криз – воєнних, безпекових, економічних, гуманітарних. Відкритість у такій конфігурації перестає бути самоціллю й перетворюється на інфраструктуру для швидкого збору, обробки та використання сигналів, що надходять від суспільства, ринків, інфраструктурних систем і міжнародних партнерів. Інформація стає не стільки «контентом для публікації», скільки основою керуючих впливів, які мають запускатися майже автоматично, коли певні індикатори досягають критичних порогів.

Зміна структури зв'язків – від переважно вертикальної до розподіленої мережевої – означає переосмислення ролі центрів прийняття рішень. Якщо в моделі IOGF 1.0 горизонтальна координація часто залежить від особистих контактів або політичної волі, то в моделі IOGF 2.0 вона вбудована в цифрові платформи та регламенти взаємодії. Це робить систему більш відмовостійкою: вихід із ладу окремого вузла не паралізує всю архітектуру, оскільки інші елементи можуть перебирати на себе частину функцій.

Критерії ефективності також радикально змінюються. Адже там, де раніше ключовим показником була задоволеність користувача послугами, у резильєнтній парадигмі пріоритет отримує час відновлення керованості та здатність системи витримувати й поглинати удари без руйнівних наслідків. Це не скасовує важливості «класичних» індикаторів (якість сервісу, зручність, прозорість), але переводить їх у ширший контекст – збереження функціональної цілісності держави. Нарешті, механізм довіри еволюціонує від «довіри через бачення» (суспільство бачить, як працює влада) до «довіри через дієвість» (суспільство відчуває ефект від рішень у критичні моменти). Прозорість і відкриті дані тут залишаються фундаментом, але довіра остаточно закріплюється лише тоді, коли громадяни переконуються, що система здатна їх реально захистити, забезпечити базові послуги та швидко адаптуватися до нових загроз. У цьому й полягає сутність переходу до IOGF 2.0 як цифрового дизайну НМС. Інструментарій реалізації IOGF у форматі НМС доцільно описувати як повний цикл: від фіксації змін середовища до корекції політик і захисту самої системи управління (таблиця 5.6).

Таблиця 5.6

Інструментарій реалізації IOGF у форматі НМС

Компонент стійкості	Функція в структурі управління	Цифровий інструмент (приклади в Україні)	Управлінський ефект	Україна 2022–2024
1	2	3	4	5
Моніторинг загроз	Сенсор – безперервний збір структурованих і неструктурованих даних про стан середовища, фіксація пертурбацій та відхилень від «нормального» режиму	ІАС «СОТА» (податкові, фінансові показники), застосунок «єВорог» та інші краудсорсингові інструменти повідомлень, реєстри пошкодженого та зруйнованого майна, реєстри ВПО, карти обстрілів, муніципальні геоінформаційні системи, телеметрія з інфраструктурних об'єктів	Формування інтегрованої ситуаційної картини в режимі, наближеному до реального часу, раннє виявлення «гарячих точок» (масові руйнування, міграційні хвилі, дефіцит ресурсів), можливість пріоритизації ресурсів на основі об'єктивних даних	Сотні тисяч записів у реєстрах пошкодженого майна; мільйони звернень від громадян через мобільні застосунки, боти та гарячі лінії; оновлення карт обстрілів, даних про ВПО, інфраструктурні пошкодження як основою для рішень уряду, ОВА, міжнародних партнерів

Продовження таблиці 5.6

1	2	3	4	5
Прийняття рішень	Контролер – агрегація та аналіз даних, фільтрація спаму, виявлення закономірностей, моделювання сценаріїв; на цьому етапі «сирі» сигнали перетворюються на керуючі дії (накази, протоколи, політики, плани реагування)	AI-аналітика та системи підтримки прийняття рішень у РНБО, МОУ, Мінфін, Мінсоцполітики; інтегровані ситуаційні центри (урядові аналітичні дашборди, регіональні центри даних), ризик-скорингові системи у фінансовій, митній, податковій сферах; модулі прогнозування в енергетиці, логістиці, гуманітарній допомозі	Зменшення суб'єктивізму та «ручного» управління в кризових умовах. Підвищення швидкості ухвалення рішень за рахунок попередньо налаштованих аналітичних моделей та алгоритмів. Можливість тестувати декілька сценаріїв розвитку подій до запуску повномасштабної реакції	Мільйони записів з реєстрів (ВПО, соцвиплати, податки, енергоспоживання) інтегровані в аналітичні панелі для уряду та РНБО; рішення щодо таргетованих виплат, змін тарифів, евакуацій чи пріоритетів відновлення ухвалюються з опорою на моделі навантажень і ризиків
Виконання	Виконавчий механізм – реалізація керуючих сигналів – доведення рішень до конкретних бенефіціарів, запуск чи зупинка сервісів, перерозподіл ресурсів. Перетворення управлінських намірів на реальні дії	Платформа «Дія» (масові виплати, електронні документи, послуги для ВПО, бізнесу, військових), система «Шлях» (керування критичними переміщеннями через кордон), сервіси «єДопомога» та інші програми підтримки, електронні черги, цифрові сервіси органів місцевого самоврядування	Скорочення часу між ухваленням рішення й фактичним наданням послуги чи ресурсу з тижнів/місяців до годин/днів, Масштабування рішень, зменшення корупційних ризиків і транзакційних витрат за рахунок мінімізації фізичного контакту	Масові програми виплат (підтримка ВПО, компенсації за пошкоджене майно тощо), реалізуються через цифрові платформи протягом обмеженого часу; значна частина адміністративних послуг стала доступною 24/7 у цифровому форматі, включно з прифронтовими територіями
Контроль та корекція	Зворотний зв'язок – постійне порівняння планових параметрів із фактичними результатами, виявлення розривів, коригування політик, бюджетів і процесів. Це «система самокорекції», що перетворюють помилки на інформацію для навчання системи	Екосистема DREAM (цифровий контур планування і моніторингу проєктів відновлення), інструменти Digital Resilience Assessment (DRA), публічні дашборди виконання урядових програм, модулі оцінки якості послуг та скарг у «Дії» та на порталах органів влади, платформи громадського моніторингу	Підвищення підзвітності за використання ресурсів (насамперед у відбудові й соціальних програмах). Раннє виявлення корупційних схем, затримок, неефективних чи дублюючих проєктів. Можливість коригувати пріоритети та дизайн програм, без очікування завершення бюджетного циклу	Тисячі проєктів відбудови зареєстровані та відстежуються в DREAM із публічним доступом до ключових параметрів; дані використовуються донорами для ухвалення рішень про фінансування. Масові відгуки й скарги користувачів цифрових сервісів стають підставою для зміни умов програм

Продовження таблиці 5.6

1	2	3	4	5
Захист системи	Компенсатор пертурбацій (Disturbance Compensator): протидія зовнішнім і внутрішнім загрозам (кібератаки, фізичні руйнування, відключення енергопостачання), підтримання безперервності й цілісності роботи критичних елементів. Це «імунна система» цифрового контуру.	Комплексні системи кіберзахисту державних реєстрів і ключових інформаційних систем, багаторівнева автентифікація та шифрування, хмарні архітектури та «data embassies» (резервні копії критичних реєстрів у закордонних дата-центрах), георезервовані центри обробки даних, альтернативні канали зв'язку (зокрема супутникові рішення), системи резервного електроживлення.	Забезпечення роботи критичних цифрових сервісів навіть за умов масованих кібератак, фізичного ураження інфраструктури або тривалих відключень електроенергії. Зниження ризику «єдиної точки відмови» та втрати даних. Підтримання довіри користувачів до цифрового державного сервісу навіть у пікові періоди небезпеки.	Під час ракетних атак і блекаутів зберігалася працездатність ключових державних реєстрів (акти цивільного стану, податкові, соціальні реєстри) та більшості е-сервісів; перенесення частини інфраструктури до хмарних і зарубіжних дата-центрів дозволило уникнути повної зупинки управлінських процесів навіть у разі пошкодження фізичних серверів в Україні.

Джерело: сформовано автором

Удосконалена матриця показує, що реалізація IOGF у форматі НМС не зводиться до простого переліку цифрових сервісів. Кожен інструмент виконує чітко окреслену функцію в контурі НМС, й у сукупності ці елементи формують замкнений контур управління, у якому інформація перестає бути «пасивною звітністю» й перетворюється на активний драйвер рішень. Для дисертаційного дослідження така таблиця слугує основою для побудови системи цифрових управлінських стандартів, коли для кожного компоненту легко виокремити вимірювані показники (швидкість оновлення даних, час реакції, частка послуг, що зберігають доступність під час криз, частота й глибина коригування політик тощо). Це дозволить перейти від опису IOGF як концепції до кількісної оцінки ступеня його впровадження в контексті НМС.

Варто наголосити, що ключовою відмінністю IOGF від класичного New Public Management (NPM) є зміна джерела легітимності. Якщо NPM фокусувався на «клієнтоорієнтованості» та ефективності надання послуг (держава як сервіс), то IOGF в умовах війни фокусується на екзистенційній стійкості. Саме тому інституціональна довіра в моделі IOGF формується не

через комфорт, а через здатність системи функціонувати в умовах хаосу (resilient legitimacy) (таблиця 5.7).

Таблиця 5.7

Оцінка інституціональної довіри в моделі IOGF

Критерій порівняння	Класичне електронне врядування (E-Gov)	Integrated open governance framework (IOGF)
Інституційна мета	Оптимізація існуючих процесів, надання послуг (Service delivery).	Забезпечення життєстійкості системи та національної безпеки (Resilience).
Природа взаємодії	Вертикальна, ієрархічна (G2C - Government to citizen).	Мережева, екосистемна (G2C2G - Держава-Громадян-Суспільство).
Реакція на кризу	Зупинка сервісів або перехід в ручний режим («Paper fallback»).	Адаптація алгоритмів, масштабування хмарних рішень, безперервність («Digital by default»).
Роль громадян	Пасивні споживачі послуг (Users).	Активні учасники створення безпеки (Co-creators), сенсори загроз (напр., «Ворог»).
Тип легітимності	Раціонально-легальна (Веберівська): довіра до процедур.	Резильєнтна – довіра до здатності виживати та відновлюватися

Отже, інтегрована структура відкритого управління (IOGF) у межах НМС – це комплексна система, що поєднує прозорість, підзвітність, участь та доброчесність, використовуючи технології та дані, щоб зробити державне управління більш відкритим, ефективним та орієнтованим на громадян, сприяючи довірі та кращим результатам завдяки співпраці між урядом та громадянським суспільством.

5.3. Класифікація цифрових управлінських стандартів як нормативно-алгоритмічного формату НМС

В умовах повномасштабної збройної агресії та гібридної війни проти України поняття «цифрова резильєнтність» (digital resilience) вийшло далеко за межі академічних дискусій про кібербезпеку, трансформувавшись у фундаментальну складову національної екзистенційної стратегії. Сучасна українська система державного управління перебуває в унікальній ситуації: одночасно відбуваються глибока цифрова трансформація, повномасштабна

війна та інституційна адаптація до європейського правового простору. У цих умовах застосування цифрових технологій не може обмежуватися автоматизацією окремих адміністративних процедур чи модернізацією сервісів для громадян. Цифрові рішення фактично стають ядром управлінського процесу: через них збираються дані, формуються управлінські рішення, доводяться розпорядження, здійснюється моніторинг виконання й запуск корекцій. Саме тому потрібен чітко визначений, формалізований і відтворюваний комплекс управлінських алгоритмів, який задаватиме єдину логіку функціонування цифрових управлінських систем незалежно від політичних циклів, кадрових змін чи технологічних оновлень. Такий комплекс управлінських алгоритмів у даному дослідженні описується через поняття цифрових управлінських стандартів.

Практична реалізація НМС у цифровому вимірі передбачає відмову від жорсткої централізації на користь розподілених систем. Досвід війни показав, що цифрова інфраструктура є менш вразливою до кінетичних ударів, ніж фізична, за умови належної архітектури. Наприклад, міграція державних реєстрів у хмару та використання розподіленої системи обміну даними дозволили уникнути «цифрового колапсу» держави в перші дні вторгнення.

Отже, під цифровими управлінськими стандартами слід визначати системно впорядкований набір нормативно закріплених і технічно реалізованих вимог щодо проєктування та функціонування цифрових управлінських платформ і сервісів, обробки та використання даних в управлінських рішеннях, взаємодії між органами влади, інфраструктурами та громадянами в цифровому середовищі, а також забезпечення стійкості, підзвітності, прозорості та правомірності управлінських дій. Фактично, мова йде про управлінські норми, інтегровані в алгоритми, які: 1) визначають, які саме дані можуть і мають використовуватися для ухвалення рішень; 2) регламентують, як ці дані циркулюють між реєстрами, відомствами, рівнями влади; 3) задають, яким чином рішення перетворюються на дії (виплати,

дозволи, заборони, регуляторні заходи): 4) встановлюють, як контролюється результат та якими є процедури корекції державних політик; 5) гарантують, що всі ці етапи відбуваються в межах національного права, з передбачуваними наслідками та фіксованою відповідальністю.

Отже, цифрові управлінські стандарти виступають ланкою інтеграції між правовими приписами (закони, підзаконні акти, стратегії) та практикою функціонування цифрових управлінських платформ (портали, реєстри, аналітичні системи, мобільні застосунки). Вони перетворюють абстрактні норми державної політики на конкретні правила роботи інформаційних систем і сервісів.

Як визначено у розділі 4, у сучасній архітектурі державного управління централізовані цифрові управлінські платформи C-eGovPro (зокрема, національні портали на кшталт «Дії», галузеві платформи, міжвідомчі дата-хаби, системи на кшталт DREAM, «Трембіта» тощо) виконують роль: «операційних середовищ» для реалізації управлінських процесів; «транспортних каналів» для управлінських сигналів між рівнями влади; «точок контакту» між державою, громадянами та бізнесом. Але без чітко визначених стандартів такі платформи залишаються переважно технологічними продуктами, кожен зі своєю логікою, обмеженнями та ризиками (vendor lock-in, фрагментація, різні режими доступу й захисту). Натомість цифрові управлінські стандарти: по-перше, уніфікують правила функціонування для всіх платформ (як проєктувати, підключати, експлуатувати); по-друге, забезпечують несуперечливість управлінських рішень при одночасній роботі багатьох систем; задають єдину управлінську логіку, у межах якої платформи стають елементами спільного контуру, а не ізольованими «цифровими островами».

Якщо цифрові управлінські платформи (C-eGovPro) доцільно умовно розглядати як функціональні модулі державного управління (канали прийому звернень, модулі аналізу, сервіси виплат, реєстри, кабінети посадовців), то цифрові управлінські стандарти – це метарівень, який описує вимоги до їх

поведінки, взаємодії та стійкості. Саме завдяки стандартам:

- уніфікуються формати даних та інтерфейси взаємодії;
- задаються правила резервування й відновлення сервісів;
- визначаються обов’язкові механізми контролю, аудиту, зворотного зв’язку;
- обмежуються «допустимі режими» прийняття і виконання рішень.

Це критично для НМС, коли управлінська система має працювати як цілісний багаторівневий контур, а не як сума розрізнених інформаційних систем. Потреба у чіткій детермінації (визначенні, формалізації й закріпленні) цифрових управлінських стандартів зумовлена низкою взаємопов’язаних факторів. В умовах війни, гібридних загроз і високої турбулентності середовища держава не може дозволити собі ситуативні, «ручні» рішення у сфері цифрового управління.

Запропонована класифікація цифрових управлінських стандартів розглядається як ядро нової архітектури державного управління, у якій цифрові інструменти не просто автоматизують окремі операції, а формують замкнений управлінський контур Національної моделі стійкості (НМС). В умовах постійних пертурбацій безпекового, економічного та інформаційного середовища держава змушена діяти як цілісна керована система, де кожен елемент – від реєстру до мобільного застосунку – виконує чітко визначену роль у виявленні загроз, ухваленні рішень, реалізації управлінських впливів, контролі результатів та адаптації інституцій. Саме в цій логіці цифрова трансформація виходить за межі «сервісної оптимізації» й перетворюється на інфраструктуру екзистенційної безпеки держави.

Перехід від домінування парадигми «захисту» до парадигми «резильєнтності» означає, що органи влади більше не можуть обмежуватися побудовою статичних бар’єрів навколо інформаційних систем. Потрібна здатність у режимі, наближеному до реального часу, фіксувати зміни стану середовища, оцінювати їхній вплив на ключові функції держави, змінювати власні налаштування, маршрути й пріоритети та відновлювати керованість

після ударів. Цифрова резильєнтність у такому розумінні є інтегральною властивістю всієї системи державного управління: її організаційної структури, нормативної бази, кадрової спроможності та цифрової інфраструктури. Вона включає не лише захищені канали зв'язку та розподілені дата-центри, а й здатність урядових інституцій працювати з даними як з управлінськими сигналами, інтегрувати зворотний зв'язок від суспільства та міжнародних партнерів, перезапускати політики й програми без руйнування цілісності системи.

У цьому контексті національна екосистема e-Resilience постає як інтегрований простір взаємодії всіх суб'єктів НМС – центральних органів виконавчої влади, органів місцевого самоврядування, сил безпеки й оборони, критичної інфраструктури, бізнесу, волонтерського сектору. Вона функціонує як розподілена мережа збору та обробки даних, де кожен рівень влади й кожен інституційний гравець є одночасно джерелом сигналів і адресатом управлінських рішень. Такий підхід вимагає відмови від фрагментарної цифровізації окремих відомств і переходу до цілісної архітектури, в якій стійкість закладена «за проектом» – у формі заздалегідь визначених маршрутів резервування, пріоритетів відновлення, алгоритмів реагування на типові сценарії кризи.

Ключовим механізмом, що забезпечує функціонування цієї архітектури у внутрішній логіці державного управління, виступає адаптивна розбудова інституційної спроможності. Йдеться про те, що здатність органів влади виконувати свої функції в цифровому середовищі не може бути результатом одноразової реформи чи впровадження окремої інформаційної системи. Вона формується як безперервний процес «налаштування» інституцій під змінні умови: через регулярну діагностику слабких місць, оновлення регламентів роботи, переналаштування цифрових сервісів, добір та навчання кадрів. У практичному вимірі це означає, що типова управлінська петля в органі влади має включати не лише стадії планування та виконання, а й закладений наперед механізм корекції, який автоматично запускається при досягненні

певних критичних значень показників (перевантаження системи, сплеск звернень, поява нових загроз). У цій логіці формується поняття нормативно-алгоритмічного каркаса цифрової резильєнтності. Нормативна складова задає правила гри: закони, підзаконні акти, стратегії, стандарти, які визначають, що саме вважається належною поведінкою органів влади в цифровому середовищі, які вимоги висуваються до захисту даних, як мають організовуватися процеси взаємодії між реєстрами, якими є права й обов'язки користувачів. Алгоритмічна складова перетворює ці норми на конкретні технічні обмеження й процедури: структуру баз даних, протоколи обміну, схеми авторизації, логіку бізнес-процесів у інформаційних системах. У результаті значна частина управлінських рішень фактично «вмонтована» у цифрову інфраструктуру: чиновник не може видати довідку без підтвердження статусу в реєстрі, змінити дані без фіксації цифрового сліду, обійти обов'язкову перевірку подвійних виплат тощо. Таке поєднання норм і алгоритмів створює жорсткий, але водночас адаптивний каркас, у межах якого держава може швидко перебудовувати свої сервіси без втрати контрольованості.

Потреба у чіткій детермінації (визначенні, формалізації й закріпленні) *цифрових управлінських стандартів* зумовлена низкою взаємопов'язаних факторів, які мають як теоретичне обґрунтування в сучасних наукових концепціях, так і емпіричне підтвердження у практиці державного управління.

По-перше, *стійкість до перманентних криз*. В умовах війни, гібридних загроз і високої турбулентності соціального середовища держава не може дозволити ситуативні, «ручні» рішення у сфері цифрового управління. Помилка в алгоритмі виплат, збій у реєстрі чи відмова платформи під час пікового навантаження безпосередньо впливають на здатність держави виконувати базові функції. Саме чіткі, відтворювані стандарти дозволяють системам продовжувати функціонування у кризових умовах.

Концепція антикрихкості, розвинута Н. Талебом (2014), вказує на

необхідність створення систем, які не лише витримують стрес, а й посилюються через нього, адже високостандартизовані технічні системи демонструють значно вищу адаптивність до кризових сценаріїв порівняно з ситуативними рішеннями [386]. При цьому детермінація стандартів дозволяє:

1) зафіксувати мінімально допустимі параметри стійкості систем (час відновлення, рівень резервування, вимоги до захисту), що створює вимірюваний базис для оцінки «здатності до виживання» систем;

2) задати типові сценарії реагування на відмови й атаки, що, відповідно до теорії високонадійних організацій (Weick & Sutcliffe, 2015), критично для трансформації потенційних катастроф у керовані інциденти;

3) гарантувати відтворюваність рішень і процедур незалежно від персонального складу чи політичної кон'юнктури, що, як показали дослідження NIST (2021), є ключовим фактором відновлення систем після масштабних кібератак.

Емпіричні дослідження кризового управління в цифровому урядуванні (Gil-Garcia et al., 2021) підтверджують, що ті держави, які мали формалізовані стандарти відмовостійкості для цифрових сервісів, змогли забезпечити значно кращу безперервність критичних функцій під час COVID-19 та інших кризових явищ.

По-друге, *подолання фрагментації цифрової екосистеми*. Україна уже має розвинений набір цифрових рішень, але без спільної стандартної основи вони ризикують перетворитися на множину несумісних між собою систем як проблема фрагментації цифрових урядових систем. Згідно з аналізом Joia & Zamot (2023), відсутність стандартизації в цифровому урядуванні призводить до ефекту «цифрових дискретностей», коли кожне відомство розвиває власні рішення без урахування інтеоперабельності, що значно знижує ефективність і збільшує вразливості всієї системи. Тобто, стандартизація є необхідною умовою для подолання цього ефекту.

Отже, детермінація стандартів:

1) уніфікує формати даних і протоколи взаємодії, що, за результатами досліджень Європейської рамки інтероперабельності (EIF, 2022), дозволяє скоротити час інтеграції систем до 70% і зменшити вартість підтримки на 40%;

2) задає інституційні вимоги до підключення нових учасників до спільного управлінського контуру (ЦОВВ, ОМС, держпідприємства), що відповідає принципам системної адаптивності за Мітлтоном-Келлі (2017);

3) мінімізує ризики «залежності» від окремих постачальників (vendor lock-in), оскільки робить вимоги до платформ публічними й відтворюваними. За даними Світового банку (2020), країни з високим рівнем стандартизації в середньому економлять до 25% бюджету на ІТ через зменшення залежності від єдиного постачальника.

Так, для Естонії саме чіткі стандарти обміну даними (X-Road) дозволили створити єдиний цифровий простір країни, де більше 900 організацій та 1300 сервісів працюють як цілісна екосистема.

По-третє, *забезпечення підзвітності та правової визначеності*. Фактично, коли критичні управлінські рішення (нарахування допомог, реєстрація статусів, доступ до пільг) приймаються за участю цифрових систем і алгоритмів, постає питання: хто відповідає за результат, якщо сталася помилка, дискримінація чи зловживання. Це явище отримало назву «проблеми розподіленої відповідальності» (distributed accountability problem) [387].

Отже, чіткі управлінські стандарти:

- закріплюють відповідальних суб'єктів (політичних, адміністративних, технічних) за кожним етапом цифрового процесу;
- роблять логіку роботи платформ прозорою для аудиту (у тому числі зовнішнього – антикорупційні органи, донори, громадськість), що, підвищує довіру громадян до державних сервісів;

– забезпечують узгодженість між юридичними приписами й технічною реалізацією, що відповідає концепції «code as law» та сучасним дослідженням у галузі правової інформатики.

По-четверте, *адаптація до європейського цифрового правового простору*. Вступ України до ЄС і приєднання до Єдиного цифрового ринку вимагають не лише гармонізації законів, а й сумісності управлінських практик і цифрових рішень. Дослідження європейської цифрової інтеграції вказують на критичну роль стандартів як «мосту» між нормативними вимогами та реальною інтеграцією національних систем. Аормалізація стандартів на національному рівні є найбільш ефективним механізмом імплементації директив та регламентів ЄС, оскільки дозволяє перевести загальні вимоги у конкретні технічні параметри.

Стандарти:

1) дозволяють перекласти вимоги DSA , DMA, GDPR, AI Act на мову конкретних управлінських і технічних вимог до українських органів влади та платформ, що скорочує час повної імплементації директив ЄС на 40-50%;

Тут *DSA – Digital Services Act* (повна назва «Regulation on a Single Market for Digital Services» – Регламент ЄС про цифрові послуги, який встановлює правила відповідальності онлайн-платформ (соцмереж, маркетплейсів тощо) за контент, прозорість алгоритмів, модерацію, боротьбу з дезінформацією та незаконним контентом.

DMA – Digital Markets Act (повна назва «Regulation on Contestable and Fair Markets in the Digital Sector» – Регламент ЄС про цифрові ринки, спрямований проти зловживань найбільших платформ («gatekeepers» – Google, Apple, Meta тощо), щоб забезпечити чесну конкуренцію, відкриті ринки та запобігти монополізації.

GDPR – General Data Protection Regulation (повна назва *General Data Protection Regulation (Regulation (EU) 2016/679)* – Загальний регламент ЄС про захист даних, який встановлює жорсткі правила обробки персональних даних, права суб'єктів даних та обов'язки організацій щодо конфіденційності

й безпеки.

2) створюють прогнозоване середовище для міжнародних партнерів і донорів, які працюють із даними та цифровими сервісами держави, що є ключовим фактором залучення інвестицій у цифрову інфраструктуру;

3) спрощують взаємне визнання електронних ідентичностей, довірчих послуг, реєстрових даних, що є критичним для інтеграції у транскордонні сервіси ЄС.

Досвід європейських країн показує, що саме рання формалізація цифрових стандартів відповідно до вимог ЄС дозволила цим країнам швидко інтегруватися в єдиний цифровий простір і отримати доступ до транскордонних послуг.

По-п'яте, *підтримка адаптивної розбудови інституційної спроможності*. Очевидно, що без чітко окреслених стандартів неможливо вибудувати сталі механізми навчання й розвитку персоналу, оновлення регламентів, бюджетного планування у цифровій сфері. Дослідження інституціональної спроможності в цифрову еру (О.Баштанник) [388-390] вказують на стандарти як ключовий елемент трансформаційних процесів. Саме тому слід визначити стандартизацію як інструмент подолання «культурної прірви» між традиційними управлінськими структурами та цифровими інноваціями. В умовах України це особливо актуально з огляду на необхідність паралельного розвитку державного управління та відбудови після руйнувань.

Загалом, детермінація стандартів:

- задає цільовий орієнтир для органів влади (до якого рівня цифрової зрілості та стійкості вони мають прийти), що є передумовою цілеспрямованої модернізації;

- дозволяє будувати системи оцінювання (на зразок авторської Digital Resilience Assessment), порівнювати підрозділи й відомства між собою, що відповідає принципам доказового державного управління (evidence-based governance);

– створює основу для керованої еволюції цифрових управлінських платформ (оновлення, міграція, консолідація), що знижує ризики катастрофічних змін і забезпечує стабільну траєкторію розвитку.

Наведений аналіз підтверджує, що потреба в детермінації цифрових управлінських стандартів має глибоке наукове обґрунтування та відповідає як сучасним теоретичним концепціям (від теорії високонадійних організацій до принципів алгоритмічної підзвітності), так і практичному досвіду країн, які успішно розвивають стійке цифрове урядування. В умовах України ця потреба посилюється поєднанням безпекових викликів, євроінтеграційних процесів та масштабної інституційної трансформації. На основі аналізу наукових досліджень, українського законодавства та європейських нормативних актів виокремлено десять цифрових управлінських стандартів, які спільно утворюють інституціональний фундамент НМС.

1) стандарти кібербезпеки, які задають мінімально необхідні вимоги до захисту систем і даних від кібератак і несанкціонованого доступу;

2) стандарти відкритого управління, що визначають режими прозорості, підзвітності й участі громадян;

3) стандарти цифрової інклюзії, спрямовані на забезпечення рівного доступу до цифрових послуг незалежно від місця проживання, соціально-економічного статусу чи віку;

4) стандарти якості публічних послуг в електронному форматі, які фіксують вимоги до швидкості, надійності, зручності та безпечності сервісів;

5) стандарти управління даними, що регламентують повний цикл роботи з даними – від збору й валідації до зберігання, обміну та повторного використання;

6) стандарти міжвідомчої взаємодії, які визначають правила інформаційного обміну між державними структурами, забезпечуючи інтероперабельність систем;

7) стандарти моніторингу й оцінювання, покликані забезпечити зворотний зв'язок щодо ефективності впроваджених цифрових рішень;

8) стандарти навчання та розвитку персоналу, що встановлюють вимоги до цифрових компетентностей публічних службовців;

9) стандарти адаптивності управлінських структур як набір принципів гнучкого реагування на зміни;

10) стандарти правового регулювання, які закріплюють правові основи цифрового врядування та імплементацію міжнародних норм.

Стандарти пропонується згрупувати у три кластери з позицій їхньої ролі в системі державного управління: фундамент безпеки, інфраструктура взаємодії та соціотехнічна підсистема, що поєднує інститути влади й суспільство (таблиця 5.8).

Таблиця 5.8

Класифікація цифрових управлінських стандартів НМС

Кластер	№	Стандарт (укр / англ.)	Ключова управлінська функція в НМС	Основні суб'єкти впровадження	Нормативні референси (ЄС / Україна)
1	2	3	4	5	6
I. База безпеки та правової визначеності	1	Стандарти кібербезпеки / Cybersecurity Standards	Задають мінімально необхідні вимоги до захисту ІС, мереж і реєстрів від кібератак, несанкціонованого доступу та саботажу; забезпечують збереження керованості державою в умовах кіберінцидентів.	РНБО, Держспецзв'язку, СБУ, МВС, профільні ЦОВВ, власники об'єктів критичної інфраструктури, ОМС	NIS2 Directive, ISO/IEC 27001, ENISA Guidelines / Закон України «Про основні засади забезпечення кібербезпеки України», акти про КІ, нормативи КСЗІ
	5	Стандарти управління даними / Data Governance Standards	Регламентують повний цикл роботи з даними – збір, валідацію, класифікацію, зберігання, доступ, обмін і повторне використання; забезпечують якість, цілісність і правомірність обробки як державних, так і персональних даних	Мінцифри, Мін'юст, Мінфін, розпорядники державних реєстрів, ЦОВВ секторів (охорона здоров'я, соц.захист, освіта тощо)	GDPR, Data Governance Act, Open Data Directive / Закон «Про захист персональних даних», акти про держреєстри, про відкриті дані
	10	Стандарти правового регулювання цифрового врядування / Legal & Regulatory Standards for Digital Governance	Закріплюють правові основи цифрового врядування, визначають статус електронних документів, сервісів, ідентичностей, а також імплементацію ключових міжнародних та європейських норм у національне право	Верховна Рада України, КМУ, Мін'юст, Мінцифри, профільні комітети ВР, Нацкомісії та регулятори секторів	DSA, DMA, GDPR, AI Act, eIDAS Regulation / закони про електронні довірчі послуги, електронні комунікації, медіа, кібербезпеку, цифрові послуги

Продовження таблиці 5.8

1	2	3	4	5	6
II. Інфраструктура взаємодії та управлінського контуру	6	Стандарти міжвідомчої взаємодії / Interagency Interaction & Interoperability Standards	Визначають правила інформаційного обміну між державними органами, забезпечують інтеоперабельність систем та уніфікацію форматів і протоколів, мінімізуючи дублювання й ручну обробку даних	Мінцифри, адміністратори базових реєстрів, ЦОВВ та ОМС як учасники системи електронної взаємодії, держпідприємства – провайдери платформ	European Interoperability Framework, Single Digital Gateway Regulation / закони та постанови про електронну взаємодію, система «Трембіта», акти про пріоритетність електронного документообігу
	7	Стандарти моніторингу й оцінювання / Monitoring & Evaluation Standards	Забезпечують формалізований зворотний зв'язок щодо ефективності цифрових рішень: визначають показники (KPI, індикатори стійкості), методології збору й аналізу даних, цикли звітування та корекції політик	КМУ, Мінцифри, Мінфін, НАДС, Рахункова палата, аналітичні центри, органи внутрішнього аудиту та стратегічного планування в ЦОВВ і ОМС	eGovernment Benchmark, DESI (Digital Economy and Society Index), OECD Digital Government Indicators / акти про моніторинг якості адмінпослуг, результати діяльності органів влади, методики оцінювання цифрової зрілості
III. Соціо-технічна система та людський вимір	2	Стандарти відкритого управління / Open Governance Standards	Визначають режими прозорості, підзвітності та участі громадян у прийнятті рішень; регламентують публікацію відкритих даних, електронні консультації, участь громадян у співтворенні політик	КМУ, ЦОВВ, ОМС, громадянське суспільство, антикорупційні органи, омбудсмени, наглядові ради	Open Data Directive, Open Government Partnership standards, Aarhus Convention / закони про доступ до публічної інформації, відкриті дані, публічні консультації, антикорупційне законодавство
	3	Стандарти цифрової інклюзії / Digital Inclusion Standards	Спрямовані на забезпечення рівного доступу до цифрових послуг незалежно від місця проживання, віку, стану здоров'я, соціально-економічного статусу; враховують потреби вразливих груп	Мінсоцполітики, Мінцифри, МОН, МОЗ, НАДС, ОМС, інституції з прав людини, громадські організації	WCAG 2.1/2.2, EN 301 549, European Accessibility Act / Стратегія безбар'єрності, нацстандарти доступності вебресурсів і мобільних застосунків, акти про інклюзивні послуги
	4	Стандарти якості публічних послуг в електронному форматі / E-Public Service Quality Standards	Фіксують вимоги до швидкості, надійності, узгодженості, зручності та безпечності електронних сервісів; інтегрують підхід «людиноцентричності» й «життєвих подій» у проектування послуг	Мінцифри, ЦОВВ – надавачі адмінпослуг, ЦНАП, ОМС, контакт-центри, служби підтримки користувачів	eGovernment Benchmark, Tallinn Declaration on eGovernment / Закон «Про адміністративні послуги», акти про надання е-послуг, UX/UI-гайдлайни для держсервісів, методики оцінювання задоволеності користувачів

Продовження таблиці 5.8

1	2	3	4	5	6
	8	Стандарти навчання та розвитку персоналу / Digital Capacity & Training Standards	Встановлюють вимоги до цифрових компетентностей публічних службовців, формують рамки підготовки, підвищення кваліфікації, сертифікації та безперервного професійного розвитку в цифровій сфері.	НАДС, МОН, Мінцифри, школи публічного управління, заклади вищої освіти, кадрові служби органів влади.	DigComp 2.2, EU Public Administration Competency Frameworks / Стратегія реформування держуправління, професійні стандарти держслужбовців, програми «Дія.Освіта», «Цифрограм».
	9	Стандарти адаптивності управлінських структур / Organisational Adaptivity Standards	Формують набір принципів і вимог до гнучкого реагування органів влади на зміни (кризи, технологічні інновації, нормативні оновлення), включно з перепроєктуванням процесів, делегуванням повноважень, створенням кросфункціональних команд.	КМУ, Секретаріат КМУ, ЦОБВ, ОМС, НАДС, урядові офіси реформ, CDTO в органах влади.	OECD Recommendation on Public Governance, OECD Principles on Digital Government, SIGMA Principles / акти про стратегічне планування, регуляторну політику, положення про CDTO, концепції цифрової трансформації секторів.

Джерело: розроблено автором

Наведена класифікація дозволяє побачити, як цифрові стандарти перетворюються на структурні елементи керуючого контуру держави. Стандарти фундаменту безпеки гарантують, що базові «життєві функції» цифрової держави не будуть зруйновані навіть за умов цілеспрямованих атак. Інфраструктурні стандарти визначають, яким чином вхідні сигнали (дані) циркулюють між органами влади, як формується спільна управлінська картина, як швидко й без втрат передається управлінський вплив від центру до периферії. Соціотехнічні стандарти, у свою чергу, регулюють взаємодію держави з громадянами як з повноцінними учасниками управлінського процесу, формуючи канали зворотного зв'язку, через які система може оцінювати власну результативність і коригувати політики.

Наведений аналіз підтверджує, що потреба в детермінації цифрових управлінських стандартів має глибоке наукове обґрунтування та відповідає як сучасним теоретичним концепціям (від теорії високонадійних організацій до принципів алгоритмічної підзвітності), так і практичному досвіду країн, які успішно розвивають стійке цифрове урядування. В умовах України ця потреба посилюється поєднанням безпекових викликів, євроінтеграційних

процесів та масштабної інституційної трансформації.

У цьому контексті знаковою подією стало видання наказу Адміністрації Держспецзв'язку № 54 у січні 2025 року, яким затверджено базові заходи з кіберзахисту на основі NIST Cybersecurity Framework (CSF) 2.0 [391]. Це рішення можна розглядати як інституційне «коригування» попередньої парадигми, яке формалізує відмову від домінування суто техніко-формальних підходів на користь комплексного фреймворку, розробленого Національним інститутом стандартів і технологій США, що орієнтує державні органи на системне управління кіберризиками. Фреймворк NIST CSF 2.0 базується на шести ключових функціях: управління (Govern), ідентифікація (Identify), захист (Protect), виявлення (Detect), реагування (Respond) та відновлення (Recover). На відміну від попередніх версій, включення функції Govern має принципове значення для системи державного управління. Воно фактично піднімає кібербезпеку з рівня «технічної задачі IT-підрозділу» до рівня керуючої підсистеми, де вищий менеджмент органу влади зобов'язаний:

- 1) установлювати цілі та політику кібербезпеки як частину загальної стратегії розвитку організації;
- 2) визначати прийнятний рівень ризику та пріоритети його зниження;
- 3) забезпечувати ресурсне, кадрове й організаційне підкріплення заходів безпеки;
- 4) інтегрувати вимоги кібербезпеки в цикли планування, закупівель, управління проєктами й кадрової політики.

Таким чином, NIST CSF 2.0 виступає не просто технічним орієнтиром, а управлінським стандартом, який задає еталонну структуру процесів для національного стандарту «Кібербезпека та захист критичної інфраструктури» в межах Національної моделі стійкості. Функції Identify–Protect–Detect–Respond–Recover, у свою чергу, дозволяють деталізувати вимоги до операційного рівня: від інвентаризації активів і вразливостей до процедур реагування й відновлення, що напряду пов'язано з параметрами стійкості,

закладеними у класифікації цифрових управлінських стандартів (час відновлення, рівень резервування, глибина моніторингу). Впровадження NIST CSF 2.0 є обов'язковим для об'єктів критичної інформаційної інфраструктури. Це означає, що ключові елементи цифрового «скелета» держави – енергетичні, транспортні, фінансові, телекомунікаційні системи, державні реєстри, інформаційні системи сектору безпеки й оборони – переходять на уніфікований, ризик-орієнтований підхід до безпеки. Показовим прикладом є діяльність Державного оператора тилу (ДОТ), який розпочав сертифікацію системи управління постачанням Збройних Сил України «DOT-Chain» відповідно до NIST Risk Management Framework (RMF) [392]. У цьому випадку NIST виступає не лише як внутрішній орієнтир, а й як мова сумісності з інформаційними системами країн-членів НАТО, що:

- полегшує інтеграцію з союзницькими логістичними платформами;
- знижує ризики помилок і неузгодженостей у спільних операціях;
- підвищує довіру до українських інформаційних систем як до елементів ширшої коаліційної інфраструктури.

З позицій нашої класифікації цифрових управлінських стандартів, NIST CSF 2.0 і NIST RMF можна інтерпретувати як еталонні зовнішні рамки для:

- стандартів кібербезпеки – визначення мінімально необхідних заходів захисту й процедур управління інцидентами;
- стандартів управління даними – зокрема в частині класифікації активів, оцінки їх критичності, побудови моделей загроз;
- стандартів моніторингу й оцінювання – завдяки використанню показників зрілості процесів і ризик-орієнтованих метрик;
- стандартів адаптивності управлінських структур – оскільки NIST закріплює циклічну логіку періодичного перегляду політик, процедур і налаштувань систем залежно від зміни загроз і контексту.

Особливо важливим є те, що впровадження NIST CSF 2.0 фактично задає шаблон управлінського контуру у сфері кібербезпеки: від

формулювання політики та визначення ролей (Govern), через ідентифікацію об'єктів захисту й загроз (Identify), побудову бар'єрів (Protect) та систем моніторингу (Detect) – до структурованого реагування (Respond) і відновлення (Recover) з обов'язковим аналізом уроків. У такий спосіб безпекова підсистема держави набуває властивостей, притаманних стійким керованим системам: вона здатна не лише фіксувати відхилення від нормального режиму, а й повертатися до нього або формувати новий, більш захищений стан.

Разом з тим, імплементація NIST CSF 2.0 виявляє значний диференціал спроможності між різними рівнями публічної влади. Якщо в секторах оборони, фінансів, національного зв'язку спостерігається відносно високий рівень готовності до переходу на ризик-орієнтовані моделі (наявність профільних фахівців, досвіду міжнародної взаємодії, доступу до експертної підтримки), то на рівні органів місцевого самоврядування виникає низка проблем:

- кадровий дефіцит фахівців із кібербезпеки та управління ІТ-активами;
- ресурсні обмеження, що не дозволяють створювати повноцінні служби безпеки чи закуповувати комплексні рішення;
- організаційна інерція, коли питання безпеки залишаються периферійними щодо «традиційних» напрямів діяльності (ЖКГ, благоустрій, соціальні послуги).

У такій ситуації NIST CSF 2.0 для багатьох громад працює радше як цільовий орієнтир, до якого необхідно наблизитися поетапно, через стандартизацію базових процедур (керування обліковими записами, резервне копіювання, оновлення ПЗ, мінімізація прав доступу тощо) та поступову інтеграцію їх у локальні регламенти. Це безпосередньо пов'язано зі стандартами навчання та розвитку персоналу (8), оскільки без підготовлених кадрів на місцях навіть найкращі рамкові документи залишаються формальними.

З урахуванням гармонізації з європейським правом важливо, що впровадження NIST CSF 2.0 не суперечить, а доповнює вимоги Директиви NIS2, стандартів ISO/IEC 27001 та інших європейських рамок. Вони можуть бути інтегровані в єдиний національний профіль кібербезпеки, де:

- 1) NIS2 і GDPR задають регуляторні вимоги й зони відповідальності суб'єктів;
- 2) ISO/IEC 27001 визначає структуру системи управління інформаційною безпекою (ISMS);
- 3) NIST CSF 2.0 надає процесну модель управління ризиками, адаптовану для практичного застосування органами влади та операторами інфраструктури.

У підсумку, впровадження NIST CSF 2.0 можна розглядати як перший системний крок до формування в Україні узгодженого набору цифрових управлінських стандартів у сфері безпеки, що перетворює кібербезпеку на інтегровану частину Національної моделі стійкості, пов'язуючи стандарти кіберзахисту із стандартами управління даними, міжвідомчої взаємодії, моніторингу та інституційної адаптивності.

5.4. Інституціональні механізми реалізації НМС

Національна модель стійкості розглядається як цілісна архітектура державного управління, покликана забезпечити здатність держави та суспільства протистояти системним викликам, адаптуватися до них і відновлюватися на вищому рівні функціонування. Однак стійкість не виникає лише внаслідок ухвалення концепцій чи стратегій, вона формується через конкретні інституціональні механізми, які закріплюють розподіл повноважень, відповідальності, ресурсів і процедур взаємодії між суб'єктами публічної влади, суспільством і приватним сектором.

Традиційні моделі державного управління й інституціонального розвитку спиралися на декілька базових припущень, які в сучасному

контексті перманентної кризи втрачають актуальність: по-перше, *стабільність і передбачуваність середовища*, за наявності припущення, що зміни будуть поступовими, а кризи – рідкісними й обмеженими; по-друге, *лінійність інституційних змін*, коли передбачається, що інституції розвиваються за чітко спланованою траєкторією (від точки А до точки Б); по-третє, *централізоване планування*, за сталого переконання, що реформи найефективніші, коли їх координує єдиний центр прийняття рішень; по-четверте, універсальність моделей, на основі впевненості щодо можливості перенесення готових організаційних рішень з одного контексту в інший.

National E-Resilience як національну модель інтегрованого управління передбачає створення інтегрованої цифрової платформи, що забезпечує оперативний обмін даними та координацію дій усіх суб'єктів НМС. Це вимагає відходу від фрагментарної цифровізації окремих відомств до побудови цілісної архітектури, де стійкість є вбудованою характеристикою (*resilience by design*).

Реалізація НМС вимагає відмови від статичних, жорстко ієрархічних структур на користь динамічних систем, здатних до саморегуляції, навчання та швидкої адаптації. У цій логіці ключовим інструментом переходу виступає механізм *Adaptive Institutional Capacity Building (AICB)* – адаптивної інституційної розбудови, що забезпечує спроможність публічної адміністрації не лише витримувати зовнішні шоки, але й еволюціонувати під їхнім тиском. Для концептуального обґрунтування та операціоналізації AICB, необхідно спиратися на низку взаємодоповнюючих теоретико-методологічних підходів.

Сучасні реалії, особливо для України в умовах повномасштабної війни, кардинально трансформували ці припущення. Теоретично обґрунтований перехід до адаптивного підходу вимагає переосмислення самої природи інституційних змін. Теоретичні основи AICB пропонується формувати на перетині кількох наукових парадигм:

- 1) теорія комплексних адаптивних систем (*Complex Adaptive Systems*),

яка розглядає інституції як багаторівневі системи взаємодіючих агентів, здатних адаптуватися до змін середовища через самоорганізацію, навчання та еволюцію;

2) теорія інституційних змін, що аналізує механізми формальних і неформальних правил, які структурують взаємодію між суб'єктами, та вивчає процеси їх трансформації.

3) теорія організаційної стійкості (organizational resilience), яка досліджує, як організації підтримують функціонування в умовах стресу та дестабілізації;

4) теорія проблемно-орієнтованої політики (problem-driven iterative adaptation), що зосереджується на інкрементальних, контекстно-чутливих підходах до розв'язання конкретних проблем замість перенесення готових моделей.

5) теорія цифрової трансформації державного управління, що вивчає, як цифрові технології змінюють структуру, процеси та механізми державного управління.

Adaptive Institutional Capacity Building (AICB), на відміну від класичної «розбудови спроможності» (capacity building), часто зосереджується на накопиченні ресурсів (кадрів, техніки, фінансів), фокусується на динамічних властивостях системи державного управління, її здатності змінювати власну структуру та функції в реальному часі.

Парадигма Adaptive Institutional Capacity Building (AICB) постає як відповідь на обмеження традиційних моделей інституційного розвитку, що виходили з припущення про відносну стабільність середовища, можливість довгострокового планування та домінування ієрархічних структур. На відміну від класичної логіки, орієнтованої на створення фіксованих організаційних форм і комплексних реформ «згори донизу», AICB виходить із розуміння інституцій як комплексних адаптивних систем, які мають постійно переналаштовувати свої процедури, структури та компетентності у відповідь на зміну контексту. У порівняльному плані це зближує AICB із

практиками країн, що функціонують у режимі постійних загроз. Так, Ізраїль демонструє пріоритет культивування організаційної гнучкості та швидкого навчання в секторі безпеки; Естонія розглядає цифрову державу як «постійний стартап», де ключові платформи спроектовано модульно, із закладеною можливістю швидких змін; Фінляндія розвиває модель «всеосяжної безпеки», у якій інституційна стійкість забезпечується через широку участь суспільства та мережеву координацію, а не лише через вертикаль управління. Правовий режим воєнного стану в Україні від 2022 року створив унікальне емпіричне поле для прояву логіки АІСВ у сфері державного управління, демонструючи адаптивність як багаторівневий процес безперервного циклу діагностики, експериментування, масштабування та інституціоналізації. Обласні військові адміністрації та громади формували кризові штаби на базі Указу Президента України про запровадження правового режиму воєнного стану, адаптуючи плани евакуації (понад 2 млн евакуйованих, з використанням ГІС-систем для щоденної корекції маршрутів у 15+ регіонах), перерозподіляли повноваження між цивільними та військовими компонентами через тимчасові регламенти КМУ, використовуючи цифрові реєстри для моніторингу (понад 10 млн запитів до Єдиного реєстру ВПО), геоінформаційні системи та системи оповіщення як інструменти постійної корекції рішень.

Характерно, що значна частина цих змін не була заздалегідь передбачена законодавством, а виникала як послідовність малих інституційних експериментів, які згодом інкорпоровалися в акти Президента та постанови КМУ про функціонування публічної влади в умовах воєнного стану, демонструючи адаптивність як системну властивість: швидкість реакції (середній час коригування норм – 7-14 днів), використання даних для рекурсивного навчання (аналіз 1 млрд+ транзакцій у «Дії» для 40+ ітерацій процесів) та баланс між централізованими орієнтирами й локальною автономією (громади адаптували 70%+ процедур самостійно). На цьому тлі механізм АІСВ можна інтерпретувати як спробу теоретично узагальнити й

систематизувати такі підходи: замість разових структурних реформ пропонується безперервний цикл діагностики, експериментування, масштабування та інституціоналізації успішних практик; замість домінування централізованих приписів – поєднання стратегічних орієнтирів із високим ступенем автономії «периферії» у виборі засобів досягнення цілей. Для України, що одночасно перебуває в полі військової агресії та глибокої трансформації, АІСВ дає методологічну рамку, яка дозволяє не механічно запозичувати естонські, ізраїльські чи скандинавські рішення, а будувати власну траєкторію через послідовні, контекстуально вмотивовані інституційні адаптації, використовуючи цифрові платформи як середовище швидких змін, а правовий режим воєнного стану – як каталізатор інституційного навчання.

Варто детермінувати принципи-аксіоми АІСВ:

- 1) принцип адаптивності – інституціональна спроможність визначається передусім здатністю до змін, а не стабільністю структур;
- 2) принцип рекурсивного навчання – інститути повинні безперервно накопичувати, аналізувати та інтегрувати знання про власну діяльність, постійно переоцінюючи свої припущення і стратегії;
- 3) принцип контекстуальності – вказує, що немає універсальних інституційних рішень; ефективні підходи завжди вкорінені в місцевому контексті, історії та культурі;
- 4) принцип розподіленого прийняття рішень – адаптивність вимагає децентралізації повноважень, щоб рішення приймалися на рівні, найближчому до проблеми (аналог субсидіарності);
- 5) принцип модульності та зв'язності – детермінує стан системи державного управління, коли інститути мають бути організовані як система взаємопов'язаних, але відносно незалежних модулів, де проблеми в одному компоненті не призводять до каскадного колапсу;
- 6) принцип керованої надлишковості, за яким критичні функції повинні мати альтернативні механізми реалізації, навіть якщо це знижує

короткострокову ефективність всієї системи;

7) принцип відкритих рамок, за яким інституціональні структури мають забезпечувати простір для інновацій, експериментування та залучення нових агентів.

З позицій неоінституціоналізму АІСВ можна визначити як цілеспрямований, керований даними процес реінституціоналізації, що включає: діагностику наявних правил і практик (виявлення «розривів» між формальними нормами й реальною поведінкою); переосмислення та реінженіринг інститутів (оновлення процедур, моделей взаємодії, розподілу повноважень); закріплення змін у правових актах, організаційних регламентах і цифровій інфраструктурі (нормативно-алгоритмічний формат); постійний перегляд цих інститутів на основі результатів і нових загроз.

АІСВ як складна екосистему правових, організаційних, технологічних та кадрових трансформацій пов'язана у методологічному плані з Digital Resilience Assessment (DRA) – методологією оцінювання цифрової стійкості, яка виконує функцію діагностичного ядра та механізму зворотного зв'язку в процесі адаптації. Саме тому цифрові управлінські стандарти (досліджені у цьому розділі), визначені в рамках НМС, набувають нового значення крізь призму АІСВ:

1) стандарти кібербезпеки трансформуються з набору статичних вимог на динамічну систему безперервної адаптації безпекових практик до проблеми еволюції загроз (принцип «security by design» доповнюється принципом «security by adaptation»;

2) стандарти управління даними стають основою для розвитку «стратегічної сенсорики» інституцій, їх здатності збирати, аналізувати й інтерпретувати сигнали середовища для швидкої адаптації;

3) стандарти міжвідомчої взаємодії визначають не лише технічні протоколи, а й регламенти для горизонтальної координації та формування тимчасових структур в умовах криз;

4) стандарти якості публічних послуг інкорпорують механізми для

швидкого переналаштування сервісних моделей відповідно до зміни потреб і можливостей.

Adaptive Institutional Capacity Building виступає як процесний, динамічний вимір, своєрідний «двигун», що приводить у дію НМС. Якщо НМС задає цільовий профіль стійкості (якою система має бути), то АІСВ описує технологію постійних ітерацій змін, завдяки яким ця система наближається до цільового стану – через реорганізацію інститутів, експериментування з форматами послуг, перегляд регламентів, удосконалення кадрових та цифрових спроможностей. У глобальному порівняльному контексті (практики Естонії, Ізраїлю, Фінляндії) можна побачити спільну закономірність, коли успішні моделі стійкості завжди спираються на адаптивні контури інституціональної розбудови, де управлінські експерименти, зворотний зв'язок і швидка декомпозиція правил є не аномалією, а штатним режимом функціонування. Україна, особливо в умовах правового режиму воєнного стану, фактично вже діє в логіці АІСВ, хоча цей механізм ще не завжди рефлексований і формалізований як окрема парадигма. У таблиці 5.9 подано концептуалізовану матрицю взаємодії НМС та АІСВ за основними компонентами стійкості, при чому НМС розуміється як набір цільових вимірів стійкості, а АІСВ як набір процесних механізмів, через які ці виміри досягаються та підтримуються.

Таблиця 5.9

АІСВ як механізм реалізації компонентів НМС

Компонент НМС	Цільовий стан стійкості (що має забезпечувати НМС)	Роль АІСВ (механізм реалізації)	Приклади інструментів / індикаторів
1	2	3	4
Суспільна стійкість	Соціальна згуртованість, захищеність вразливих груп, безперервність доступу до базових послуг навіть під час криз	Забезпечення цифрової інклюзії та безперервності соціальних виплат через цифрові платформи (зокрема «Дія») з постійною адаптацією сервісів до нових категорій населення й умов середовища	Кількість отримувачів виплат через е-канали; частка ВПО, охоплених цифровими послугами; скорочення часу призначення допомоги; адаптація інтерфейсів під різні групи

Продовження таблиці 5.9

1	2	3	4
Інституційна стійкість	Здатність органів влади зберігати й відновлювати функціональність, забезпечувати керування у надзвичайних ситуаціях	Оптимізація й перерозподіл функцій органів влади (функціональний аудит), релокація даних і критичних систем у хмарну інфраструктуру	Проведені функціональні аудити; скорочення дублювання повноважень; частка ключових реєстрів у хмарі; час відновлення після інцидентів (RTO/RPO)
Кіберстійкість	Захищеність критичних інформаційних ресурсів та інфраструктури від кібератак, здатність систем функціонувати під час загроз	Впровадження стандартів кіберзахисту, регулярні «кібер-аудити», створення SOC/CSIRT, системне навчання персоналу та побудова механізмів швидкого оновлення політик безпеки	Відсоток систем, сертифікованих за стандартами (ISO/NIST/нацстандарти); кількість проведених аудитів; середній час виявлення/реагування на інциденти; охоплення навчанням
Правова стійкість	Своєчасне оновлення нормативної бази, здатність права оперативно легітимізувати нові практики та режими управління	Використання процедур fast-track законодавства й підзаконної нормотворчості для швидкої легалізації нових практик, з подальшою їх кодифікацією й уніфікацією	Кількість надзвичайних процедур ухвалення актів; середній час від виявлення потреби до набрання чинності; частка тимчасових актів, інтегрованих у сталу правову систему
Економічна стійкість	Здатність економіки підтримувати базові ланцюги постачання, фінансову стабільність та інвестиційну привабливість під час шоків	Адаптивне бюджетування й перерозподіл ресурсів, впровадження гнучких режимів регулювання для бізнесу, цифровізація податкових і митних процедур із можливістю швидкого спрощення/посилення вимог	Частка операцій у податковій та митній сферах онлайн; час адаптації податкових режимів до кризових умов; обсяги підтримки бізнесу, наданої через цифрові інструменти
Інфраструктурна стійкість	Безперервність функціонування критичної інфраструктури (енергетика, транспорт, зв'язок) у разі фізичних та кіберзагроз	Побудова модульних, резервованих інфраструктурних рішень, застосування цифрових систем моніторингу стану мереж, гнучке перепланування маршрутів і режимів роботи на основі даних у реальному часі	Кількість резервованих об'єктів/каналів; частка інфраструктури, підключеної до систем моніторингу; час відновлення послуг після атак/аварій; гнучкість маршрутів логістики
Інформаційно-комунікаційна (когнітивна) стійкість	Здатність суспільства та інституцій протидіяти дезінформації, підтримувати довіру та ефективні канали комунікації	Розгортання адаптивних систем стратегічних комунікацій, моніторинг інформаційного середовища, швидке коригування наративів і форматів донесення інформації, включно з двостороннім цифровим зворотним зв'язком	Показники довіри до інституцій; охоплення офіційних комунікаційних каналів; кількість виявлених/нейтралізованих дезінформаційних кампаній; швидкість оновлення офіційних повідомлень

RTO (Recovery Time Objective) – цільовий час відновлення (максимально допустимий час, протягом якого система або послуга може бути недоступною після інциденту).

RPO (Recovery Point Objective) – цільова точка відновлення (максимально допустима втрата даних у часі, яка вимірюється проміжком між останньою доступною резервною копією і моментом інциденту).

Ця матриця відображає кілька важливих теоретико-методологічних висновків:

по-перше, AICB є крос-секторальним механізмом, який не обмежується окремою сферою (наприклад, кібербезпекою чи цифровими послугами), а синхронізує усі компоненти НМС, від соціальної політики до правової системи та інфраструктури;

по-друге, цільові стани НМС завжди мають операційний «вимір AICB», адже стійкість не є статичним результатом, а підтримується серією малих і великих адаптацій, що реалізуються через цифрові управлінські платформи (зокрема, C-eGovPro), нормативні зміни, організаційні реформи та навчання;

по-третє, індикатори (як видно з таблиці) задають основу для емпіричних досліджень, їх можна використовувати для побудови систем оцінювання «адаптивної зрілості» держави, порівняння галузей і регіонів, а також для міжнародних порівнянь.

На основі проведеного дослідження цифрову резильєнтність інституцій у контексті НМС доцільно визначити як комплексну соціотехнічну властивість публічних органів влади, що поєднує технологічну, організаційну та правову складові. Цифрова резильєнтність інституцій – це спроможність органів публічної влади забезпечувати безперервність, адаптацію та відновлюваність своїх функцій, сервісів і цифрової інфраструктури в умовах цифрових та комплексних кризових шоків (кібератаки, блекаути, руйнування інфраструктури, масові переміщення населення тощо), зберігаючи при цьому керованість, легітимність і відповідність вимогам верховенства права.

Ключовою передумовою цифрової резильєнтності є інституціональна гнучкість, яка виступає внутрішньою організаційною характеристикою суб'єктів публічної влади: інституціональна гнучкість – властивість органів публічної влади та пов'язаних із ними організаційних структур оперативно змінювати свою архітектуру (структуру підрозділів, розподіл повноважень), управлінські процедури та інструменти (включно з цифровими), реагуючи на нові виклики й шоки без критичної втрати керованості, підзвітності та якості публічних послуг.

У запропонованій рамці дисертаційного дослідження інституціональна гнучкість виступає організаційною умовою, що дозволяє інститутам переформатовуватися, тоді як цифрова резильєнтність інститутів є цільовою характеристикою їх спроможності підтримувати та відновлювати цифрові функції в умовах криз, спираючись на цю гнучкість. Важливо також концептуалізувати у межах АІСВ систематизовані процеси організаційного пізнання, що дозволяють інститутам не лише реагувати на зміни, а й передбачати їх та проактивно адаптуватися. АІСВ оперує на декількох рівнях організаційного навчання:

1) операційне навчання (single-loop learning) – коригування дій в межах існуючих параметрів і процедур для усунення відхилень від очікуваних результатів;

2) тактичне навчання (double-loop learning – перегляд базових припущень і правил, що визначають дії інститутів, зміна самих параметрів і критеріїв успішності;

3) стратегічне навчання (triple-loop learning) – метакогнітивний рівень, на якому інституція трансформує сам процес свого навчання, розвиваючи спроможність адаптуватися до ще невідомих викликів;

4) колективне рефлексивне навчання – спільне осмислення досвіду різними суб'єктами НМС, формування спільної мови та розуміння для координованої адаптації.

Таким чином, АІСВ є не просто одним із механізмів реалізації НМС, а

фундаментальним переосмисленням природи і призначення державних інституцій в умовах невизначеності та перманентних криз. AICB формує нову управлінську парадигму, яка замінює прагнення до «оптимального стану» інститутів на розвиток їх здатності еволюціонувати; переходить від циклу «планування → впровадження» до циклу «експериментування → навчання → адаптація», інтегрує цифрові технології не як засіб автоматизації, а як середовище для інституціональної гнучкості; розглядає громадян і бізнес не лише як отримувачів послуг, а як співтворців адаптивних рішень; переосмислює ефективність як здатність змінюватися відповідно до контексту, а не як оптимізацію під статичні умови. AICB як теоретико-методологічна основа НМС не лише відповідає на поточні виклики, з якими стикається Україна, але й формує новий горизонт розвитку системи публічного управління в цілому.

Національна модель стійкості та механізм AICB формують інституціональну рамку, у межах якої держава переходить від реактивного управління до проактивної та адаптивної моделі публічної політики. Саме тому ключовими передумовами такої трансформації є інституційна гнучкість, цифрова резильєнтність інституцій та правова стійкість, які разом забезпечують спроможність органів влади не лише виживати в умовах шоків, а й відновлюватися на якісно новому рівні. Водночас самих лише організаційних і правових змін у системі державного управління недостатньо, якщо операційний контур публічної політики залишається інерційним, повільним і надмірно залежним від ручних рішень. Практика воєнного часу продемонструвала, що традиційні інструменти планування, нормотворчості та моніторингу не встигають за динамікою безпекових, економічних і соціальних процесів. Це породжує потребу в таких рішеннях, які дозволяють адаптувати політику в реальному часі, спираючись на дані, прогнозу аналітику та єдину цифрову інфраструктуру. Саме в цьому контексті виникає необхідність розгорнути подальший аналіз у площині авторських концептів Smart Digital Policies (розумних цифрових політик) та

інституціонального SaaS (Institutional Software as a Service). Ці концепти виступають логічним продовженням попередніх теоретичних напрацювань, адже вони показують, як саме ідеї AICB, інституціональної гнучкості та цифрової резильєнтності можуть бути втілені у вигляді конкретних цифрових рішень, платформ та алгоритмів, що щоденно «прокручують» механізми стійкості в публічному управлінні.

У контексті теоретичного обґрунтування Adaptive Institutional Capacity Building (AICB), інституційної гнучкості, цифрової резильєнтності інституцій та правової стійкості важливо концептуалізувати новий формат публічної політики – Smart Digital Policies, а також пов'язану з ним інфраструктурну модель Institutional Software as a Service (інституціонального SaaS), що разом формують операційну основу National E-Resilience.

Smart Digital Policies пропонується трактувати як якісно новий тип публічної політики, в основі якого лежить не лише текст нормативного акту, а й програмно реалізовані алгоритми, сценарні моделі та динамічні параметри, що забезпечують безперервну адаптацію управлінських рішень до змін середовища. У академічному значенні Smart Digital Policies доцільно визначити як «цифрово закріплені, даноцентричні та алгоритмічно керовані публічні політики, що формуються й реалізуються на основі штучного інтелекту, прогнозової аналітики та динамічного сценарного моделювання, забезпечуючи адаптацію управлінських рішень у режимі, максимально наближеному до реального часу, без необхідності постійних масштабних змін нормативно-правової бази, за умови дотримання засад верховенства права, підзвітності та прозорості».

На відміну від традиційних політик, які фіксуються переважно у вигляді статичних нормативних приписів, Smart Digital Policies функціонують як «живі» конфігурації – сукупність взаємопов'язаних алгоритмів, порогових значень, показників ризику та сценарних гілок, що можуть бути оперативно переналаштовані через цифрову інфраструктуру відповідно до змін економічної, безпекової та соціальної ситуації. Такий

підхід дозволяє перемістити значну частину адаптивності з рівня формальної нормотворчості на рівень політики як керованої алгоритмічної системи, зберігаючи стабільність базових правових рамок і водночас підвищуючи швидкість реакції на шоки та невизначеність.

У свою чергу, концепція Institutional Software as a Service (інституційного SaaS) у межах цього дослідження виконує роль соціотехнічної інфраструктури, у якій Smart Digital Policies набувають операційної форми. Інституційний SaaS доцільно визначити як «єдину багатосуб'єкторендну (multi-tenant) хмарну платформу для органів публічної влади, що функціонує у форматі програмного забезпечення як послуга (Software as a Service) і надає стандартизований набір модулів планування, моніторингу, аналізу, управління ризиками та підтримки прийняття рішень, у яких інституційні правила, процедури та політики трансформуються у програмному коді, даних та конфігурованих алгоритмах».

На відміну від фрагментованих відомчих інформаційних систем, інституційний SaaS виступає не просто технічним рішенням, а інституційною інфраструктурою нового покоління, що: по-перше, забезпечує модульну та масштабовану цифрову архітектуру для центральних і місцевих органів влади; по-друге, уніфікує управлінські інструменти (шаблони звітності, показники ефективності, моделі прогнозування, аналітичні панелі) та формує спільний простір даних; по-третє, створює операційне середовище, у якому AICB реалізується як безперервний цикл оновлення, тестування та тиражування інституційних рішень. У такій конфігурації інституційна гнучкість матеріалізується через можливість швидкого підключення, конфігурації та ре-конфігурації модулів платформи, а цифрова резильєнтність інституцій – через резильєнтну, розподілену й стандартизовану хмарну архітектуру, здатну забезпечувати безперервність, відновлюваність і інтероперабельність ключових управлінських процесів. Взаємодія Smart Digital Policies та Institutional SaaS, таким чином, формує цілісний інституційно-цифровий комплекс, у межах якого політика

розглядається як сервіс (policy-as-a-service), реалізований у вигляді конфігурованих алгоритмів і сценаріїв на єдиній платформі, а National E-Resilience – як здатність держави підтримувати та відновлювати функціонування цієї платформи, її даних та вмонтованих у неї політик в умовах багатовимірних криз і шоків. У запропонованій логіці Smart Digital Policies розглядаються як новий тип публічної політики, що: по-перше, ґрунтується на алгоритмічній адаптивності (застосування штучного інтелекту, сценарного моделювання, прогнозової аналітики); по-друге, забезпечує динамічну конфігурацію управлінських рішень без постійної зміни нормативно-правової бази; по-третє, дозволяє моделювати наслідки управлінських впливів до їх фактичного впровадження, знижуючи ризики й вартість помилок. Це означає, що політика перестає бути виключно формальним текстом нормативного акту і набуває форми програмованої, даноцентричної архітектури, яка може оновлюватися через зміну параметрів, алгоритмів та сценаріїв, а не лише через формальну зміну закону чи постанови. Таким чином, Smart Digital Policies стають цифровим інтерфейсом між правовою стійкістю та інституційною гнучкістю.

Таблиця 5.10

Інтегровний аналіз інституціональних механізмів НМС

Критерій	Smart Digital Policies	Institutional SaaS	National E-Resilience
1	2	3	4
Онтологічний статус	Тип публічної політики нового покоління (algorithmic / data-driven policy)	Соціотехнічна інфраструктура (хмарна платформа, цифрова ОС для інституцій)	Цільовий стан НМС в цифровому вимірі; інтегральна характеристика здатності держави зберігати й відновлювати цифрові функції під час криз
Рівень	Змістовий та алгоритмічний рівень політики (логіка рішень)	Інфраструктурний та операційний рівень (інструменти, платформи, дані)	Макрорівень національної системи (державна, суспільство, критична та цифрова інфраструктура)
Основний фокус	Що і як змінюється в політиці на основі даних, ризиків і сценаріїв.	Як організовано спільне цифрове середовище для інституцій (модулі, платформи, дані)	Яким є цілісний рівень стійкості цифрової екосистеми держави та її здатності діяти у кризах.

Продовження таблиці 5.10

1	2	3	4
Зміст	Цифрово закріплені, даноцентричні, алгоритмічно керовані політики, що використовують ШІ, прогнозу аналітику та сценарне моделювання для адаптації управлінських рішень у режимі, наближеному до реального часу, без постійних змін НПА	Єдина багатоклієнтська / багатосуб'єктна (multi-tenant) хмарна платформа для органів публічної влади у форматі SaaS, що надає стандартизовані модулі планування, моніторингу, аналізу, управління ризиками та підтримки рішень	Інтегральна здатність держави підтримувати, захищати й відновлювати цифрові сервіси, ресстри, платформи та дані, забезпечуючи безперервність критичних функцій управління і прав людини під впливом багатовимірних шоків
Тип адаптивності	Змістова й алгоритмічна: параметри політик, сценарії, пороги ризику	Інфраструктурна й організаційна: підключення/масштабування модулів, тиражування рішень	Системна: узгоджена адаптація інституцій, інфраструктур, правових режимів і цифрових сервісів на національному рівні
Зв'язок з AICB	Операціоналізація AICB у площині політик (policy-as-code, сценарне управління)	«Операційна система» AICB: середовище тестування, оновлення й масштабування інст. інновацій	Стратегічна мета AICB: AICB розглядається як механізм поступового нарощування національної електронної стійкості
Роль в інституційній гнучкості	Робить гнучкими самі політики, дозволяє швидко змінювати логіку рішень без постійних змін законів	Дозволяє інститутам змінювати організацію роботи через модулі платформи, не будує власні системи	Вимагає та консолідує інституційну гнучкість на рівні всієї держави (координація, розподіл повноважень, спільні стандарти)
Роль у цифровій резильєнтності інституцій	Забезпечує «інтелектуальну» резильєнтність: політики автоматично реагують на зміни контексту	Забезпечує «структурну» резильєнтність: хмарна, модульна, розподілена архітектура знижує ризики відмов	Є надсистемною рамкою: цифрова резильєнтність окремих інституцій інтегрується у національний контур стійкості
Вплив на правову стійкість	Зменшує нормативне перевантаження, зміщуючи адаптацію на рівень конфігурації політик у межах стабільних правових рамок	Полегшує імплементацію правових норм через стандартизовані модулі, показники, регламенти в коді	Вимагає режимів надзвичайних повноважень, процедур швидкої, але легітимної адаптації права для підтримки цифрових систем у кризах

Продовження таблиці 5.10

1	2	3	4
Ключові інструменти	Алгоритми III, сценарне моделювання, прогнозна аналітика, rule engines, системи управління ризиками	Хмарна платформа, стандартизовані модулі (планування, моніторинг, аналітика, ризики), API, реєстри	Національні стратегії, рамкові закони, стандарти безпеки й інтероперабельності, розподілені дата-центри, резервні канали зв'язку, кіберзахист
Об'єкт впливу	Логіка прийняття рішень, параметри політик, моделі розподілу ресурсів	Управлінські процеси інституцій, їх цифрові інструменти та обіг даних	Національна система як ціле: сукупність інституцій, цифрових і критичних інфраструктур та їхня взаємодія
Типовий результат впровадження	Менший лаг між шоком і корекцією політики, кращий прогноз наслідків рішень, більш таргетовані інтервенції	Зниження транзакційних витрат, сумісність даних, швидке масштабування кращих практик, прозорість	Підвищення здатності держави витримувати й перетворювати цифрові та гібридні шоки без втрати керованості й базових функцій

Отже, Smart Digital Policies та Institutional SaaS доцільно інтерпретувати як операційне ядро національної моделі стійкості: Smart Digital Policies забезпечує алгоритмічно й даноцентрично керовану адаптацію змісту публічних політик, Institutional SaaS – уніфіковану хмарну інфраструктуру та спільний простір даних, у межах яких ці політики реалізуються, масштабуються та моніторяться. У такій конфігурації National E-Resilience виконує роль стратегічного «даху», що задає цільовий стан і вимоги до всієї системи (безперервність, відновлюваність, інтероперабельність, безпека), визначаючи, якою має бути архітектура цифрової держави, аби вбудовані в неї Smart Digital Policies та інституційний SaaS не лише функціонували, а й забезпечували керовану стійкість у умовах багатовимірних криз.

Очевидно, що навіть за наявності концепцій Smart Digital Policies та інституційного SaaS цифрова трансформація публічних інституцій не відбувається автоматично. Аналіз практик цифровізації показав, що більшість ініціатив мають фрагментарний, проєктний і техноцентричний

характер: цифрові рішення впроваджуються без цілісного бачення інституційної еволюції, без урахування «цифрової спадщини» конкретного органу влади та без чіткої прив'язки до завдань стійкості й резильєнтності. У результаті цифрова трансформація часто залишається декларативною, а не керованою: інституції отримують окремі сервіси чи системи, але не послідовну траєкторію розвитку, здатну вивести їх на якісно інший рівень адаптивної інституційної спроможності.

Саме ця суперечність між стратегічними цілями (National E-Resilience, розвиток Smart Digital Policies, побудова інституційного SaaS) та реальною динамікою змін усередині окремих органів влади зумовлює потребу у спеціальному концепті, який би описував і структурував шлях цифрового розвитку інститутів як цілеспрямований, вимірюваний і орієнтований на стійкість процес. Тому в межах AICB доцільно запропонувати ідею Digital Institutional Trajectories – цифрових траєкторій розвитку інститутів, запровадження якої дозволяє перейти від розуміння цифровізації як набору розрізнених проєктів до розуміння її як керованої інституціональної еволюції, підпорядкованої завданню підвищення адаптивної спроможності та національної стійкості.

У дисертації концепцію Digital Institutional Trajectories (DIT) запропоновано як логічне продовження та операціоналізацію раніше розроблених підходів до Smart Digital Policies та Institutional SaaS. Якщо Smart Digital Policies фокусуються на змістовій та алгоритмічній трансформації публічної політики, а інституційний SaaS – на створенні спільної цифрової інфраструктури для реалізації таких політик, то DIT вводить у аналітичне поле ще один, процесно-еволюційний вимір. Цифрові траєкторії розвитку інститутів постають як інтегральний інструментарій цілеспрямованого трансформування публічних інституцій з урахуванням їхньої поточної цифрової зрілості, індивідуальних інституційних особливостей, «цифрової спадщини» (legacy) та загальнодержавних вимог щодо E-Resilience і National E-Resilience. У такий спосіб DIT заповнюють

методологічну нішу між макрорівневими стратегіями цифрової трансформації та мікрорівневими проєктами цифровізації окремих органів влади, задаючи для останніх логіку не просто впровадження окремих ІТ-рішень, а проходження послідовної інституційної еволюції.

Теоретико-методологічно Digital Institutional Trajectories визначаються як керовані, індивідуалізовані та вимірювані шляхи цифрової трансформації інституцій, що інтегрують в єдину рамку оцінку поточної цифрової зрілості, виявлення цифрових дискрецій (digital discretions), формування цільового стану та покрокове планування переходу до нього з акцентом на нарощування інституційної стійкості й адаптивної спроможності. На відміну від традиційних підходів, де «цифровізація» розглядається як відносно уніфікований процес впровадження типових рішень, концепт DIT виходить із принципу інституційної специфічності: кожна публічна інституція має унікальну конфігурацію формальних правил, організаційної культури, кадрового потенціалу та технологічної бази, що визначає її «стартову точку» в цифровому просторі. Відповідно, траєкторія цифрового розвитку не може бути відтворенням єдиного шаблону, а повинна фіксувати індивідуалізований шлях переходу між рівнями цифрової зрілості з урахуванням ресурсних і часових обмежень та об'єктивної path dependency такої інституції.

У межах DIT цифрова трансформація розуміється як градуйований, поетапний процес, що розгортається через низку якісно відмінних станів цифрової зрілості, кожен з яких характеризується певним рівнем алгоритмізації процесів, інтеграції даних, прозорості процедур та вбудованості в загальнонаціональну цифрову екосистему. Зміни при цьому не мисляться як разові «проєктні стрибки», а як послідовна еволюція, у якій кожен наступний крок є логічно й нормативно обґрунтованим продовженням попереднього. Це зумовлює необхідність виразної інтеграції DIT у рамку AICB: цифрові траєкторії розглядаються не як самодостатній технічний процес, а як складова ширшого механізму адаптивного нарощування

інституційної спроможності, де технологічні зміни підпорядковані публічно-управлінським цілям, а не навпаки. У такій логіці ключовою стає пріоритизація стійкості: розвиток цифрової інфраструктури інституції має на меті не лише підвищення ефективності, швидкості чи зручності надання послуг, а насамперед посилення її резильєнтності, здатності діяти в умовах шоків, криз та високої невизначеності.

Операціоналізація концепту DIT у дослідженні здійснюється через виокремлення структурних компонентів і процесного циклу цифрової траєкторії. Першим етапом є цифровий інституційний аудит (Digital Institutional Audit), що передбачає комплексну оцінку наявної інформаційної інфраструктури органу влади, рівня цифрових компетентностей персоналу, ступеня цифровізації адміністративних процесів, стану захисту даних та кібербезпеки, режимів використання та обміну даними, а також нормативно-правових обмежень цифрової трансформації. Такий аудит дозволяє сформувати цілісне уявлення про реальний інституційно-цифровий профіль органу та виявити розриви між його фактичним станом і проголошеними стратегічними орієнтирами.

Наступним кроком стає виявлення «цифрових дискрецій» (Digital Discretions Mapping) – зон суб'єктивного, неформалізованого прийняття рішень, процесів із низькою алгоритмічною прозорістю, «чорних скриньок» у ланцюжках управлінських рішень, областей підвищеного корупційного ризику, пов'язаних із відсутністю цифрового відслідковування, а також процедур, де посадові особи володіють надмірними дискреційними повноваженнями. У термінах інституційної теорії така робота дозволяє перевести латентні, неформальні практики у площину явних, підзвітних і контрольованих процесів, тим самим зменшуючи простір для довільного тлумачення норм і посилюючи режим правової визначеності. У цифровій вимірності це означає перехід від *analog discretion* до *digitally constrained discretion*, коли простір суб'єктивності свідомо звужується за рахунок алгоритмізації, стандартизації та трасування рішень.

На підставі отриманих результатів формується цільова модель цифрової зрілості (Digital Maturity Target Model), яка задає бажаний стан інституції в середньостроковій перспективі. Ця модель враховує функціональний профіль органу, його місце у системі AICB, вимоги щодо участі в інституційному SaaS, необхідний рівень цифрової стійкості, а також роль у реалізації Smart Digital Policies. Ідеться не лише про технічні параметри (кількість цифрових сервісів, рівень автоматизації тощо), а й про інституційні якості: прозорість процедур, передбачуваність управлінських рішень, здатність до роботи з даними в режимі реального часу, вбудованість інституції в національні механізми E-Resilience. Таким чином, цільова модель фіксує не абстрактний «ідеальний стан», а прагматично досяжну конфігурацію цифрової та інституційної зрілості, релевантну як внутрішнім потребам органу, так і зовнішнім стратегічним вимогам.

Важливою ланкою DIT є розробка багатовимірної дорожньої карти (Multidimensional Roadmap), яка деталізує траєкторію переходу від поточного стану до цільової моделі. Ця карта охоплює поетапне впровадження цифрових інструментів, модернізацію бізнес-процесів та адміністративних процедур, оновлення нормативно-правового забезпечення, інтеграцію з іншими інформаційними системами, розвиток цифрових компетентностей персоналу, а також заходи з управління змінами та ризиками. Важливо, що дорожня карта вибудовується як багаторівнева: вона синхронізує технічні, організаційні, правові та кадрові вектори розвитку, не допускаючи їх розходження в часі та змісті. У такий спосіб DIT дозволяють подолати характерну для публічного сектору розірваність між IT-проектами, організаційним дизайном та нормативно-правовим полем.

Фаза динамічної імплементації та адаптації (Dynamic Implementation) закріплює DIT як живий, а не статичний інструмент. Запровадження встановлення контрольних точок (milestones), системи вимірюваних індикаторів та KPI цифрової трансформації, інкрементальне, поетапне впровадження з можливістю коригування, а також організація ефективних

каналів зворотного зв'язку забезпечують здатність траєкторії реагувати на зміну зовнішнього контексту (політичного, безпекового, ресурсного) без втрати загальної логіки розвитку. У результаті цифрова трансформація перестає бути одноразовою «кампанією» і набуває рис безперервного, але структурованого процесу покрокового підвищення інституційної спроможності.

Науково-теоретична інноваційність концепту Digital Institutional Trajectories полягає, по-перше, в тому, що він долає методологічний розрив між загальними, часто декларативними стратегіями цифрової трансформації та конкретними цифровими проєктами в окремих інституціях, надаючи цим проєктам місце в чітко окресленій логіці інституційної еволюції. По-друге, DIT індивідуалізують процес цифровізації, виходячи з того, що інституції є різними не лише за масштабом чи сектором, а й за глибиною вкорінених практик, режимів легітимності та структур влади; отже, для них мають розроблятися диференційовані траєкторії розвитку, а не універсальні рецепти. По-третє, DIT вбудовують цифрову трансформацію в контекст інституційної стійкості, підпорядковуючи технологічні інновації завданню посилення адаптивної спроможності, а не лише оптимізації поточних процесів. По-четверте, вони формалізують неформалізоване, пропонуючи систематичну роботу з виявлення та трансформації «цифрових дискрецій» у структуровані, прозорі й підзвітні процедури, що безпосередньо впливає на зниження корупційних ризиків та підвищення передбачуваності управління. Нарешті, по-п'яте, DIT концептуально пов'язують мікро- та макрорівні трансформацій: зміни в окремих інституціях розглядаються як внесок у загальну конфігурацію National E-Resilience, тобто у здатність держави в цілому підтримувати й відновлювати цифрові функції під час криз.

У системі AICB Digital Institutional Trajectories займають проміжне, але ключове місце між Smart Digital Policies та інституційним SaaS. Якщо Smart Digital Policies визначають, що і як має змінюватися в змісті публічної політики за рахунок алгоритмізації, сценарного моделювання та

використання даних, а інституційний SaaS забезпечує, де і на якій спільній платформі ці політики реалізуються, то DIT відповідають на запитання, яким шляхом, у якій послідовності та з якими проміжними інституційними станами конкретні органи влади мають трансформуватися, щоб стати спроможними впроваджувати такі політики та повноцінно використовувати спільні цифрові платформи. Тим самим Digital Institutional Trajectories виконують функцію критично важливого перехідного елемента: вони переводять цифрову трансформацію з декларативного рівня у керований, вимірюваний і орієнтований на стійкість процес, який одночасно враховує «цифрову спадщину» інституцій і їхню цільову роль у розбудові National E-Resilience.

Важливо зробити узагальнені висновки щодо авторського дослідження тематики НМС. По-перше, цифрові технології в межах національної моделі стійкості (НМС) мають розглядатися не як самоціль і не як набір інструментів технічної модернізації, а як фундаментальний архітектурний принцип побудови стійкої держави та суспільства. Йдеться про перехід від інтуїтивного або проєктного використання цифрових рішень до такого рівня, коли цифровий вимір стає системоутворювальним чинником організації публічної влади, розподілу повноважень, управління ризиками та забезпечення прав людини. По-друге, саме цифрові управлінські стандарти та розроблена в дисертації рамка AICB формують інституційне «ядро» цифрової резильєнтності, оскільки задають стабільні правила гри, механізми адаптації й критерії якості для всіх елементів цифрової держави. Вони дозволяють уникнути як нормативного хаосу, так і техноцентричного редукціонізму, коли цифрова інфраструктура випереджає інституційні спроможності та правові гарантії.

По-третє, моделі Integrated Open Governance, Smart Digital Policies, Institutional SaaS і Digital Institutional Trajectories в сукупності формують послідовну логіку переходу від фрагментарної цифровізації до цілісної цифрової екосистеми стійкості. Integrated Open Governance забезпечує

відкритість, взаємодію та координацію між суб'єктами публічної влади та громадянами; Smart Digital Policies задають новий формат політики як алгоритмічно керованого, даноцентричного й адаптивного процесу; Institutional SaaS надає спільну соціотехнічну платформу, на якій ці політики можуть реалізовуватися, масштабуватися та моніторитися; а Digital Institutional Trajectories описують керовані шляхи еволюції окремих інституцій від стану «цифрової розрізненості» до вбудованості в національну екосистему стійкості. Сукупно ці чотири компоненти дозволяють розглядати НМС не як статичну нормативну конструкцію, а як живу цифрово-інституційну екосистему, здатну навчатися, адаптуватися й самовідновлюватися під впливом шоків.

Отже, узагальнення наведених положень дає змогу перейти від опису окремих цифрово-інституційних компонентів до цілісного подання Національної моделі стійкості як інтегрованої екосистеми. У подальшому НМС розглядається як багаторівнева цифрово-інституційна архітектура, що поєднує стандарти, інструменти, процеси та суб'єктів у єдину конфігурацію, здатну забезпечувати стійкість держави й суспільства в умовах перманентних криз. Саме така інтегральна модель НМС подається на рис.5.1.

Формування Національної моделі стійкості в умовах війни є не лише доцільним, а стратегічно необхідним процесом. Війна радикально загострила системні вразливості державного управління – фрагментарність цифрових рішень, слабку координацію між відомствами, перевантаження окремих інститутів, несталу правову базу реагування на кризи. У таких умовах НМС виступає інституціональною рамкою, яка дозволяє перейти від «ручного», ситуативного управління до інституціонально закріпленої, відтворюваної спроможності держави раціонально діяти в умовах системних викликів.

Запровадження НМС в умовах війни створює потужний символічний ефект – держава не просто реагує на кризу, а стратегічно трансформується, демонструючи союзникам і партнерам здатність до інституційної модернізації навіть у найскладніших обставинах.

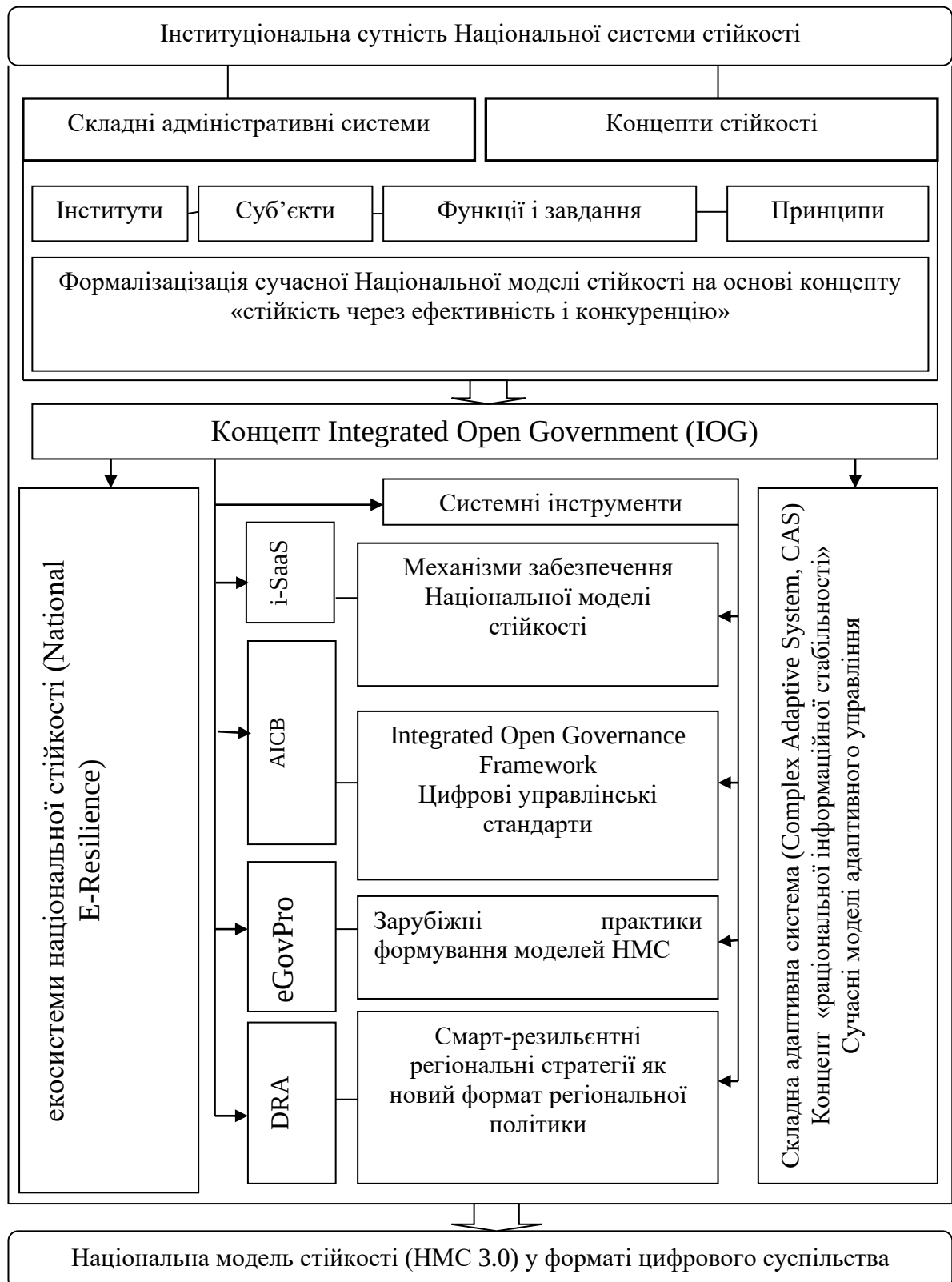


Рис. 5.1 Теоретичний концепт НМС у форматі цифрового суспільства.

Дана модель покладена в основу Концепції формування засад

національної моделі стійкості в умовах цифрового суспільства. Концепція формування засад національної моделі стійкості в системі органів державної влади, підготовлена на основі дисертаційних напрацювань, фактично є політико-управлінською «проекцією» авторської моделі НМС 3.0. Вона трактує НМС як довгострокову інституційно-цифрову рамку існування держави, що одночасно враховує потреби воєнного часу та цілі післявоєнного відновлення, поєднуючи правовий, організаційний, цифровий, кадровий, фінансовий та ідентичнісний виміри. Ключовим є бачення цифрової трансформації як архітектурного принципу: через національну цифрову інфраструктуру NEE, хмарну платформу Institutional SaaS та методологію DEV формується «цифрове ядро» НМС, повністю узгоджене з теоретичною моделлю НМС як живої цифрово-інституційної екосистеми. Концепція деталізує напрями модернізації (нормативна кодифікація стійкості, організаційна перебудова, інтегроване відкрите врядування, ризик-орієнтований підхід, смарт-резильєнтні регіональні стратегії, кадрова та ресурсна політика), перетворюючи модель НМС із наукової конструкції на практичний дорожній план для уряду та всієї публічної влади.

Позитивним є те, що Концепція уникає як технократичного редуccionізму, так і декларативності: цифрова інфраструктура NEE, Institutional SaaS і методологія DRA подаються як конкретні механізми посилення стійкості, а не абстрактні «цифрові реформи». Вона узгоджує нормативні, організаційні, регіональні та кадрові зміни з логікою Integrated Open Governance і Smart Digital Policies, створюючи цілісну, узгоджену з євроінтеграційним курсом рамку, здатну реально підвищити спроможність публічної влади діяти в умовах війни та післявоєнного відновлення.

Концепція прямо відповідає на ключові виклики воєнного стану та післявоєнного відновлення, пропонуючи не фрагментарні реформи, а цілісну рамку посилення стійкості всієї системи публічної влади. Позитивним є те, що Концепція поєднує стратегічне бачення з конкретними інструментами – від цифрової інфраструктури та Institutional SaaS до смарт-резильєнтних

регіональних стратегій, що визначає її практичну реалізацію. Концепція узгоджена з євроінтеграційними вимогами, базується на вже наявних цифрових платформах України й водночас задає чіткі орієнтири для міжнародних донорів, уряду та органів влади різних рівнів. Концепція усуває розрив між концептуальними дискусіями про стійкість і реальними управлінськими практиками, й може стати прикладною «дорожньою картою» для формування Національної моделі стійкості нового покоління.

Таким чином, у дисертації доведено, що потенціал цифрових технологій для підвищення стійкості держави й суспільства реалізується лише за умови їх системного вбудовування в авторську екосистему National E-Resilience – через інституціоналізовану цифрову політику, стандартизовані управлінські підходи, адаптивну інституційну спроможність і розумні цифрові політики, підкріплені відповідною інфраструктурою. Саме така інтеграція перетворює НМС з набору декларацій і розрізнених ініціатив на динамічну, навчальну й самовідновну систему, яка здатна не лише витримувати тривалі й багатовимірні кризи, а й використовувати їх як імпульс для інституційного й технологічного розвитку. З позицій результатів дослідження це є ключовою передумовою не лише виживання, а й якісного, суб'єктного розвитку України в умовах тривалої війни, глобальної конкуренції та радикальної невизначеності цифрової епохи, коли саме поєднання стійкості, відкритості й цифрової інноваційності визначатиме місце держави у новій архітектурі міжнародних відносин і глобальної безпеки.

Висновки до розділу 5

1. У дисертації сформульовано цілісну концепцію Національної моделі стійкості (НМС 3.0) як цифрово-інституціональної екосистеми. У роботі НМС визначено не як сукупність окремих політик чи секторних програм (кібербезпека, цифрове урядування, економічна стійкість), а як інтегровану національну модель управління, що поєднує ресурси, інститути, дані й процеси в єдину адаптивну систему. Обґрунтовано ключові

властивості цієї моделі – інтегративність, проактивність, соціотехнічний баланс і динамічність – та показано, що цифровий вимір виступає системоутворювальним чинником організації публічної влади, розподілу повноважень і управління ризиками. На цій основі НМС 3.0 інтерпретовано як «архітектуру поведінки» держави в умовах війни, гібридних загроз і радикальної цифрової невизначеності.

2. Розроблено авторську модель НМС як багаторівневої інтероперабельної цифрової екосистеми з інтегрованою платформою державного управління. Доведено, що цифрова резильєнтність держави може бути досягнута через поєднання централізованої цифрової платформи (як «нервової системи» та центру ситуаційної обізнаності) з високим рівнем інтероперабельності між розподіленими суб'єктами, системами й процесами. Запропоновано чотири рівні інтероперабельності (стандарти – сервіси – спільні процедури реагування – довіра та сертифікація) та матрицю їх зрілості, що дозволяє операціоналізувати НМС у вимірювані показники цифрової стійкості. Показано, що така архітектура забезпечує здатність держави працювати в режимі «обмеженої функціональності» без втрати базових керуючих можливостей і мінімізує ризики «єдиної точки відмови».

3. Концептуалізовано та обґрунтовано адаптивну інституційну розбудову (Adaptive Institutional Capacity Building – AICB) як процесний «двигун» НМС. На противагу класичній «розбудові спроможності», зосередженій на накопиченні ресурсів, AICB визначено як динамічний механізм безперервних інституційних змін, що спирається на теорію комплексних адаптивних систем, інституційних змін, організаційної стійкості та проблемно-орієнтованої політики. Сформульовано аксіоми AICB (адаптивність, рекурсивне навчання, контекстуальність, розподілене прийняття рішень, модульність і зв'язність, керована надлишковість, відкриті рамки), які задають нову парадигму публічного управління в умовах перманентних криз. Показано, що AICB інтегрує правові, організаційні,

технологічні та кадрові трансформації, перетворюючи НМС на живу, навчальну систему, а не статичну нормативну конструкцію.

4. Розроблено новий формат публічної політики – Smart Digital Policies – та інфраструктурну модель Institutional Software as a Service (SaaS) як операційне ядро НМС. У дисертації Smart Digital Policies визначено як цифрово закріплені, даноцентричні та алгоритмічно керовані публічні політики, що реалізуються через програмні алгоритми, сценарні моделі, параметри ризиків і показники ефективності, здатні адаптуватися до змін середовища без постійних змін законодавства. Інституційний SaaS описано як єдину багатосуб'єктну хмарну платформу для органів влади, яка надає стандартизований набір модулів планування, моніторингу, управління ризиками та підтримки рішень. Доведено, що взаємодія Smart Digital Policies та Institutional SaaS формує цілісний соціотехнічний комплекс, у якому політика розглядається як сервіс (policy-as-a-service), а НМС – як здатність держави підтримувати та відновлювати цей комплекс у кризових умовах.

5. Запропоновано концепт Digital Institutional Trajectories (цифрових інституційних траєкторій) як інструмент подолання розриву між стратегіями цифровізації й реальною еволюцією інституцій. Розроблено процесну модель цифрової траєкторії, що включає: цифровий інституційний аудит; виявлення «цифрових дискрецій» (зон неформалізованих рішень, «чорних скриньок», підвищених корупційних ризиків); побудову цільової моделі цифрової зрілості; дорожню карту змін і фазу динамічної імплементації з контрольними точками та індикаторами. Наукова новизна полягає в тому, що цифрова трансформація інтерпретується як градуїований, поетапний процес еволюції інституцій, підпорядкований завданню стійкості, а не як набір фрагментарних ІТ-проектів. Показано, що такі траєкторії індивідуалізують цифровізацію під конкретні органи влади й водночас вбудовують їх у загальну конфігурацію НМС.

6. Сформовано системну рамку цифрових управлінських стандартів НМС як умову подолання фрагментації державних цифрових систем і

узгодження з європейським правовим простором. Обґрунтовано класифікацію цифрових стандартів у три кластери – «база безпеки та правової визначеності», «інфраструктура взаємодії», «соціотехнічна система та людський вимір» – і виділено ключові їхні групи (кібербезпека, управління даними, міжвідомча взаємодія, якість послуг, моніторинг та оцінювання, навчання персоналу, адаптивність управлінських структур тощо). Показано, що стандарти виконують роль «мосту» між нормами права та технічною реалізацією (concept of code as law), а також є інструментом інтеграції України до ЄС і Єдиного цифрового ринку. Доведено, що стандартизація скорочує витрати інтеграції систем, знижує ризики «цифрових дискретностей» та підтримує адаптивну розбудову інституційної спроможності.

7. Емпірично підтверджено зв'язок між рівнем цифрової інтеграції, інтероперабельності та інституційною стійкістю в умовах війни, що верифікує запропоновану модель НМС. На основі матриць зрілості інтероперабельності, оцінок профілів різних груп суб'єктів (органи безпеки й оборони, економічні та соціальні ЦОВВ, ОМС) і результатів опитування керівників ЦОВВ та ОДА (2022–2024 рр.) показано, що підрозділи з високим рівнем цифрової інтеграції та інтероперабельності демонструють на 72 % вищу швидкість реакції та на 41 % кращі показники якості рішень у кризових ситуаціях. Проаналізовані кейси ілюструють, що інтегровані цифрові платформи, відкриті дані, краудсорсингові сервіси й смарт-резильєнтні регіональні стратегії реально підвищують здатність держави підтримувати базові функції та адаптувати політики в реальному часі. Це дозволяє розглядати екосистему НМС як практично верифіковану модель цифрової резильєнтності держави й суспільства в умовах тривалої війни.

Основні результати дослідження, що наведені у цьому розділі, були опубліковані у фахових наукових виданнях галузі знань «Публічне управління і адміністрування» та включені до списку публікацій автора [1-4; 5-9; 12-15].

ВИСНОВКИ

У дисертації вирішено актуальну наукову проблему, яка полягала у розробці теоретико-методологічних засад формування НМС у форматі цифрового суспільства. Наукові результати дослідження надали змогу сформулювати ряд висновків і рекомендацій, які мають як теоретичне, так і практичне значення для формування державноуправлінської парадигми розвитку Української держави.

1. Розкрито сутність НМС у контексті сучасних інституціональних підходів, особливостей розвитку державного управління в умовах правового режиму воєнного стану та викликів цифрового суспільства. Визначено, що національна модель стійкості (НМС) – це інтегрована, інституціоналізована система організації та здійснення державного управління, яка забезпечує здатність держави й суспільства своєчасно виявляти, оцінювати та прогнозувати воєнні, безпекові, соціально-економічні, інформаційні й технологічні загрози, адаптувати інститути влади, політики, процедури та ресурси до умов криз і невизначеності, підтримувати безперервність і легітимність функціонування публічної влади, захищати критичну інфраструктуру, зберігати суспільну згуртованість і національну ідентичність, а також використовувати потенціал цифрового суспільства (дані, цифрові платформи, інформаційно-комунікаційні технології, штучний інтелект) для підвищення ефективності, прозорості й підзвітності управління, орієнтованого на довгостроковий стійкий розвиток держави в умовах війни, гібридних загроз та глибокої цифрової трансформації. Встановлено, що НМС є ключовим складником сучасної парадигми державного управління та національної безпеки, який визначає інституціональну здатність держави адаптуватися до зовнішніх та внутрішніх викликів, зберігати свою цілісність і функціональність. У контексті сучасних наукових підходів запровадження НМС вимагає інтеграції ресурсів і зусиль державних структур, суспільства і громадян, що базується на основі реалізації принципів крос-

інституціональної співпраці. У сучасному цифровому суспільстві, де інформаційні технології стають основними інструментами управління, важливо також забезпечити кібербезпеку та захист інформаційних систем. З цією метою у роботі обґрунтовано теоретико-методологічні засади формування НМС у форматі цифрового суспільства, що передбачає дослідження специфіки цифрової трансформації державного управління, розробку авторської концепції національної стратегії державотворення на основі адаптації інституціональних механізмів до умов цифровізації, а також створення ефективних інструментів публічного адміністрування для забезпечення стійкості держави в умовах сучасних викликів – протидії збройній агресії РФ, незавершеності інституціональних реформ, формуванню нової цифрової парадигми управління.

Вимоги правового режиму воєнного стану вимагають від державного управління підвищеної адаптивності, інтеграції цифрових технологій та ефективного реагування на гібридні загрози, включаючи кіберризики та інформаційні атаки. Інституційна спроможність держави, соціальна згуртованість і технологічна адаптивність є ключовими складниками національної моделі стійкості, що забезпечують її ефективність у кризових ситуаціях. Формування національної стійкості в умовах цифровізації потребує системного підходу, який інтегрує правові, соціальні, економічні та технологічні аспекти для забезпечення стабільного розвитку держави.

2. Визначено структурні проблеми та перспективи становлення та розвитку основ законодавства у сфері формування НМС, діяльності державних інститутів у форматі цифрового суспільства та їх адаптивності до інституціональних змін. НМС визначена не лише як сукупність заходів безпеки, а як екосистема управління (National E-Resilience), що поєднує правові норми, інститути, цифрові технології, управлінські стандарти, механізми моніторингу та смарт-резильєнтні регіональні стратегії й спрямована на довгостроковий розвиток держави в умовах війни та глибокої цифрової трансформації. На основі проведеного дослідження визначено, що

структурні проблеми та перспективи становлення й розвитку основ законодавства у сфері формування національної моделі стійкості характеризуються комплексним характером викликів та можливостей. Ключовою проблемою виступає недостатня розвиненість нормативно-правового забезпечення формування НМС та процесів цифровізації державного управління, що ускладнює впровадження інновацій та знижує адаптивність державних інституцій до змін.

Визначено перспективні напрями розвитку, серед яких пріоритетними є адаптація законодавства України до міжнародних стандартів у сфері цифровізації та формування комплексної нормативної бази становлення НМС в умовах цифрового суспільства. Особливу увагу приділено розробці правового поля для регулювання відносин у сфері цифровізації, що дозволить уникнути правових колізій і забезпечити захист прав громадян. Важливим аспектом є створення стандартів правового регулювання, які визначають правові основи для впровадження цифрових технологій у державному управлінні, включаючи імплементацію міжнародних норм. Щодо адаптивності державних інститутів до змін, дослідження показало необхідність впровадження гнучких механізмів правового регулювання та розвитку інституційної спроможності через відповідне нормативне забезпечення. Це дозволить створити правові механізми для швидкого реагування на зміни та забезпечити ефективне функціонування державних інституцій у форматі цифрового суспільства.

3. Проаналізовано вплив цифровізації на розвиток державних та суспільних ініціатив в Україні щодо формування НМС, досліджено їх роль у зміцненні соціальної стабільності й безпеки функціонування управлінських систем, формалізовано феномен цифрових управлінських платформ. На основі проведеного дослідження встановлено, що цифровізація здійснює комплексний вплив на розвиток державних та суспільних ініціатив в Україні через впровадження інноваційних технологій, що трансформують традиційні механізми управління та створюють нові можливості для взаємодії держави і

суспільства. Зокрема, цифрові технології сприяють підвищенню адаптивності державних структур через впровадження гнучких управлінських механізмів, автоматизацію процесів та розвиток електронних послуг, що підвищує ефективність державного управління та його здатність реагувати на сучасні виклики.

Доведено, що цифровізація відіграє ключову роль у зміцненні соціальної стабільності та стійкості шляхом забезпечення прозорості управлінських процесів, розширення можливостей громадської участі та підвищення доступності державних послуг. Впровадження цифрових платформ створює нові канали комунікації між державою та громадянами, сприяє розвитку цифрових компетенцій населення та забезпечує соціальну інклюзію через рівний доступ до цифрових послуг. *Цифрова управлінська платформа* як складник НМС визначається як інтегрована система, яка забезпечує автоматизацію управлінських процесів, координацію між різними інституціями, моніторинг, аналітику ризиків та підтримку прийняття рішень на основі аналізу великих даних і прогнозних моделей. Такі платформи спрямовані на підвищення прозорості, ефективності та адаптивності державного управління, дозволяючи інтегрувати інформаційні ресурси, забезпечувати швидкість реагування на виклики та створювати нові типи взаємодії між державою, громадянами та бізнесом.

Формалізація феномену цифрових управлінських платформ в дизайні НМС дозволила визначити такі платформи як інтегровані системи, що забезпечують автоматизацію управлінських процесів, координацію між різними інституціями та аналітичну підтримку прийняття рішень, й виступають основою для розвитку «розумного урядування», що базується на використанні великих даних, штучного інтелекту та інших інноваційних технологій для підвищення ефективності державного управління та забезпечення національної моделі стійкості в умовах цифрової трансформації суспільства.

4. На основі проведеного дослідження розроблено теоретичну

концепцію National E-Resilience як інтегровану модель управління, спрямовану на забезпечення НМС в Україні в умовах цифровізації, особливо під час воєнного стану. Концепція базується на систематичному підході до оцінки, аналізу та посилення спроможності держави реагувати на зовнішні та внутрішні виклики. Її ключовими компонентами є централізована цифрова платформа управління, адаптивні механізми функціонування державних інституцій, інтеграція цифрових технологій у всі рівні управління та розвиток інституційної гнучкості (у форматі НМС). Основою концепції є впровадження алгоритму оцінки цифрової стійкості (Digital Resilience Assessment, DRA), який дозволяє оцінювати здатність державних структур адаптуватися до викликів цифрової трансформації. Цей алгоритм включає діагностику загроз, збір і аналіз великих даних, визначення критичних індикаторів стійкості (зокрема, рівня соціальної довіри, кібербезпеки, доступу до критичної інфраструктури), а також розробку рекомендацій для коригування стратегій реагування.

Концепція «National E-Resilience» передбачає створення інтегрованої цифрової платформи моніторингу, яка забезпечує оперативний обмін даними між органами управління, силовими структурами, громадськими організаціями та міжнародними партнерами. Ця платформа дозволяє отримувати звіти в реальному часі про готовність до кризових ситуацій, ступінь адаптації до змінних умов та ефективність заходів із відновлення функціонування державних систем. Особливу увагу приділено адаптації міжнародного досвіду до українських реалій. У межах концепції запропоновано компаративно-адаптаційну парадигму, яка дозволяє враховувати як інституційні, так і культурні особливості країни. Концепція також акцентує увагу на розвитку цифрової резильєнтності як здатності державних інституцій адаптуватися до цифрових змін і протистояти кіберзагрозам. Важливим аспектом є створення інноваційних хабів, які слугуватимуть платформами для обміну ідеями та впровадження нових технологій у державне управління.

5. Досліджено напрями інтеграції передових інформаційних технологій у систему державного управління в контексті формування національної моделі стійкості. На основі проведеного дослідження визначено, що інтеграція передових інформаційних технологій у систему державного управління є ключовим напрямом формування національної моделі стійкості (НМС), яка забезпечує адаптивність, ефективність та прозорість управлінських процесів в умовах сучасних викликів. Основними аспектами цієї інтеграції є впровадження цифрових платформ, автоматизація управлінських функцій, використання великих даних, штучного інтелекту та блокчейн-технологій, що дозволяє створити єдину систему моніторингу, аналізу та реагування на загрози. Особливу увагу приділено створенню Національного реєстру загроз, який систематизує ризики та сприяє підвищенню національної стійкості через прогнозування та попередження кризових явищ. Доведено, що впровадження штучного інтелекту та аналітики великих даних у державне управління сприяє підвищенню ефективності прийняття рішень, зокрема через автоматизацію процесів збору, обробки та аналізу інформації. Це дозволяє не лише оптимізувати використання ресурсів, але й забезпечити прозорість управлінських процесів, що підвищує довіру громадян до державних інституцій. Важливим аспектом є також розвиток електронного урядування, яке через мобільні платформи та інтуїтивно зрозумілі інтерфейси спрощує доступ громадян до державних послуг, підвищує якість та доступність таких послуг.

Запропоновано впровадження «смарт-резильєнтних регіональних стратегій» (СРРС) як інструментів НМС, які враховують унікальні соціально-економічні, географічні та культурні особливості регіонів. Ці стратегії базуються на використанні геоінформаційних систем (GIS), інтелектуальних систем управління інфраструктурою та віртуальних моделей для прогнозування кризових ситуацій. СРРС спрямовані на зміцнення регіональної здатності адаптуватися до нових умов, реагувати на кризи та забезпечувати стабільний розвиток. Окремо наголошено на важливості

формування нормативно-правової бази для регулювання цифрових трансформацій у державному управлінні. Це включає розробку стандартів цифрового врядування, які визначають правила збору, обробки та використання даних, а також забезпечують баланс між прозорістю та захистом приватного права.

6. Визначено державноуправлінські механізми формування суспільної довіри до органів влади та активізації громадянського суспільства в умовах цифрового суспільства у форматі функціонування НМС. На основі проведеного дослідження визначено, що формування суспільної довіри до органів влади та активізація громадянського суспільства в умовах цифрового суспільства є ключовими завданнями для забезпечення стійкості державного управління. У сучасних умовах функціонування національної моделі стійкості довіра до органів влади формується через прозорість, підзвітність, ефективність управлінських процесів та залучення громадян до прийняття рішень. Для досягнення цих цілей запропоновано низку державноуправлінських інструментів, які базуються на інтеграції цифрових технологій у систему публічного управління. Окрім цифрових управлінських платформ, інструментами виступають: по-перше, розвиток цифрової інклюзії, яка забезпечує рівний доступ громадян до цифрових послуг незалежно від їхнього соціального статусу, віку чи місця проживання, і включає створення інтуїтивно зрозумілих інтерфейсів для електронних послуг, підвищення цифрової грамотності населення та впровадження програм навчання для вразливих груп. Рівний доступ до цифрових ресурсів сприяє соціальній згуртованості та підвищує довіру до держави

По-друге, впровадження цифрових стандартів прозорості та підзвітності, які регулюють процеси збору, обробки та використання даних у державному управлінні; це включає стандарти відкритого управління, які забезпечують доступ громадян до інформації про діяльність органів влади, а також стандарти моніторингу та оцінки ефективності впроваджених цифрових технологій; прозорість управлінських процесів підвищує

легітимність рішень та зміцнює довіру громадян. По-третє, інтеграція громадян у процеси прийняття рішень шляхом використання цифрових технологій, що включає створення механізмів зворотного зв'язку, таких як електронні петиції, опитування та платформи для збору пропозицій від громадян. По-четверте, забезпечення кібербезпеки та захисту даних, що є критично важливим для збереження довіри громадян до цифрових платформ. Адже відсутність чітких механізмів захисту даних може призвести до втрати довіри до державних інституцій, тому впровадження національних стандартів кібербезпеки та інвестиції в захист цифрової інфраструктури є пріоритетними завданнями.

7. Досліджено роль крос-інституціонального співробітництва (на рівні крос-інституціональних платформ) в реалізації національної моделі стійкості як процесу взаємодії між державними структурами, бізнесом та неурядовими організаціями у запобіганні кризовим явищам та системним викликам. На основі проведеного дослідження встановлено, що крос-інституціональне співробітництво є ключовим елементом реалізації національної моделі стійкості (НМС) в умовах цифрового суспільства. Воно забезпечує ефективну взаємодію між державними структурами, бізнесом та неурядовими організаціями, спрямовану на запобігання кризовим явищам, адаптацію до викликів та зміцнення соціальної згуртованості. У дослідженні наголошено, що крос-інституціональні платформи виступають інструментом інтеграції ресурсів, знань та технологій, що дозволяє створювати гнучкі механізми реагування на загрози та забезпечувати стабільність державного управління.

Основними напрямками крос-інституціонального співробітництва визначено: 1) інтеграція цифрових платформ для координації дій між державними органами, бізнесом та громадськими організаціями, й такі платформи забезпечують оперативний обмін інформацією, моніторинг ризиків та спільну розробку стратегій реагування на кризові ситуації. Зокрема, у роботі запропоновано створення національної цифрової платформи моніторингу, яка дозволяє в реальному часі отримувати дані про

стан критичної інфраструктури, соціальної довіри та ефективність заходів із запобігання кризам; 2) розвиток публічно-приватного партнерства, яке сприяє залученню інвестицій, інноваційних рішень та технологій для підвищення ефективності управлінських процесів; 3) вертикальна та горизонтальна координація: вертикальна координація передбачає узгодженість дій між центральними, регіональними та місцевими органами влади; горизонтальна координація сприяє взаємодії між регіонами, бізнесом та громадськими організаціями для спільного вирішення кризових ситуацій, таких як природні катастрофи, кіберзагрози чи соціальні конфлікти; 4) становлення крос-інституціонального співробітництва через створення правових та організаційних механізмів, які регулюють взаємодію між учасниками. Це включає розробку нормативно-правової бази, яка визначає права, обов'язки та відповідальність кожної сторони, а також створення спеціалізованих органів чи платформ для координації дій; 5) впровадження міжнародних стандартів кібербезпеки та створення центрів цифрової резильєнтності, які забезпечуватимуть захист даних та безперервність функціонування критичних систем.

8. На основі проведеного дослідження розроблено та обґрунтовано *комплексну стратегію моніторингу та оцінювання ефективності реалізації національної моделі стійкості (НМС)*, яка базується на використанні сучасних механізмів публічного контролю та інноваційних цифрових технологій. Стратегія спрямована на забезпечення прозорості, підзвітності та адаптивності управлінських процесів в умовах сучасних викликів. Основою стратегії є створення інтегрованої цифрової платформи моніторингу, яка об'єднує інструменти збору, аналізу та оцінки даних щодо реалізації НМС. Платформа покликана забезпечити поточний нагляд за ключовими показниками ефективності, включаючи стан критичної інфраструктури, рівень соціальної довіри, ефективність управлінських рішень та рівень мобілізації ресурсів. Така платформа дозволяє здійснювати автоматизований збір даних, використовувати прогнозу аналітику та оперативно реагувати на

виявлені проблеми.

Ключовими елементами стратегії є: 1) визначення комплексних індикаторів ефективності для оцінювання реалізації НМС: соціальні індикатори (рівень довіри громадян до органів влади, соціальна згуртованість); економічні індикатори (стабільність економічних процесів, мобілізація ресурсів у кризових умовах); інституційні індикатори (ефективність державних структур, адаптивність до викликів); кіберстійкість (готовність до кіберзагроз і рівень захисту цифрової інфраструктури).

2) впровадження механізмів публічного контролю, які передбачають активну участь громадянського суспільства у моніторингу та оцінюванні ефективності. Інструментами такого контролю є: онлайн-інструменти контролю, такі як електронні петиції, анкетування та платформи для збору зворотного зв'язку; звітування органів влади у відкритому доступі через публічні онлайн-сервіси; проведення громадських слухань та консультацій із зацікавленими сторонами.

3) створення експертних центрів моніторингу та оцінювання. Запропоновано формування спеціалізованих аналітичних центрів, до складу яких увійдуть представники державних органів, громадських організацій, наукових установ та бізнесу. Такі центри здійснюватимуть зовнішню незалежну оцінку реалізації НМС, забезпечуючи об'єктивність результатів та пропонуючи рекомендації для вдосконалення політики.

НМС виступає як інноваційна парадигма державного управління в умовах правового режиму воєнного стану, що поєднує безпеку суспільства і громадян, розвиток держави і цифрову трансформацію в єдину екосистему управлінських рішень. НМС переводить державне управління з режиму ситуативного реагування в режим проактивної діяльності, забезпечує суб'єктність, інституційну спроможність і технологічну державної влади в умовах збройної агресії і гібридних загроз, й одночасно гарантує демократичну легітимність й людиноцентричність влади.

НМС інтегрує цифрові платформи, крос-інституціональну взаємодію,

регіональну смарт-резильєнтність, безпекові формати та європейські стандарти врядування в цілісну архітектуру National E-Resilience, яка перетворює стійкість на вимір якості функціонування сучасної держави. У цьому сенсі національна модель стійкості України постає не лише відповіддю на виклики правового режиму воєнного стану, а стратегічною матрицею модернізованої державності XXI століття – держави, що вчиться на кризах, трансформує загрози на ресурс розвитку й забезпечує громадянам безпечне, гідне та повноцінно інтегроване в цифровий простір майбутнє.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Драгомирецька Н. Концепція сталого розвитку: теоретико-історичний аспект. *Державне управління та місцеве самоврядування*. 2019. № 1. С. 6-12.
2. Серьогіна Т. Удосконалення системи надання публічних послуг в умовах децентралізації: методологічні засади : монографія. Дніпро: ГРАНІ, 2020. 288 с.
3. Легеза Є. Характеристика деяких видів публічних послуг у сфері соціального захисту населення. *Прикарпатський юридичний вісник*. 2016. Вип. 1. С. 147-151.
4. Ажажа М., Дашков А., Цикін Д. Теоретико-концептуальні засади формування клієнтоорієнтованої моделі публічного сервісу: від «послуга як процедура» до «послуга як досвід». *Публічне управління і адміністрування в Україні*. 2024. №4 2. С.188-194.
5. Мороз С., Помаза-Пономаренко А., Ажажа М. Забезпечення прав і доступу до публічних послуг внутрішньо переміщених осіб: аспекти публічного управління. *Публічне управління і адміністрування в Україні*. 2025. № 45. С. 254-257.
6. Бородін, Є., Піскоха Н., Демошенко Г. Проблеми і переваги цифровізації місцевого самоврядування. *Аспекти публічного управління*. 2021. № 9(4). С. 95-103.
7. Квітка С., Новіченко Н., Гусаревич Н., Піскоха Н., Бардах О., Демошенко Г. Перспективні напрямки цифрової трансформації. публічного управління. *Аспекти публічного управління*. 2020. № 8 (4). С.129-146.
8. Баштанник А.Г. Організаційні засади формування інтегрованих систем публічного управління в контексті європейського інтеграційного процесу. *Наук. вісн. Акад. муніцип. упр. : зб. наук. пр., Серія «Управління»*. 2012. Вип. 4. С. 15–26.

9. Chughtai H., Myers M. D. Human values in a digital-first world: the implications for qualitative research. *Cambridge handbook of qualitative digital research*. 2023. P. 91–103. URL: <https://doi.org/10.1017/9781009106436.010>.
10. Ахмедова О. Цифрова трансформація інституту публічних послуг в умовах модернізації територіального управління в Україні. *Публічне управління і адміністрування в Україні*. 2025. №46. С.136-139/
11. Арістова І. Еволюційний розвиток поняття «інформаційна сфера». *Вісник Національного університету внутрішніх справ*. 2005. Вип. 31. С. 239–245
12. Арістова І. Органи державного управління інформаційною сферою: концепція розвитку. *Вісник Харківського національного університету внутрішніх справ*. 2004. Вип. 25. С. 287-292.
13. Hood, C. (1991). A public management for all seasons? *Public Administration*, 69(1), 3-19. URL: <https://eclass.uoa.gr/modules/document/file.php/PSPA108/4NMP%20all%20seasonsfulltext.pdf>.
14. Hood, C., Lodge, M. (2006). The politics of public service bargains: Reward, competency, loyalty – and blame. *Journal of Public Administration Research and Theory*, 16(2), 217-234. URL: https://www.researchgate.net/publication/30529626_The_Politics_of_Public_Service_Bargains_Reward_Competency_Loyalty_-_and_Blame.
15. Hood, C. (2005). Public management: The word, the movement, the science. *International Public Management Journal*, 8(2), 109-126. URL: https://www.researchgate.net/publication/288078011_Public_Management_The_Word_the_Movement_the_Science.
16. Mulgan, G. (2009). *The art of public strategy: Mobilizing power and knowledge for the common good*. Oxford University Press. URL: <https://archive.org/details/artofpublicstrat0000mulg/page/n5/mode/2up>.
17. Mulgan, G. (2023). What are governments for? Geoff Mulgan Substack. URL: <https://geoffmulgan.substack.com/p/what-are-governments-for>.

18. Mulgan, G. (2025). Building the next generation of public institutions. Project Syndicate. URL: <https://www.project-syndicate.org/commentary/next-generation-public-institutions-innovative-designs-by-geoff-mulgan-2025-02>.

19. Rosenbloom, D. H. (2000). Public administration: Understanding and managing in government. In *Public administration: Concepts and cases* (pp. 1-20). Houghton Mifflin. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9781003198116/public-administration-david-rosenbloom-robert-kravchuk-richard-clerkin/>

20. Rosenbloom, D. H. (2016). The American system of public administration: The consequences of the federal structure. *Public Administration Review*, 76(1), 9-17. URL: <https://www.american.edu/uploads/docs/2025cvapril27.pdf>.

21. Eymery-Duzen, J. (2019). Innovations in public service delivery: The role of information technology. *International Journal of Public Sector Management*, 32(3), 311-326.

22. Дзевелюк М.В. Сервісна держава як функціональна модель сучасної держави. *Актуальні проблеми держави і права*. 2017. Вип. 78. С. 64.

23. Лопушинський І. П. «Цифровізація» як основа державного управління на шляху трансформації та реформування українського суспільства. *Теорія та практика державного управління і місцевого самоврядування*. 2018. № 2. С. 33–45.

24. Кравцов О. Концептуалізація моделі державотворчих процесів в Україні на основі проблемного підходу: феномен цифрової резильєнтності державних структур. *Держава і регіони*. 2023. № 1. URL: http://pa.stateandregions.zp.ua/archive/1_2023/1_2023.pdf.

25. Кравцов О.В., Губа М.І., Андросович А.В. Роль цифрових технологій у покращенні доступності та якості публічних послуг в Україні. *Державне управління: удосконалення та розвиток*. 2024. № 9. (електронне видання) URL: <https://www.nayka.com.ua/index.php/dy/article/view/4612>.

26. Баштанник В, Гавриленко К., Інтегровані системи публічного управління 3.0: трансформації концептуальної моделі національної стратегії розвитку. *Публічне управління і місцеве самоврядування*. 2023. №3. С.57-64.

27. Weber, M. (1947). *The Theory of Social and Economic Organization*. Translated by A. M. Henderson and T. Parsons. New York: Oxford University Press. – URL: https://ia804503.us.archive.org/32/items/weber-max.-the-theory-of-social-and-economic-organization-1947_202106/Weber%2C%20Max.%20-%20The%20Theory%20of%20Social%20and%20Economic%20Organization%20%5B1947%5D.pdf. (дата звернення: 12.04.2025)

28. Weber, M. (1968). *Economy and Society: An Outline of Interpretive Sociology*. Edited by G. Roth and C. Wittich. Berkeley: University of California Press. – URL: <https://ia600202.us.archive.org/8/items/MaxWeberEconomyAndSociety/MaxWeberEconomyAndSociety.pdf>. (дата звернення: 12.04.2025).

29. Peters, B. Guy. *The Future of Governing: Four Emerging Models*. 2nd ed. Lawrence, KS: University Press of Kansas, 2001. URL: <https://link.springer.com/book/10.1057/9780230512641>.

30. Лахижа М.І. Диджиталізація в Україні: поняття, проблеми, перспективи та завдання публічного управління. *Науковий вісник: Державне управління* №2(4) 2020 С.202-213

31. Квітка С. Цифрові трансформації як сучасний тренд періодичного циклу розвитку суспільства. 3б. наук.праць НАДУ. Спецвипуск. 2020. 131-134. <http://doi.org/10.36.030/2664-3618-2020-si-131-134>

32. Osborne, D. Reinventing Government. *Leadership Abstracts*. 1993. Vol. 6. No. 1. January. ERIC Document No. ED367424.

33. Georg Jellinek, *General Theory of the State* (англ. переклад нім. Allgemeine Staatslehre). URL: <https://sk.sagepub.com/encyclopedia/law/chapter/jellinek-georg-1851-1911.pdf/>

34. Hughes, O. E. *Public Management and Administration: An Introduction*. 4th ed. Basingstoke: Palgrave Macmillan, 2012. 373 p. URL:

<https://nibmehub.com/opac-service/pdf/read/Public%20Management%20and%20Administration%20An%20Introduction%20by%20Owen%20E.%20Hughes.pdf>.

35. Keating, P. *Engagement: Australia Faces the Asia–Pacific*. Sydney: Macmillan, 2000.

36. Walsh, P. *Confessions of a Failed Finance Minister*. Milsons Point, NSW: Random House Australia, 1995.

37. Pollitt, C., Bouckaert, G. *Public Management Reform: A Comparative Analysis – New Public Management, Governance, and the Neo-Weberian State*. – 3rd ed. Oxford: Oxford University Press, 2011. 368 p.

38. Scourfield, P. Social care and the modern citizen: Client, consumer, service user, manager and entrepreneur? *British Journal of Social Work*. 2007. Vol. 37, No. 1. P. 107–12.

39. Державне управління : підручник : у 2 т. / ред. кол. : Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови) та ін. Київ: НАДУ, 2012. Т. 1. 564 с.

40. Kooiman, J. (2003). *Governing as Governance*. London: SAGE Publications. URL:https://sk.sagepub.com/book/mono/governing-as-governance/toc#_.

41. Rhodes, R. A. W. (1997). *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*. Open University Press. – URL: <https://archive.org/details/understandinggov0000rhod/page/n3/mode/2up>. (дата звернення: 04.12.2024).

42. Stoker, G. (2018). *Governance as theory: five propositions*. *International Social Science Journal*, 50(155), 17-28. – URL: https://www.academia.edu/1820158/Governance_as_theory_five_propositions. (дата звернення: 04.12.2024).

43. Sorensen E., Torfing J. Metagoverning Collaborative Innovation in Governance Networks. *The American Review of Public Administration*. 2017. Vol. 47, No. 7. P. 826–839. DOI: 10.1177/0275074016643181.

44. Sorensen E., Torfing J., Peters B. G., Pierre J. Interactive Governance: Advancing the Paradigm. Oxford : Oxford University Press, 2012. 273 p.
45. Torfing J. Collaborative Innovation in the Public Sector. Washington, DC : Georgetown University Press, 2016. 368 p. URL:https://www.academia.edu/63751628/Collaborative_Innovation_in_the_Public_Sector.
46. Fucuyama F. State-Building: Governance and World Order in the 21st Century. – URL: <https://www.jstor.org/stable/10.7591/j.ctvrf8c1g> (дата звернення: 23.12.2024).
47. Denhardt J. V., Denhardt R. B. The New Public Service: Serving Rather than Steering // *Public Administration Review*. 2000. Vol. 60, №о. 6. P. 549–559. URL: <https://doi.org/10.1111/0033-3352.00117> (дата звернення: 19.04.2025).
48. Denhardt J. V., Denhardt R. B. The New Public Service: Serving, Not Steering. Armonk, NY : M. Sharpe, 2011. 288 p. URL: <https://www.routledge.com> (дата звернення: 19.04.2025).
49. Bozeman B. Public Values and Public Interest: Counterbalancing Economic Individualism. Washington, DC : Georgetown University Press, 2007. 238 p. URL: <https://press.georgetown.edu> (дата звернення: 19.04.2025).
50. Bozeman B. All Organizations Are Public: Bridging Public and Private Organizational Theories. San Francisco : Jossey-Bass, 1987. 300 p. URL: <https://www.wiley.com> (дата звернення: 19.04.2025).
51. Bryson J. M., Crosby B. C., Bloomberg L. Public Value Governance: Moving Beyond Traditional Public Administration and the New Public Management *Public Administration Review*. 2014. Vol. 74, No. 4. P. 445–456. URL: <https://doi.org/10.1111/puar.12238> (дата звернення: 19.04.2025).
52. De Vries H., Bekkers V., Tummers L. Innovation in the Public Sector: A Systematic Review and Future Research Agenda. *Public Administration*. 2016. Vol. 94, №. 1. P. 146–166.

53. De Vries H., Tummers L., Bekkers V. The Diffusion and Adoption of Public Sector Innovations: A Meta-Synthesis of the Literature. *Perspectives on Public Management and Governance*. 2018. Vol. 1, №. 3. P. 159–176.

54. Van de Walle S., Bouckaert G. Public Service Performance and Trust in Government: The Problem of Causality. *International Journal of Public Administration*. 2003. Vol. 26, №. 8–9. P. 891–913.

55. Rosanvallon P. La légitimité démocratique. Impartialité, réflexivité, proximité. Paris : Éditions du Seuil, 2008. 367 p.

56. Fountain J. E. Building the Virtual State: Information Technology and Institutional Change. Washington, D.C. : Brookings Institution Press, 2001. URL: <https://www.brookings.edu/books/building-the-virtual-state/>.

57. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston, New York : Houghton Mifflin Harcourt, 2013. URL: <https://www.harpercollins.com/products/big-data-viktor-mayer-schonbergerkenneth-cukier>.

58. Drechsler W. The Rise and Demise of the New Public Management: Lessons and Opportunities for South East Europe. *Central European Public Administration Review*. 2005. Vol. 7, №. 3. URL: <https://journals.uni-lj.si/CEPAR/article/view/20285>.

59. O'Reilly T. Government as a Platform. *Innovations: Technology, Governance, Globalization*. 2011. Vol. 6, №. 1. P. 13–40. URL: https://doi.org/10.1162/INOV_a_00056.

60. Noveck B. S. Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful. – Washington, D.C. Brookings Institution Press, 2009. : URL <https://www.brookings.edu/books/wiki-government>.

61. Kotka T. Estonian e-Residency: Redefining the Nation-State in the Digital Era? : working paper . 2015. (e-Residency Series ; Working Paper No. 3) URL: https://proudengineers.com/wp-content/uploads/2025/01/Working_Paper_No.3_Kotka_Vargas_Korjus.pdf .

62. Chua B. H. Singapore as model: planning innovations, knowledge experts and the making of a city-state. *Worlding Cities: Asian Experiments and the Art of Being Global* / ed. by A. Roy, A. Ong. Malden, MA ; Oxford : Wiley-Blackwell, 2011. P. 29–54.

63. Foo S. L. Singapore's vision of a Smart Nation. Singapore Management University, 2015. URL: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=2558&context=soa_research.

64. Luhmann N. *Social Systems*; transl. by J. Bednarz Jr., D. Baecker. Stanford, CA : Stanford University Press, 1995. 627 p.

65. Сорокіна Н., Філатов В. Цифровізація публічного управління в Україні: теоретичний аспект. *Аспекти публічного управління*. 2025. №14 (1). С.77-81.

66. Черниш В., Баштанник В. Публічне управління в умовах інституціональних альтерацій в системі державної влади: теоретико-методологічні засади. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. №. 5. С. 7-13.

67. Rose, R. (1999). Living in an Anti-Modern Society. *East European Politics and Societies*, 13(2), 175–187. URL: <https://www.taylorfrancis.com/chapters/mono/10.4324/9780203884935-8/living-anti-modern-society-richard-rose>.

68. Черниш В. Інституціональні виклики для системи публічного влади в особливих режимах адміністрування. *Slovak international scientific journal*. 2023. № 70. С. 81-85. doi: 10.5281/zenodo.7808851/

69. Агафонова Н. В. Конституційна реформа в Україні: механізми реалізації та проблеми ефективності : монографія. Київ : Інститут законодавства Верховної Ради України, 2016. 416 с.

70. Woods, D. (2015). Four concepts for resilience. *Reliability Engineering & System Safety*. URL: <https://doi.org/10.1016/j.ress.2015.03.018>.

71. Morozov, E. (2013). To Save Everything, Click Here: The Folly of Technological Solutionism. New York: PublicAffairs. URL: <https://www.publicaffairsbooks.com/titles/evgeny-morozov/to-save-everything-click-here/9781610391399>.

72. Morozov, E. (2011). The Net Delusion: The Dark Side of Internet Freedom. New York: PublicAffairs. URL: <https://www.publicaffairsbooks.com/titles/evgeny-morozov/the-net-delusion/9781586488741>.

73. Баштанник В. Трансформація державного управління в контексті європейських інтеграційних процесів : монографія / В. В. Баштанник. – Дніпро : Моноліт, 2010. 390 с.

74. Баштанник В. Організаційні засади формування інтегрованих систем публічного управління як основи процесу реформування державного управління. Дніпровський науковий часопис публічного управління, психології, права. 2020. № 1. С. 5-12.

75. Баштанник В. Структурні характеристики та тенденції організаційного розвитку національних систем публічного управління в умовах сучасних євроінтеграційних процесів. Вісник НАДУ. 2009. № 1. С. 5 – 16.

76. Rudenko O. Conceptualization of the theory of public stability in the science of public administration Association agreement : driving integrational changes : monograph. Chicago, Illinois, USA. 2019. P. 13-25

77. Руденко О. Суспільні протиріччя як важливий фактор впливу на стабільність суспільного розвитку. Вісник НАДУ. 2005. № 4. С. 59–68.

78. Руденко О. Влада в системі забезпечення політичної стабільності : теоретико-методологічні аспекти. *Актуальні проблеми державного управління та самоврядування* : Донецьк : ДонДУУ, 2008. Т. IX. С. 202–217.

79. Руденко О. Інноваційна модель державного управління в контексті забезпечення суспільної стабільності. *Механізми державного управління та місцевого самоврядування : наук. вісн. Акад. муніцип. упр.* 2008. Вип. 1 (3). С.

95–103.

80. Руденко О. Забезпечення державної безпеки України в системі захисту національних інтересів. *Збірник наукових праць Донецького державного університету управління. Серія «Державне управління»*. 2019. Т. XX; Вип. 312. С. 42-50.

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

82. Резнікова О., Сьомін С. Проблеми організаційного забезпечення розбудови національної стійкості в Україні. *Public and municipal administration: theory, methodology, practice : Collective monograph. VERN' University of Applied Sciences, Zagreb, Croatia. Riga : Izdevnieciba «Baltija Publishing», 2020. С. 188–205.*

83. Бородін Є. І., Поступна О. В. Цифровізація як інструмент муніципального менеджменту: оптимізація функціонування органів місцевого самоврядування на деокупованих територіях. *Дніпровський науковий часопис публічного управління, психології, права*. 2025. Вип. 3 (2025). С. 13-20. DOI: 10.51547/ppp.dp.ua/2025.3.2.

84. Антонова О. В., Шаталов С. О. Електронна демократія та цифрова держава як інструменти громадянського суспільства в Україні. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2025. № 15. DOI: 10.54929/2786-5746-2025-15-02-04.

85. Fountain J. E. *Building the Virtual State: Information Technology and Institutional Change*. Washington, DC : Brookings Institution Press, 2001. 303 p. URL: <http://www.jstor.org/stable/10.7864/j.ctvcb59n3>.

86. Wegrich K. Is the turtle still plodding along? Public management reform in Germany. *Public Management Review*. 2021. Vol. 23, № 8. P. 1107–1116. URL: <https://www.tandfonline.com/doi/abs/10.1080/14719037.2020.1771011?needAccess=true>.

87. Walker B. H., Salt D. *Resilience Thinking: Sustaining Ecosystems and*

People in a Changing World. Washington, DC: Island Press, 2006. 192 p. URL: <https://faculty.washington.edu/stevehar/Resilience%20thinking.pdf>.

88. Holling C. S. Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*. 1973. Vol. 4. P. 1-23. URL: <https://pure.iiasa.ac.at/id/eprint/26/1/RP-73-003.pdf>.

89. Пирожков С. І., Майборода О. М., Хамітов Н. В. та ін. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз : національна доповідь. Київ : ІПіЕЕД ім. І. Ф. Кураса НАН України, 2022. 552 с.

90. Горбулін В. П. Як перемогти Росію у війні майбутнього. Київ : Брайт Букс, 2021. 248 с.

91. Резнікова О. О. Стратегічний аналіз безпекового середовища України. *Стратегічна панорама*. 2022. Спецвипуск. С. 45–53.

92. Ситник Г. П., Орел М. Г. Публічне управління у сфері національної безпеки : підручник. Київ : Видавець Кравченко Я. О., 2020. 360 с.

93. Резнікова О. О. Проблеми і перспективи забезпечення національної стійкості в умовах гібридних загроз. *Стратегічні пріоритети*. 2020. № 1. С. 45-56.

94. 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

95. Суходоля О. Стійкість критичної інфраструктури та життєво важливих функцій і послуг: формалізація завдань і змісту дій суб'єктів забезпечення. *Стратегічна панорама*. 2022. С. 5-20.

96. Резнікова О. О. Забезпечення національної стійкості: сутність та шляхи реалізації. *Стратегічна панорама*. 2020. № 1-2. С. 30-42.

97. Кондратенко О. Ю. Геополітичний вимір національної стійкості України. Міжнародні відносини, суспільні комунікації та регіональні студії. 2023. № 1 (15). С. 44-58.

98. Лазебник Я. Концепція національної стійкості: український

контекст. Вісник Львівського університету. Серія філософсько-політологічні студії. 2024. Вип. 56. С. 223-228.

99. Масик М. Клименко О. Теоретичні основи дослідження проблем інституціональної стійкості у міждисциплінарному дискурсі. Вчені записки ТНУ ім. В.І. Вернадського. Серія: Публ. управління та адміністрування. 2022. Том 33 (72). № 5. С. 53-58.

100. Національна доповідь: Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз / ред. кол. С.Пирожков та ін. / Київ: ІПіЕН ім. І. Ф. Кураса НАН України. 2022. 552 с.

101. Орел М. Аксіологічний аспект концепту «стійкість держави» у контексті функцій публічного управління у сфері безпеки та в історії наукової думки. Інвестиції: практика та досвід. 2018. № 24. С. 95-101.

102. Пирожков С. Національна стійкість України: стратегія забезпечення. Український географічний журна. 2022. № 2(118). С. 3-10.

103. Лопатченко І.М., Помаза-Пономаренко А.Л., Батир Ю.Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану. *Вісник Національного університету цивільного захисту України*. 2024. № 1 (20). С. 14–24.

104. Юхно І. Феномен стабільності публічноуправлінської діяльності в умовах системних реформ / Юхно І., Баштанник В. *Право та державне управління*. 2021. №2. С. 252-257.

105. Юхно І. Інституціональні засади публічноуправлінських змін в системі судової влади в умовах конституційного реформування. *Дніпровський науковий часопис публічного управління, психології, права*. 2021. №4. С. 50-54.

106. Помаза-Пономаренко А.Л., Микитюк Ю.М. Цифровізація державної політики vs. державна політика цифровізації у сфері правового регулювання : монографія. Х.: НУЦЗУ. 2021. 200 с.

107. Вітер Д., Руденко О. Теоретичне осмислення ідеальної сутності громадянського суспільства. Розвиток громадянського суспільства в Україні:

минуле, сучасність, перспективи. Видавництво Національного університету «Острозка академія» 2014. с. 21-46.

108. Рось О. Поняття та сутність нормативно-правового забезпечення інституційної спроможності представницьких органів місцевого самоврядування. Інвестиції, практика та досвід. 2019. №18. С. 97-100.

109. Жукова Л. Інституційна стійкість держави в умовах глобальної нестабільності. Економіка і суспільство. 2017. № 13. С. 3-7.

110. Баштанник О.В. The features of maintenance for institutial capacity of the Verkhovna Rada of Ukraine in modern conditions. *Débats scientifiques et orientations prospectives du développement scientifique* : c avec des matériaux de la VI conférence scientifique et pratique internationale, Paris, République Française, Mars 1er, 2024. Vinnytsia (Ukraine). 2024. P. 85-88.

111. Wilson W. (1887).The Study of Administration. *Political Science Quarterly*. 2(2), 197–222. – URL: <https://www.archives.gov/research/administration-of-government>.

112. Bouckaert G., Van de Walle S. Comparing measures of citizen trust and user satisfaction as indicators of «good governance». *International Review of Administrative Sciences*. 2003. Vol. 69, №. 3. P. 329-343.

113. Van de Walle S., Van Roosbroek S., Bouckaert G. Trust in the public sector: Is there any evidence for a long-term decline? *International Review of Administrative Sciences*. 2008. Vol. 74, №. 1. P. 47-64.

114. Harteveld E., Van der Meer T. W. G., De Vries C. E. In Europe we trust? Exploring three logics of EU trust. *European Union Politics*. 2013. Vol. 14, №. 4. P. 542–565.

115. Morozov E. To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems that Don't Exist. London: Allen Lane, 2013. 432 p.

116. Morozov E. The Folly of Technological Solutionism: What Happens When Bad Ideas Become Even Worse Tools. *The Breakthrough Journal*. 2013. Vol. 3. №. 1. P. 42-49.

117. Маматова Т., Чикаренко І., Бородін Є. (2022). Цифрові платформи Smart Specialisation Platform та Espon: структура та можливості для регіонів і громад ЄС. *Аспекти публічного управління*. 2022. № 10(6). С. 37-45.
118. Про правовий режим воєнного стану: Закон України від 12 травня 2015 року № 389-VIII. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text>.
119. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі: монографія. Харків: НУЦЗУ, 2024. 244 с.
120. Саганович Д.В. Інституціоналізація публічних послуг на основі принципу респонсивності: виклики в умовах змін механізмів територіального управління. *Публічне управління і адміністрування в Україні*. 2025. № 45. С.258-263.
121. Хожило І., Ковтун В. Внутрішньо переміщені особи у фокусі публічноуправлінської діяльності: аналіз понять і категорій в умовах збройного конфлікту. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. №3. С.19-25.
122. Бородін Є. І., Поступна О. В. Цифровізація як інструмент муніципального менеджменту: оптимізація функціонування органів місцевого самоврядування на деокупованих територіях. *Дніпровський науковий часопис публічного управління, психології, права*. 2025. Вип. 3 (2025). С. 13-20.
123. Кравцов О.В., Баштанник В.В. Інституціональні механізми забезпечення участі громади в муніципальному управлінні. *Публічне управління та адміністрування в Україні*. 2023. № 35. С.201-210/
124. Saganovich D. Features of the formation of the institute of public services in the context of the transformation of territorial organization of authority. *Slovak international scientific journal*. 2025. № 97. С. 83-86.
125. Osborne, S. P. Public Service Logic: Creating Value through Public Service Delivery. URL: <https://www.researchgate.net/publication/>

346310525_Public_Service_Logic_Creating_Value_for_Public_Service_Users_Citizens_and_Society_Through_Public_Service_Delivery.

126. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: Постанова Кабінету Міністрів України від 3 березня 2021 року № 167. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text/>

127. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Постанова Кабінету Міністрів України від 17 січня 2018 року № 67. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>.

128. Cheshire L., Esparcia J., Shucksmith M. Community resilience, social capital and territorial governance. P. 7-38. DOI: 10.4422/ager.2015.08.

129. Colantoni A., Halbac-Cotoara-Zamfir R., Halbac-Cotoara-Zamfir C., Cudlin P., Salvati L., & Gimenez Morera A. Demographic Resilience in Local Systems: An Empirical Approach with Census Data. *Systems*. 2020. № 8(3). 34 p. DOI: 10.3390/systems8030034.

130. Антонова Л. В., Антонов А.В. Електронне урядування як сервісно-орієнтований інструмент державного управління соціальною сферою. *Публічне управління та регіональний розвиток*. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2020. Вип. 7 С. 37–56. URL: <https://doi.org/10.34132/pard2020.07.02>

131. Антонова Л., Мохова Ю. Удосконалення механізмів електронного урядування в Україні в умовах цифрових перетворень. *Публічне управління та регіональний розвиток*. Миколаїв : Вид-во ЧНУ ім. Петра Могили. 2022. №15. С. 10–29. URL: <https://doi.org/10.34132/pard2022.15.01>.

132. Вовк М. М. Теоретико-концептуальні основи використання інформаційних систем в механізмі комунікації місцевої влади з громадянськістю. *Публічне управління і політика*. 2025. № 3(7). DOI: 10.70651/3041-2498/2025.3.04.

133. Dunleavy, P., Margetts, H. (2023). Digital government transformation: Changes in organizational capabilities and infrastructure. *Public Policy and Administration*, 38(4), 456-475. DOI: 10.1177/09520767231168234

134. Макурін А. Цифрова трансформація взаємодії: удосконалення публічного управління та інформаційна обробка облікових даних через діджиталізацію в Україні. *Публічне управління і адміністрування в Україні*. 2025. №45. С.249-253.

135. Блінова Г. Правові засади використання електронних інформаційних ресурсів в концепції цифрової держави. *Проблеми сучасних трансформацій*. Серія: право, публічне управління та адміністрування. 2021 №2. С. 53-60.

136. Красников Є. Управління ефективністю надання публічних послуг. *Наукові перспективи*. 2023. № 11(41). URL: <http://perspectives.pp.ua/index.php/np/article/view/7651/7696>.

137. Ортіна Г.В. Діджиталізація державного управління: виклики та перспективи впровадження в Україні. *Вісник національного університету цивільного захисту України*. Серія «Державне управління». 2025. № 1 (22). С. 33–42.

138. Ковальов В.Г., Кравцов О.В. Діджиталізація публічних послуг для внутрішньо переміщених осіб в Україні: огляд, виклики та перспективи. *Публічне управління і адміністрування в Україні*. 2025. №46. С.156-161.

139. Філатов В. Цифрові платформи у публічній владі: виклики правового регулювання діджиталізації для розвитку демократичної участі громадянськості. *Публічне управління та адміністрування в Україні*. 2025. №46. С. 151-155. DOI <https://doi.org/10.32782/TNU-2663-6468/2024.6/37>.

140. Ковтун В. Правове регулювання міжсекторальної взаємодії в системі життєзабезпечення внутрішньо переміщених осіб. *Національні інтереси України*. 2025. №6. URL: <http://perspectives.pp.ua/index.php/niu/article/view/25300>.

141. Легеза Є. О. Особливості реформування надання публічних

послуг в Україні. Право і суспільство. 2016. № 3. Ч. 1. С. 117–121.

142. Саганович Д.В. Модернізація механізму надання публічних послуг в контексті викликів для системи державної влади. *Публічне управління і адміністрування в Україні*. 2024. № 42. С.195-200. <https://doi.org/10.32782/pma2663-5240-2024.42.34>.

143. Yevgen Krasnykov, Oleksandr Bobos, Ihor Lavrinets, Tetiana Khabarova, Nataliia Zozulia. The Impact of Electronic Governance on the Quality of Public Services and Municipal Property Management. *Pakistan Journal of Criminology*. January-March 2024. Vol. 16, № 01, p. 201-216. URL: <https://www.pjcriminology.com/publications/the-impact-of-electronic-governance-on-the-quality-of-public-services-and-municipal-property-management>.

144. Платформа «Дія.Цифрова освіта». URL: https://egap.in.ua/project/diyacifrova_osvita.

145. Olsen J. (2007). The Institutional Dynamics of the European Union. Oxford: Oxford University Press. – URL: https://www.researchgate.net/publication/5014564_The_Institutional_Dynamics_of_the_European_University.

146. Pierson, P. (2000). Increasing Returns, Path Dependence, and the Study of Politics. *American Political Science Review*. 94(2). P. 251–267.

147. March J., Olsen J. Rediscovering Institutions: The Organizational Basis of Politics – URL: <https://books.google.com.ua/books/about>.

148. Ostrom E. Governing the Commons: The Evolution of Institutions for Collective Action (Political Economy of Institutions and Decisions). Cambridge: Cambridge University Press. 1991. 298 p.

149. Поченчук Г. Теоретичні основи інституціонального реформування. Міжнародний гуманітарний вісник. 2017. № 28. URL: <http://www.vestnik-econom.mgu.od.ua/journal/2017/28-2017/7.pdf>.

150. Стрельцов В. Ю. Формування та розвиток концепції європейського врядування. *Актуальні проблеми державного управління*. 2009. № 1. С. 377-384.

151. Руденко О.М. Дефініції суспільної стабільності в державному управлінні. *Стратегічні пріоритети*. № 3. 2009. С. 10– 09.
152. Чубара Т. Організаційно-правові засади реалізації функцій влади з охорони громадського порядку на місцевому рівні. *Державне управління та місцеве самоврядування* : зб. наук. пр. Дніпро : ДРІДУ НАДУ, 2010. Вип. 4. С. 112-120.
153. Чубара Т. Удосконалення взаємодії державних служб охорони порядку з населенням у контексті реалізації правозабезпечувальної функції публічної влади. *Державне управління та місцеве самоврядування* : зб. наук. пр. – Д. : ДРІДУ НАДУ, 2011. Вип. 1. С. 78-86.
154. Мерзляк А. Механізми державного управління іноземними інвестиціями: регіональний аспект: монографія. Київ : Вид-во УАДУ, 2002. 300 с.
155. Рудніцька Р. Сутність та зміст механізмів державного управління та принципів їх функціонування. *Публічне управління: теорія та практика*. 2014. Вип. 4. С. 50- 60.
156. Федорчак О. Класифікація механізмів державного управління. *Демократичне врядування : Науков. вісник ЛРІДУ НАДУ*. Електронний ресурс URL: Режим доступу: www.lvivacademy.com_O_Fedorchak.pdf.
157. Boas T.C. Conceptualizing continuity and change: the composite-standard model of the Path dependence . *Journal of Theoretical Politics*. 2007. № 19 (1). P. 33-54.
158. Havrylenko A., Yukhno I., Chernysh V. Institutional principles of public management activity in the conditions of constitutional reform. *Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia*: collective monograph. Izdevnieciba “Baltija Publishing” (Riga, Latvia). 2023. P. 203-230. URL: <http://baltijapublishing.lv/omp/index.php/bp/catalog/view/293/8191/17095-1>.
159. Макурін А. Ефективна публічна влада без корупції: економічна та антикорупційна політики у розбудові правової держави. *Дніпровський*

науковий часопис публічного управління, психології, права. 2025. №1. С.49-53.

160. Akimova L., Litvinova I., Ilchenko H., Pomaza-Ponomarenko A., Yemets O. The negative impact of corruption on the economic security of states. *Scientific journal «International Journal of Management»*. 2020. № 11(5). P.1058-1071. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3632656.

161. Pasternak, I., Krap, A., Yastrubetska, L., Grytsyshen, D., & Sergiienko, L. (2023). The Role and Influence of International Organizations in Shaping and Maintaining International Legal Order and Global General and Financial Security. *Journal of Law and Sustainable Development*, 11(12), e2363.

162. Бондар В. Національна стійкість в системі національної безпеки: інформаційно-психологічний чинник. *Суспільство та національні інтереси*. 2024. № 5(5). URL: [https://doi.org/10.52058/3041-1572-2024-5\(5\)-477-487](https://doi.org/10.52058/3041-1572-2024-5(5)-477-487) (дата звернення: 22.12.2024).

163. Александров В. Основні наукові підходи щодо публічного управління забезпечення національної стійкості України. Наукові перспективи (Naukovі perspektivi). 2022. № 9(27). URL: [https://doi.org/10.52058/2708-7530-2022-9\(27\)-21-34](https://doi.org/10.52058/2708-7530-2022-9(27)-21-34) (дата звернення: 22.12.2024).

164. Коваль З., Повов С. Комплексний механізм державного управління: національна доктрина стійкості України, стратегія стійкої та активної оборони, тактика стійких асиметричних дій в інформаційно-психологічну епоху. *Актуальні проблеми державного управління*. 2021. №3(84). С. 99-104.

165. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

166. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII : станом на 18 груд. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

167. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 27 квіт. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.

168. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 15 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>.

169. General Data Protection Regulation(GDPR). URL:<https://gdpr-info.eu>.

170. Що таке Цілі сталого розвитку? URL: <https://www.undp.org/uk/ukraine/tsili-staloho-rozvytku>.

171. Міжнародний союз електрозв'язку (МСЕ). URL: <https://geneva.mfa.gov.ua/posolstvo/2616-itu>.

172. The European Interoperability Framework. URL: <https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail>.

173. Міляєва М. В. Адміністративно-правове забезпечення розбудови електронного врядування. *Expert paradigm of law and public administration*. 2024. № 2(30). С. 39–45.

174. Цифрова трансформація економіки України в умовах війни. Квітень 2024 року. URL: <https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-kviten-2024>.

175. Богоніс А. Цифровізація інформації: нові виклики в системі державного управління. *Успіхи і досягнення у науці*. 2024. № 5(5). URL: [https://doi.org/10.52058/3041-1254-2024-5\(5\)-269-276](https://doi.org/10.52058/3041-1254-2024-5(5)-269-276).

176. Abbasi S., Jung B.K. Mapping of Key Digital Health Initiatives Building Resilience for Current and Future Pandemics. *Mapping of Key Digital Health Initiatives Building Resilience for Current and Future Pandemics*. 2023. p.1-23.
URL:<https://ieeexplore.ieee.org/abstract/document/10026166/authors#authors>.

177. Digital transformation challenges: strategies emerging from a multi-

stakeholder approach / F. Brunetti et al. The TQM journal. 2020. Vol. 32, no. 4. P. 697–724. URL: <https://doi.org/10.1108/tqm-12-2019-0309>.

178. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навч. посібник. Ірпінь, 2000. 304 с.

179. Новицький Г. В. Теоретико-правові основи забезпечення національної безпеки. Київ : Інтертехнологія, 2008. 496 с.

180. Голубь В. Інституціоналізація інтеракцій держави і суспільства як основа формування ефективної держави. *Актуальні проблеми державного управління*. 2021. № 1(59). С. 8–16. С. 13..

181. Фердман Г.П. Корупція як одна з головних загроз національній безпеці України. Вчені записки Таврійського національного університету ім. В.І.Вернадського серія Публічне управління у сфері державної безпеки та охорони громадського порядку. Том 35 (74) № 1, 2024, С. 201-205.

182. Castells, M. The Rise of the Network Society. *The Information Age: Economy, Society and Culture*, Vol. 1. 2nd ed. Oxford: Blackwell, 2009. URL: https://www.researchgate.net/publication/339282743_The_Rise_of_the_Network_Society_-_The_Information_Age_Economy_Society_and_Culture

183. Sassen, S. Territory, Authority, Rights: From Medieval to Global Assemblages. Princeton: Princeton University Press, 2006. URL: https://www.researchgate.net/publication/30529777_Territory_Authority_Rights_From_Medieval_to_Global_Assemblages.

184. Kveliashvili I., Akimova L., Yevdokymov V., Kotviakovskiy Y., Akimov O. Legal bases and features of public administration in the budget sphere in ukraine and foreign countries Ad Alta: Journal Of Interdisciplinary Research The 2021.April.

185. Kveliashvili I., Kupriichuk V., Pershko B., Kyrychenko H., Danylyuk E. Development of the financial and economic security of the company based on the superintendence of its business activity. *Ad Alta: Journal Of Interdisciplinary Research* . 2021. January.

186. Kveliashvili Iryna and other. Theoretical Foundations Of Innovation

In Public Administration Larysa Gaievska, Ad Alta: Journal Of Interdisciplinary Research. 2021. March. Web of Science

187. Квеліашвілі І. М. Комунікаційна стратегія як засіб стимулювання трансформаційних процесів у митній сфері. *Публічне управління та митне адміністрування*. 2021. №4(31). С. 59-65.

188. Бобровська О. Ю., Хожило І. І., Шумік І. В. Корпоративне управління соціальною сферою: концептуальні засади : навч. посіб. Дніпропетровськ, 2011. 215 с.

189. Блінова Г. Сучасні виклики та перспективи публічного управління у сфері регіональної екологічної політики у контексті антикорупційного законодавства. *Дніпровський науковий часопис публічного управління, психології, права*. 2025. №1. С.25-32/

190. Нова парадигма державного управління та корпоративної культури в Україні: монографія. Чернівці : Технодрук, 2016. 244 с.

191. Драгомирецька Н. М., Піроженко Н. В., Матвєєнко І. В. Державно-громадянське партнерство у сфері соціального розвитку : навч. посіб. Одеса : ОРІДУ НАДУ, 2017. 290 с.

192. Колосовська І. І. Детермінуючі фактори формування соціальної концепції публічного управління. *Демократичне врядування*. Львів : НУ «Львівська політехніка», 2023. Вип. 1(31). С. 108-117.

193. Колосовська І. І. Соціальні вектори публічної політики у контексті викликів війни в Україні. *Розвиток публічного управління в контексті європейської інтеграції України* : матер. наук.-практ. конф. (28 квітня 2023 р., м. Львів). Львів : НУ «Львівська політехніка», 2023. С. 16-19. URL: <https://lpnu.ua/dpv/tezy-konferentsii>.

194. Ortina G. The role of the state in transforming the public administration system for sustainable regional development in the context of digitalization // *Public administration and state security aspects*. 2025. Vol. 1. Pp. 229–241. URL: <http://passa.nuczu.edu.ua/en/archive/238-ortina-g-the-role-of-the-state-in-transforming-the-public-administration-system-for-sustainable->

regional-development-in-the-context-of-digitalization.

195. Safarov I. Institutional dimensions of open government data implementation: Evidence from transition countries. *Public Performance & Management Review*. 2020. Vol. 43. №. 6. P. 1359–1389. URL: <https://www.tandfonline.com/doi/epdf/10.1080/15309576.2020.1805336?needAccess=true>.

196. Sydorchuk, O., Bashtannyk, V., Terkhanov, F., Kravtsov, O., Akimova, L., & Akimov, O. (2024). Integrating digitization into public administration: Impact on national security and the economy through spatial planning. *Edelweiss Applied Science and Technology*, 8(5), 747–759. URL: <https://learning-gate.com/index.php/2576-8484/article/view/1740>.

197. Кравцов О. Кравцова Т.В., Лащенко О.В. Теоретичні основи впровадження антикризового менеджменту в діяльність органів публічного управління. *Аспекти публічного управління*. 2021. № 9. 64-72.

198. Кравцов О.В. Баштанник В.В. Інституціональні механізми забезпечення участі громади в муніципальному управлінні. *Публічне управління та адміністрування в Україні*. 2023. № 35. С.201-210.

199. Кравцов О.В., Баштанник В.В., Порівняльний аналіз сучасних моделей участі громади в муніципальному управлінні країн ЄС та України у контексті сучасних трендів адміністрування. *Публічне управління та адміністрування в Україні*. 2023. № 37. С.202-214.

200. Кравцов О.В., Кандзюба С.П., Титаренко О.М. Методика формування простору електронної взаємодії у межах об'єднаної територіальної громади. *Аспекти публічного управління*. 2015. № 5-6. С. 76-84.

201. Кравцов О.В. Краудсорсинг в системі державного управління. *Державне управління та місцеве самоврядування*. 2014. № 4. С. 15-23.

202. Broadhurst K., Gray N. (2022). Understanding resilient places: Multi-level governance in times of crisis. *Local Economy: The Journal of the Local Economy Policy Unit*. № 37. URL:

<https://journals.sagepub.com/doi/10.1177/02690942221100101>.

203. Ахмедова О.О., Помаза-Пономаренко А.Л. Цифровізація державного сектору як чинник ефективного публічного управління. *Наукові перспективи*. 2025. Вип.2(56). URL:

<http://perspectives.pp.ua/index.php/np/article/view/20697>.

204. Гройсман В. Процеси централізації та децентралізації в сучасному державному управлінні. *Державне управління та місцеве самоврядування* : зб. наук. 2015. Вип. 2 (25). С. 26–37.

205. Роман В. Досвід децентралізації та деконцентрації влади країн ЄС/ *Державне управління та місцеве самоврядування* : Вип. 2 (29). 2016. С. 51–58.

206. European Governance. A White Paper. Commission of the European Communities. COM (2001) 428 final. Brussels, 25.07.2001. URL: www.ec.europa.eu/governance/contrib_efc_en.pdf.

207. Milward Alan S. The European Rescue of the Nation State. London : Routledge. 2000. 453 p.

208. Moravcsik A. Preferences and Power in the European Community. A Liberal Intergovernmentalist Approach. *Journal of Common Market Studies*. 1993. Vol.31. №4. P. 482-498.

209. Facing the challenge. The Lisbon strategy for growth and employment. Luxembourg : Office for Official Publications of the European Communities, 2004. 54 p.

210. Nomenclature of territorial units for statistics – NUTS Statistical Regions of Europe. URL: ec.europa.eu/comm/eurostat/ramon/nuts/home_regions_en.html.

211. Westley, F. Social Innovation and Resilience: How One Enhances the Other. *Stanford Social Innovation Review*. 2013. URL: https://ssir.org/articles/entry/social_innovation_and_resilience_how_one_enhances_the_other.

212. Expressions of Resilience: From “Bounce Back” to Dynamic

Adaptation and Transformation. Factsheet. URL: <https://www.files.ethz.ch/isn/170633/Factsheet-Expressions-of-Resilience.pdf>.

213. Гладкий С. Теоретичні засади оптимізації публічного управління в умовах розвитку цифрових ресурсів в Україні. *Інвестиції: практика та досвід*. 2023. № 9. С. 150–155.

214. Pushing the Boundaries of Innovation in Sustainable and Resilient Infrastructure. ICSI (Infrastructure and Climate-Sustainable Innovation) Report. 2024. URL: https://sustainability-coalition.org/wp-content/uploads/2024/07/Pushing-the-Boundaries-of-Innovation-in-Sustainable-and-Resilient-Infrastructure_.pdf.

215. Helmrich A., Chester M., Underwood B. Centralization and decentralization for resilient infrastructure systems: Concepts, models, and tradeoffs. *Current Opinion in Environmental Sustainability*. 2021. URL: <https://iopscience.iop.org/article/10.1088/2634-4505/ac0a4f>.

216. Hotchkiss E. et al. Resilience Roadmap: A Collaborative Approach to Multi-Jurisdictional Resilience Planning. NREL, 2019. URL: <https://docs.nrel.gov/docs/fy19osti/73509.pdf>.

217. Белікова М. Цифровізація публічного адміністрування в умовах воєнного стану. *Наукові інновації та передові технології*. 2022. № 8(10). URL: [https://doi.org/10.52058/2786-5274-2022-8\(10\)-381-392](https://doi.org/10.52058/2786-5274-2022-8(10)-381-392) (дата звернення: 20.11.2024).

218. Демчишак Н. Б., Юрків Р. Р., Демид В. М. Іноземний досвід стимулювання розвитку інноваційного підприємництва: імплементація в умовах цифровізації економіки України та зміцнення національної безпеки. *Агросвіт*. 2023. № 17. С. 30–38. URL: <https://doi.org/10.32702/2306-6792.2023.17.30> (дата звернення: 20.11.2024).

219. Дяченко В., Дяченко Н. Публічний digital-маркетинг як елемент державної інформаційної політики. *Наукові перспективи*. 2024. № 2(44). URL: [https://doi.org/10.52058/2708-7530-2024-2\(44\)-245-254](https://doi.org/10.52058/2708-7530-2024-2(44)-245-254) (дата звернення: 20.11.2024).

220. Дяченко Н. Державні механізми сприяння відновленню громадського здоров'я у період воєнного стану. *Суспільство та національні інтереси*. 2024. № 3(3). URL: [https://doi.org/10.52058/3041-1572-2024-3\(3\)-21-33](https://doi.org/10.52058/3041-1572-2024-3(3)-21-33) (дата звернення: 20.11.2024).

221. Панькова, О.В., Касперович, О.Ю. Соціальний діалог і трудова сфера України в умовах воєнного стану, євроінтеграції, цифровізації: проблеми та перспективи для повоєнного відновлення. *Економіка промисловості*. 2023. № 2 (102). С. 78-104. URL: <http://dspace.nbuv.gov.ua/handle/123456789/191399>(дата звернення: 20.11.2024).

222. Подобєд І. Цифровізація як сучасний тренд трансформації ресурсного механізму системи цивільного захисту. *Науковий вісник: державне управління*. 2024. № 1 (15). С. 82–103.

223. Цифровізація як інструмент побудови інноваційної стратегії розвитку бізнесу країн єс в умовах адаптації до кризових тенденцій міжнародної економіки / В. Ю. Стрілець та ін. *Scientific bulletin of PUET: economic sciences*. 2024. № 3(113). URL: <https://doi.org/10.37734/2409-6873-2024-3-11>

224. Худолєй Я., Загребельна Н. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *Legal Bulletin*. 2023. С. 75–82.

225. Поврозник П. П. Бюджетно-податкові інструменти стимулювання інноваційного розвитку підприємництва в умовах цифровізації національної економіки. *Наукові записки Національного університету «Острозька академія». Серія «Економіка»*. Острог : Вид-во НаУОА, вересень 2023. № 30(58). С. 4–13.

226. Конституція України. Закон України від 28 червня 1996р. Відомості Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 20.11.2024).

227. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII : станом на 27 лип. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text> (дата звернення: 20.11.2024).

228. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 9 серп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

229. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII : станом на 1 січ. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

230. Про стимулювання розвитку цифрової економіки в Україні : Закон України від 15.07.2021 № 1667-IX: станом на 1 січ. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text>.

231. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX : станом на 1 січ. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>.

232. 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.mbo.gov.ua/ua/Ukazy/5017.html>.

233. Дія : державні послуги онлайн. URL: <https://diia.gov.ua>.

234. Estonian e-Government: URL: <https://e-estonia.com>.

235. «єВідновлення». URL: <https://erecovery.diia.gov.ua>.

236. «єВорог». URL: <https://evorog.gov.ua>.

237. Регламент e-IDAS (Регламент Європейського парламенту і Ради ЄС № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС. URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text.

238. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.

Вимоги (ISO/IEC 27001:2022, IDT). URL:
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398.

239. В Апараті РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему «COTA». URL:
<https://www.rnbo.gov.ua/ua/Diialnist/5011.html>.

240. Екосистема Defense Tech. URL:
<https://defensetechforukraine.org/ua>.

241. Платформа «Армія+». URL: <https://aplus.mod.gov.ua>.

242. Проект Закону про внесення змін до Конституції України (щодо скасування адвокатської монополії). URL:
https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66242/

243. Проект Закону про внесення змін до Конституції України щодо закріплення повноважень президента України утворювати незалежні регуляторні органи, Національне антикорупційне бюро, призначати на посади та звільняти з посад директорів Національного антикорупційного бюро та Державного бюро розслідувань (№1014). URL:
<https://zakon.rada.gov.ua/laws/show/29-20#Text/>

244. Проект Закону про внесення змін до Конституції України щодо законодавчої ініціативи народу (№1015). URL:
https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66254.

245. Проект Закону про внесення змін до статей 85 та 101 Конституції України (щодо уповноважених Верховної Ради України) (№1016). URL:
https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66256

246. Проект Закону про внесення змін до Конституції України щодо зменшення конституційного складу Верховної Ради та закріплення пропорційної виборчої системи (№1017). URL:
[:https://zakon.rada.gov.ua/laws/show/488-IX#Text](https://zakon.rada.gov.ua/laws/show/488-IX#Text).

247. Проект Закону про внесення змін до Конституції України щодо додаткових підстав дострокового припинення повноважень народного депутата.. URL: <https://ips.ligazakon.net/document/JI00017A?an=332>.

248. Проект Закону про внесення змін до Конституції України щодо консультативних, дорадчих та інших допоміжних органів Верховної Ради (№1028) URL: <https://ips.ligazakon.net/document/JI00016A>.

249. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України №392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037>.

250. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013>.

251. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. *Законодавство України : офіц. портал*. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>

252. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України №121/2021. *Законодавство України : офіц. портал*. URL: <https://zakon.rada.gov.ua/laws/show/n0022525-21>.

253. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України №56/2022. *Законодавство України : офіц. портал*. URL: <https://zakon.rada.gov.ua/laws/show/56/2022#Text>.

254. Про рішення Ради національної безпеки і оборони України від 30 липня 2021 року «Про Стратегію зовнішньополітичної діяльності України» : Указ Президента України від 26.08.2021 № 448/2021. URL: <https://www.president.gov.ua/documents/4482021-40017>.

255. Деякі питання реформування державного управління: Розпорядження Кабінету Міністрів України від 24 червня 2016 року № 474 . URL: <https://zakon.rada.gov.ua/laws/show/474-2016-%D1%80#Text>.

256. Деякі питання реформування державного управління: Розпорядження Кабінету Міністрів України від 21 липня 2021 р. № 831. URL: <https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#Text>.

257. Про Збройні Сили України: Закон України від 6 грудня 1991 року № 1934-XII. URL: <https://zakon.rada.gov.ua/laws/show/1934-12#Text>.

258. Про оборону України: URL: Закон України від 6 грудня 1991 року № 1932-XII. URL: <https://zakon.rada.gov.ua/laws/show/1932-12#Text>.

259. Про Стратегію сталого розвитку «Україна–2020» : Указ Президента України від 12 січня 2015 року № 5/2015. URL: <http://www.president.gov.ua/documents/18688.html>.

260. Баштанник В. Структурні характеристики та тенденції організаційного розвитку національних систем публічного управління в умовах сучасних євроінтеграційних процесів. Вісник НАДУ. 2009. № 1. С. 5 – 16.

261. Юхно І. Феномен стабільності публічноуправлінської діяльності в умовах системних реформ. *Право та державне управління*. 2021. №2. С. 252-257.

262. Баштанник В. Управління в системі наддержавних інтеграційних процесів в Європі : теоретико-методологічні засади. *Вісник НАДУ*. 2006. №3. С. 302 – 307.

263. Лозицька І. О. Теоретико-методологічні засади імплементації зарубіжного досвіду реформування державного управління. *Аспекти публічного управління*. 2016. № 1-2. С. 34-41.

264. Лозицька І.О. Зарубіжний досвід адміністративного реформування: організаційні та інституціональні засади теоретичного аналізу. Наук. вісн. Академії муніципального управління. 2016. Вип. 4. С. 161–168.

265. Лозицька І.О. Аналіз та адаптація зарубіжного досвіду як напрям удосконалення системи державного управління. *Публічне адміністрування*:

теорія та практика. 2016. № 2. Режим доступу:
[http://www.dridu.dp.ua/zbirnik/2016-02\(16\)/index.html](http://www.dridu.dp.ua/zbirnik/2016-02(16)/index.html).

266. Лозицька І. Імплементация зарубіжного досвіду в умовах розвитку державотворення та державного управління. *Державне управління та місцеве самоврядування*. 2018. Вип. 2. С. 42-49.

267. Лозицька І. О. Теоретико-методологічні засади імплементації зарубіжного досвіду реформування державного управління : Дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.01 Теорія та історія держ. упр.; Нац. акад. держ. упр. при Президентові України, Дніпропетров. регіон. ін-т держ. упр. Дніпро, 2018. 220 с.

268. Kryshchanovych M., Dragan I., Grytsyshen D., Sergiienko L., Baranovska T. The Public and Environmental Aspect of Restoring Sustainable Regional Development in the Face of the Negative Impact of Military Actions on the Territory of the Country. *International journal of sustainable development and planning*. Vol. 17, No. 5, August, 2022, pp. 1645-1651. URL: <https://www.iieta.org/journals/ijstdp/paper/10.18280/ijstdp.170530>.

269. Khomyshyn I., Dragan I., Sidelkovskyi O., Yepryntsev P., Olena Fatkhutdinova. Features of Digitalization of Jurisprudence in the Context of Improving the Legal System. *IJCSNS. International Journal of Computer Science and Network Security*. 2022. Vol. 22. No. 11. pp. 585-589. URL: <https://doi.org/10.22937/IJCSNS.2022.22.11.82>

270. Bashtannyk, A., Akimova, L., Kveliashvili, I., Yevdokymov, V., Kotviakovskiy, Y., & Akimov, O. (2021). Legal bases and features of public administration in the budget sphere in Ukraine and foreign countries. *Ad Alta: Journal of interdisciplinary research*, 1(1), XVIII, pp. 63-68.

271. Ткаченко О. В., Євтушенко І. В. Удосконалення нормативно-правового регулювання сфери безпеки і оборони в умовах військової агресії. *Чесць і закон*. 2022. №3 (89). С. 61-66.

272. OECD. Open Government: The Global Context and the Way Forward. <https://www.oecd.org/gov/open-government.htm>.

273. O'Reilly T. Government as a Platform. URL:<https://www.oreilly.com/radar/the-government-as-a-platform>.
274. Семілетов, О. (2023) Вплив цифровізації на трансформацію місцевого самоврядування. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління , 4(70), 63-69. URL:[https://doi.org/10.32689/2523-4625-2023-4\(70\)-9](https://doi.org/10.32689/2523-4625-2023-4(70)-9).
275. O'Reilly, T. (2011). Government as a Platform. *Innovations: Technology, Governance, Globalization*. 6(1). P.13-40. URL:https://doi.org/10.1162/INOV_a_00056.
276. Kitsing, M. (2021). Success Without Strategy: E-Government Development in Estonia. *Policy & Internet*, 13(2), 159-176. URL:<https://doi.org/10.1002/poi3.254>.
277. Janssen, M., van der Voort, H., & Wahyudi, A. (2017). Factors influencing the adoption of e-government initiatives: The case of the digital public platform. *Government Information Quarterly*. 2017. 34(3). p. 495-505.
278. Janssen, M., & van der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly*, 33(1), 1-5. URL:<https://doi.org/10.1016/j.giq.2016.02.003/>
279. Lips, M. Understanding public service provision using digital government services: A complexity theory perspective. *Government Information Quarterly*. 2022. Vol. 39(4). Article 101723.
280. Amdahl, G.M. (1967). Validity of the Single Processor Approach to Achieving Large Scale Computing Capabilities. *Proceedings of the April 18-20, 1967, Spring Joint Computer Conference*, 483-485. URL: <https://dl.acm.org/doi/10.1145/1465482.1465560>.
281. Bondi, A.B. (2000). Characteristics of Scalability and Their Impact on Performance. *Proceedings of the 2nd International Workshop on Software and Performance*, 195-203. URL: <https://dl.acm.org/doi/10.1145/350391.350432>.
282. Alexander, D.E. (2013). Resilience and disaster risk reduction: an etymological journey. *Natural Hazards and Earth System Sciences*, 13(11), 2707-

2716. URL: <https://nhess.copernicus.org/articles/13/2707/2013/nhess-13-2707-2013.html>.

283. Criado, J.I., & Gil-Garcia, J.R. (2019). Creating public value through smart technologies and strategies: From digital services to artificial intelligence and beyond. *International Journal of Public Sector Management*, 32(5), 438-450. URL: <https://www.emerald.com/ijpsm/article/32/5/438/151593/Creating-public-value-through-smart-technologies>.

284. Позняковська Н., Міклуха О. Аналіз зрілості екосистеми відкритих даних та розвиток громадянського суспільства. *Економіка та суспільство*. 2023. № 52. С. 1–8. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/2524/2442>.

285. Dunleavy, P., & Margetts, H. (2013). The second wave of digital-era governance: a quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 371(1987), 20120382. URL: <https://pubmed.ncbi.nlm.nih.gov/23419851>.

286. Sołtysik-Piorunkiewicz A., Zdonek I. How society 5.0 and industry 4.0 ideas shape the open data performance expectancy. *Sustainability*. 2021. Vol. 13. No. 2. 917. URL: <https://www.mdpi.com/2071-1050/13/2/917>.

287. Козієнко Р. Відкриті дані в Україні: досягнення, переваги, застереження. *Cedos*. 2021. URL: <https://cedos.org.ua/researches/vidkryti-dani-v-ukrayini-dosyagnennya-perevagy-zasterezhennya>.

288. Доброгорський О. Відкритість та громадська залученість у забезпеченні принципів ефективності та прозорості публічного управління. *Наукові перспективи*. 2023. Вип. 11 (41). С. 102–115. DOI: [https://doi.org/10.52058/2708-7530-2023-11\(41\)-102-115](https://doi.org/10.52058/2708-7530-2023-11(41)-102-115) .

289. Савченко О. Інноваційні аспекти розвитку цифровізації публічного управління в США. *Democratic Governance*. 2022. Vol. 15 (2). Р. 120–130. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2023/jan/29806/verstka30-122-132.pdf> .

290. Бондар Г. Л. Цифрова трансформація уряду України, відкриті дані (open data) та електронні послуги. *Публічне управління та регіональний розвиток*. 2021. № 11. С. 97–123. URL: http://nbuv.gov.ua/UJRN/purr_2021_11_7.

291. Сіленко А. О., Крук Н. В. Відкритий уряд: досвід Сполучених Штатів Америки та європейських країн. *Актуальні проблеми політики*. 2020. Вип. 65. С. 76–82. URL: http://app.nuoua.od.ua/archive/65_2020/13.pdf.

292. Каретна О. О., Милосердна І. М., Ігнат'єва І. І. Роль та особливості інформаційно-комунікаційних технологій у взаємодії органів державної влади з громадянським суспільством. *Політикус*. 2020. Вип. 5. С. 62–68. URL: http://politicus.od.ua/5_2020/11.pdf.

293. Лунін Д. С. Зарубіжний досвід адміністративно-правового забезпечення електронного урядування та його впровадження в Україні. *Юридична наука*. 2020. № 1 (103). С. 178–192. DOI: <https://doi.org/10.32844/2222-5374-2020-103-1.22>.

294. Gil-Garcia J. R., Dawes S. S., Pardo T. A. Digital government and public management research: finding the crossroads. *Public Management Review*. 2017. Vol. 20 (5). P. 633–646. DOI: <https://doi.org/10.1080/14719037.2017.1327181>.

295. Lapuente V., Van de Walle S. The effects of new public management on the quality of public services. *Governance*. 2020. Vol. 33 (3). P. 461–475. DOI: <https://doi.org/10.1111/gove.12502>.

296. Ansell C., Gash A. Collaborative Platforms as a Governance Strategy. *Journal of Public Administration Research and Theory*. 2018. Vol. 28 (1). P. 16–32. DOI: <https://doi.org/10.1093/jopart/mux030>.

297. Millard J. Open governance systems: Doing more with more. *Government Information Quarterly*. 2018. Vol. 35 (4). P. 577–587. DOI: <https://doi.org/10.1016/j.giq.2015.08.003>.

298. Janowski T., Estevez E., Baguma R. Platform governance for sustainable development: Reshaping citizen-administration relationships in the

digital age. *Government Information Quarterly*. 2018. Vol. 35 (4). P. 511–516. DOI: <https://doi.org/10.1016/j.giq.2018.09.002>.

299. Twizeyimana J. D., Andersson A. The public value of E-Government – A literature review. *Government Information Quarterly*. 2019. Vol. 36 (2). P. 167–178. DOI: <https://doi.org/10.1016/j.giq.2019.01.001>.

300. Єдиний вебпортал використання публічних коштів: офіційний вебсайт. URL: <https://spending.gov.ua> .

301. Платформа електронної демократії: офіційний вебсайт. URL: <https://e-dem.ua> .

302. Консультації з громадськістю: офіційний вебсайт. URL: <https://consult.e-dem.ua/0710100000> .

303. Єдиний портал публічних послуг «Дія»: офіційний вебсайт. URL: <https://diia.gov.ua> .

304. X-Road – цифрова платформа для обміну даними між державними установами: офіційний вебсайт. URL: <https://x-road.global> .

305. Data.gov.uk – портал відкритих даних Великої Британії: офіційний вебсайт. URL: <https://data.gov.uk> .

306. Data.gouv.fr – портал відкритих даних Франції: офіційний вебсайт. URL: <https://www.data.gouv.fr> .

307. Платформи електронних консультацій Канади: офіційний вебсайт. URL: <https://www.canada.ca/en/transparency/consulting-canadians.html> .

308. GovData – портал відкритих даних Німеччини: офіційний вебсайт. URL: <https://www.govdata.de> .

309. Громадянське суспільство і влада: офіційний вебсайт. URL: <https://www.kmu.gov.ua/gromadskosti/gromadyanske-suspilstvo-i-vlada> .

310. Prozorro: офіційний вебсайт. URL: <https://prozorro.gov.ua> .

311. Національний портал відкритих даних: офіційний вебсайт. URL: <https://data.gov.ua>.

312. Detthamrong, U., & Saengchote, K. (2025). Thematic shifts in E-governance research: A bibliometric review. *Government Information Quarterly*, 42(1), 101861. URL: https://www.researchgate.net/publication/394841857_Thematic_Shifts_in_E-governance_Research_From_Foundational_Frameworks_to_Emerging_Technologies.
313. Gil-Garcia, J.R., & Dawes, S.S. (2023). Building Digital Government That Works: Architectural Principles for Sustainable eGovernment Systems. *Public Administration Review*, 83(4), 712-725. URL: <https://doi.org/10.1111/puar.13542>
314. Janowski, T., Estevez, E., & Ojo, A. (2022). Digital Government for Social Stability: A Framework for Institutional Design. *Government Information Quarterly*, 39(3), 101684. URL: <https://greatquestion.com.au/wp-content/uploads/2023/09/Gil-Garcia-et-al-Digital-government-and-public-management-research-finding-the-crossroads-2017.pdf>
315. Vassil, K., & Solvak, M. (2021). E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years. *Journal of Democracy*, 32(2), 135-149. URL: https://skytte.ut.ee/sites/default/files/2023-02/E_voting_in_Estonia_Solvak_Vassil_2016.pdf.
316. Meijer, A., & Webster, C.W.R. (2022). The COVID-19 Crisis and the Informational Governance of Public Health Emergency Response. *Information Polity*, 27(1), 17-29. URL: https://biblio.vub.ac.be/vubirfiles/53929429/COVID19and_information_polity.pdf
317. Аналітичний звіт «Думки і погляди населення України щодо державних електронних послуг у 2023 році». URL: <https://www.undp.org/uk/ukraine/publications/analychnyy-zvit-dumky-i-pohlyady-naselennya-ukrayiny-shchodo-derzhavnykh-elektronnykh-posluh-u-2023-rotsi>.
318. Держспецзв'язку презентує звіт «Війна та кібер: три роки боротьби та уроки для глобальної безпеки». URL:

<https://cip.gov.ua/ua/news/derzhspeczv-yazku-prezentuye-zvit-viina-ta-kiber-tri-roki-borotbi-ta-uroki-dlya-globalnoyi-bezpeki>.

319. Декларація про державний суверенітет України. *Відомості Верховної Ради УРСР*. 1990. № 31. Ст. 429.

320. Акт проголошення незалежності України від 24 серп. 1991 р. *Відом. Верховної Ради України*. 1991. № 38. Ст. 502.

321. Про інформацію: Закон України від 2 жовтня 1992 р. №2657 .URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

322. Концепція формування системи національних електронних інформаційних ресурсів : розпорядження КМУ від 5 травня 2003 року № 259. URL: <https://zakon.rada.gov.ua/laws/show/259-2003-%D1%80#Text>.

323. Про електронні документи та електронний документообіг: Закон України від 23 травня 2003 року № 851. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>.

324. Закон України «Про електронний цифровий підпис» (від 22.05.2003 № 852) – втратив чинність. URL: <https://zakon.rada.gov.ua/laws/show/852-15#Text>.

325. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

326. Українці стали більш задоволеними державними е-послугами – опитування КМІС. URL: <https://www.undp.org/uk/ukraine/press-releases/ukrayintsi-staly-bilsh-zadovolenymy-derzhavnymy-e-posluhamy-opytuvannya-kmis/>

327. e-Government Development Index (EGDI). URL: <https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index>.

328. Digital Economy and Society Index (DESI). URL: <https://digital-strategy.ec.europa.eu/en/policies/desi>.

329. Стандарт ISO 27001. <https://www.iso.org/ru/standard/27001>.

330. LOGFAS (Logistic Functional Area Services). URL: <https://nexuslcm.com/what-is-logfas>.

331. IAC «COTA». URL: <https://gur.gov.ua/content/vvedeno-v-ekspluatatsiiu-informatsiinoanalitichnu-systemu-holovnoho-sytuatsiinoho-tsentru-krainy-sota.html>.

332. Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance - Doing more with less. *Government Information Quarterly*, 30. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0740624X12001517>.

333. Brown, A., Fishenden, J., Thompson, M., & Venters, W. (2017). Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service reform: Towards a Platform Assessment Framework (PAF). *Government Information Quarterly*, 34(2), 167-182. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0740624X17301077>.

334. Holland, J.H. (2006). Studying Complex Adaptive Systems. *Journal of Systems Science and Complexity*, 19(1), 1-8. URL: <https://scispace.com/pdf/studying-complex-adaptive-systems-16lssx11oh.pdf>.

335. von Foerster H. Understanding understanding: essays on cybernetics and cognition. New York: Springer, 2003. 362 p. URL: https://www.researchgate.net/publication/200026369_Understanding_Understanding_Essays_on_Cybernetics_and_Cognition.

336. Goodhart, C. A. E. (1984). *Problems of monetary management: The UK experience*. In C. A. E. Goodhart, *Monetary theory and practice: The UK experience* (pp. 91–121). London: Macmillan. URL: <https://www.semanticscholar.org/paper/Problems-of-Monetary-Management%3A-The-UK-Experience-Goodhart/0ae623749b30de53a39cf05813f5f3842e422c01>.

337. Про засади державної регіональної політики: Закон України від 5 лютого 2015 року № 156. URL: <https://zakon.rada.gov.ua/laws/show/156-19#Text>

338. Про стимулювання розвитку регіонів : Закон України від 8 вересня 2005 року № 2850. (втратив чинність). URL: <https://zakon.rada.gov.ua/laws/show/2850-15#Text>.

339. Maier, M. W. (1998). Architecting principles for systems-of-systems. *Systems Engineering*, 1(4), 267–284. URL: https://www.researchgate.net/publication/282350448_Systems_of_Systems_Engineering.

340. Goldstein, J. (1999). Emergence as a construct: History and issues. *Journal of Consciousness Studies*, 6(6–7), 49–72. URL: <https://www.scirp.org/reference/referencespapers?referenceid=361120>.

341. Відновлення енергосистеми України займе 10–12 тижнів за умови відсутності нових російських атак. URL: <https://apostrophe.ua/economy/jenergetika/vidnovlennja-enerhosistemi-ukrajini-zajme-1012-tizhniv-za-umovi-vidsutnosti-novikh-rosijskikh-atak-kharchenko.html>.

342. Rose, S. et al. (2020). *Zero Trust Architecture* (NIST SP 800-207). National Institute of Standards and Technology. URL: <https://www.scirp.org/reference/referencespapers?referenceid=3702463>.

343. Від агро до IT: ключові напрями економічного відновлення регіонів України. URL: <https://www.undp.org/uk/ukraine/press-releases/vid-ahro-do-it-klyuchovi-napryamy-ekonomichnoho-vidnovlennja-rehioniv-ukrayiny>.

344. Проєкт «Науковий квартал». URL: <https://www.city.kharkiv.ua/uk/news/u-rimi-prezentuvali-proekt-kharkivskogo-naukovogo-kvartalu--57827.html>.

345. У Миколаєві розробляють проєкти відновлення у межах «блакитної економіки». URL: <https://www.ukrinform.ua/rubric-vidbudova/3864590-u-mikolaevi-rozroblaut-proekti-vidnovlenna-u-mezah-blakitnoi-ekonomiki.html>.

346. Американська компанія побудує індустріальний парк Bucha Techno Garden. URL: https://biz.ligazakon.net/news/237620_amerikanska-kompanya-pobudu-ndustrialniy-park-bucha-techno-garden.

347. Релокація підприємств у 2024: понад 11 тисяч компаній змінили адресу реєстрації. URL: <https://unn.ua/news/relokatsiia-pidpriemstv-u-2024-ponad-11-tysiach-kompanii-zminyly-adresu-reiestratsii>.

348. В рамках розмінування сільгоспземель обстежено 200 тисяч га, з них вже використовується аграріями - 120 тисяч. URL: <https://me.gov.ua/News/Detail?lang=uk-UA&id=93712958-6e7d-43f9-87cc-befc54c2fe15&title=VRamkakhRozminuvannia&showMenuTree=true>.

349. IT4Life: проєкт з гуманітарного розмінування. URL: <https://it-kharkiv.com/news/ua/it4life-proyekt-z-gumanitarnogo-rozminuvannya>.

350. Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року: Розпорядження Кабінету Міністрів України № 1025-р від 10 листопада 2023 року. URL: <https://zakon.rada.gov.ua/laws/show/1025-2023-%D1%80#Text>.

351. Як розвивається Стратегія Cloud First в різних країнах світу. URL: <https://denovo.ua/blog/cloud-first-v-mire>.

352. Що таке елементи керування FedRAMP? URL: <https://oath.liberty.cx.ua/ukraincyam/shho-take-elementi-keruvannya-fedramp.html.Ghj>.

353. Про хмарні послуги: Закон України від 17 лютого 2022 р. № 2075. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text>.

354. National Incident Management System. URL: <https://www.fema.gov/emergency-managers/nims>.

355. Setting the standard for open collaboration. URL: <https://www.oasis-open.org>.

356. Integrated Public Alert and Warning System. URL: <https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system>.

357. Web Emergency Operations Center (WebEOC) Interconnectivity. URL: <https://www.dhs.gov/sites/default/files/publications/FEMA%20-%20Web%20Emergency%20Operations%20Center%20%28WebEOC%29%20Interconnectivity.pdf>.

358. National Resilience Strategy. URL: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/National-Resilience-Strategy.pdf>.

359. National Preparedness System. URL: <https://www.fema.gov/emergency-managers/national-preparedness/system>.

360. National Resilience Guidance. URL: <https://www.fema.gov/emergency-managers/national-preparedness/plan/resilience-guidance>.

361. Government Digital Service. URL: <https://www.gov.uk/government/organisations/government-digital-service>.

362. Central Digital and Data Office. URL: <https://www.gov.uk/government/organisations/central-digital-and-data-office>.

363. Digital and Technology Spend Controls. URL: <https://www.gov.uk/government/publications/digital-and-technology-spend-control-version-6/digital-and-technology-spend-control-version-6>.

364. Government Roadmap for Digital and Data 2022–2025. URL: <https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025/transforming-for-a-digital-future-2022-to-2025-roadmap-for-digital-and-data>.

365. GOV.UK One Login. URL: <https://www.sign-in.service.gov.uk>.

366. Government Service Standard. URL: <https://www.gov.uk/service-manual/service-standard>.

367. Government as a Platform, GaaP. URL: <https://interoperable-europe.ec.europa.eu/collection/elise-european-location-interoperability-solutions-e-government/glossary/term/government-platform>.

368. GOV.UK Pay. URL: <https://www.payments.service.gov.uk>.

369. GOV.UK Notify. URL: <https://www.notifications.service.gov.uk>.
370. GOV.UK One Login. URL: <https://www.sign-in.service.gov.uk>.
371. X-Road. URL: <https://e-estonia.com/solutions/interoperability-services/x-road>.
372. KSI (Keyless Signature Infrastructure) Blockchain. URL: https://m.guardtime.com/files/KSI_data_sheet_201509.pdf.
373. Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems. URL: https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf.
374. Comprehensive Security / Kokonaisturvallisuus. URL: <https://turvallisuuskomitea.fi/en/comprehensive-security>.
375. NESA, Huoltovarmuuskeskus. URL: <https://www.huoltovarmuuskeskus.fi/en/organisation/the-national-emergency-supply-agency>.
376. National Emergency Supply Act, 1390/1992. URL: <https://tem.fi/en/security-of-supply-and-securing-of-vital-functions>.
377. Government Decision on the Objectives of Security of Supply 1048/2018. URL: <https://tem.fi/documents/1410877/2095070/Government+Decision+on+the+Objectives+of+Security+of+Supply>.
378. National Emergency Supply Organisation, NESO. URL: <https://varudekeskus.ee/en/neso-national-emergency-strategy-organisation>.
379. National Core Curriculum for Basic Education, 2014. URL: https://www.researchgate.net/publication/312695480_A_New_Finnish_National_Core_Curriculum_for_Basic_Education_2014_and_Technology_as_an_Integrated_Tool_for_Learning.
380. Israel National Cyber Bureau (INCB). URL: https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page.

381. Israel's Cybersecurity Strategy» (INCB/INCD, 2017). URL: https://www.gov.il/BlobFolder/news/cyber_strategy_2025/he/israel_national_cybersecurity_strategy_feb2025.pdf.
382. Cyber Dome. URL: <https://www.cybercom.mil/Media/Images/igphoto/2002914050>.
383. «Crystal Ball». URL: https://finder.startupnationcentral.org/company_page/crystal-ball.
384. Центр протидії дезінформації при РНБО України. URL: <https://cpd.gov.ua>.
385. Індекс сприйняття безпеки. URL: <https://eba.com.ua/indeks-bezpeky-v-ukrayini>.
386. Талеб Н. Антикрихкість. URL: https://nashformat.ua/pdf-preview/antykryhkist.-pro-ne-vrazlyve-u-realnomu-zhytti-nova-obkl.-709425?srsId=AfmBOop2jw3zBd_t0vWIElCGaoMhRmF98vv2qq8bVmD3nPFBiMC50ZZQ.
387. George G. Distributed accountability: designing governance architecture for multi-agent AI ecosystems. URL: https://www.researchgate.net/publication/391015025_DISTRIBUTED_ACCOUNTABILITY_DESIGNING_GOVERNANCE_ARCHITECTURES_FOR_MULTI-AGENT_AI_ECOSYSTEMS.
388. Баштанник О. В. Інституціональна парадигма реалізації державної влади: концептуалізація базових параметрів. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Публічне управління та адміністрування*. 2023. Том 34 (73). № 4. С. 1-6.
389. Баштанник О. В. Спроможність держави як суб'єкта публічного управління в політичній системі України. *Вісник Національного університету цивільного захисту України : зб. наук. пр. Серія "Державне управління"*. 2023. Вип. 2 (19). С. 90-97.
390. Баштанник О. В. Економічна безпека як складова інституційної спроможності та конкурентоспроможності держави. *Публічне управління і*

адміністрування в Україні. 2023. № 37. С. 100-105.

391. Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту Наказ Адміністрації Держспецзв'язку № 54 у січні 2025 року. URL: <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2025-54-pro-zatverdzhennya-bazovikh-zakhodiv-z-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-bazovikh-zakhodiv-z-kiberzakhistu/>

392. Маркетплейс зброї DOT-Chain Defence пройшов оцінювання відповідно до міжнародного сертифікату з кібербезпеки NIST. URL: <https://dotua.org/ua/marketpleis-zbroyi-dot-chain-defence-proisov-ociniuvannia-vidpovidno-do-miznarodnogo-sertifikatu-z-kiberbezpeki-nist.>

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

Монографії

1. Гуманізація публічної служби в Україні: науково-практичні засади. монографія. Дніпро : ДРІДУ НАДУ, 2015. 253 с.
[URL:https://palsg.nmu.org.ua/ua/Sci/Monograph/Гуманізація_публічної_служби.pdf](https://palsg.nmu.org.ua/ua/Sci/Monograph/Гуманізація_публічної_служби.pdf).

Особистий внесок: обґрунтовано напрями застосування інформаційних технологій у навчанні публічних службовців у контексті гуманізації освітнього простору (поширення гіпертекстових і гіпермедіальних систем).

2. **Кравцов О.В.**, Кравцова Т. В. Удосконалення інформаційного забезпечення органів публічної влади на місцевому рівні. Східна політика Європейського Союзу : здобутки, виклики та перспективи / Wschodnia polityka Unii Europejskiej: osiagniecia, wyzwania i perspektywy : **монографія** ; за наук. ред. Я. Турчин, Т. Астрамович-Лейк, О. Горбача. Львів-Olsztyn : РОМУС-ПОЛІГРАФ, 2021. 220 с. (С. 185-198). URL: <https://lpnu.ua/sites/default/files/2021/pages/14947/forum-monografiya-maket.pdf>.

Особистий внесок: розроблено на основі практико-орієнтованих методик сучасного інформаційного забезпечення діяльності органів влади в умовах цифровізації.

3. Маматова Т.В., **Кравцов О.В.** Забезпечення якості публічних послуг в умовах цифрової трансформації (Section 10. Ensuring the administrative services quality in the context of digital transformation). Development vectors in public management and administration: **collective monograph**. Riga, Latvia : Publishing House «Baltija Publishing», 2021. 338 p. P. 208–228. URL: <http://baltijapublishing.lv/omp/index.php/bp/catalog/book/137/>
 DOI: <https://doi.org/10.30525/978-9934-26-082-7-10>.

Особистий внесок: розроблено методологію адаптивної моделі формування критеріїв оцінювання якості публічних послуг, уточнено критерії рамкової цифровізації.

4. Kravtsov O.V. Development of digital competencies of digital competencies in management desigion-making in public administration. *Modernization of Public Authorities in the Digital State Format: Challenges and Prospects under Martial Law and Postwar Reconstruction: scientific monograph*. Riga, Latvia : “Baltija Publishing”, 2025. P. 244-260. URL: <http://baltijapublishing.lv/omp/index.php/bp/catalog/download/611/16417/34706-1?inline=1/>. DOI <https://doi.org/10.30525/978-9934-26-51-6-12>.

статті, опубліковані щонайменше у двох різних періодичних виданнях, включених до категорії «А» Переліку наукових фахових видань України, або у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus

5. Маматова Т., Chykarenko I., Chykarenko O., Kravtsova T., **Kravtsov O.** Information Systems in Project Management of The Public Sphere. IJCSNS International Journal of Computer Science and Network Security. 2021. Vol. 21. № 8. P. 141–148. URL: http://paper.ijcsns.org/07_book/202108/20210819.pdf/ doi: <https://doi.org/10.22937/IJCSNS.2021.21.8.19>. (**Web of Science**).

Особистий внесок: охарактеризовано сучасні підходи до формування інформаційних системи публічного менеджменту в умовах цифрового суспільства, розвинуто поняття управління в цифрову еру.

6. **Kravtsov O.**, Kravtsova T., Lashenko O., Lola V., Rudik N., Holokha L (2023). Strategic Security Imperatives in the Development of Communities in the Post-War Period in Ukraine. Review of Economics and Finance. 2023. Vol. 21, P. 723-730. URL: <https://refpress.org/ref-vol21-a77//>. doi: <https://doi.org/10.55365/1923.x2023.21.77>. (**Scopus**).

Особистий внесок: уточнено сучасні методологічні підходи до цифровізації державного управління в умовах війни та повоєнного відновлення.

7. Verkhovod, I., Haponenko, V., **Kravtsov, O.**, Kravtsova, T., & Bulbeniuk, S. (2024). La influencia de las tecnologías de la información y la comunicación en el desarrollo de las estructuras sociales y políticas de la sociedad red. *Interacción Y Perspectiva*, 14(2), 386-398. [URL: https://dialnet.unirioja.es/servlet/articulo?codigo=9736909](https://dialnet.unirioja.es/servlet/articulo?codigo=9736909). doi: <https://doi.org/10.5281/zenodo.10909782>. (**Web of Science**).

Особистий внесок: запропоновано нові підходи запровадження цифрового інструментарію визначення стану стійкості систем управління, обґрунтовано особливості формування спеціальних інструментів цифрового урядування.

8. Sydorchuk, O., Bashtannyk, V., Terkhanov, F., **Kravtsov, O.**, Akimova, L., & Akimov, O. (2024). Integrating digitization into public administration: Impact on national security and the economy through spatial planning. *Edelweiss Applied Science and Technology*, 8(5), 747–759. URL: <https://learning-gate.com/index.php/2576-8484/article/view/1740>. doi: <https://doi.org/10.55214/25768484.v8i5.1740> (**Scopus**).

Особистий внесок: запропоновано авторські підходи до впровадження диджиталізації публічного управління у межах безпекового концепту національної моделі стійкості.

9. Mamatova T., Chykarenko I., Chykarenko, O., Kravtsova T., **Kravtsov O.** (2022). Innovative digital technologies in the pr-management specialists training for public administration bodies on the blended learning. *Revista Eduweb*. 16(3), 160–176. URL: <https://revistaeduweb.org/check/16-3/12-160-176.pdf> doi: <https://doi.org/10.46502/issn.1856-7576/2022.16.03.12>. (**Web of Science**).

Особистий внесок: розроблено авторську методику запровадження цифрових технологій в системі навчання публічних службовців,

запропоновано удосконалені алгоритми асинхронного навчання в системі вищої освіти.

10. Bashtannyk, O., Bykov, I., **Kravtsov, O.**, Bashtannyk, V., Baikevych, R., & Pushkar, O. (2025). Evolution of economic security institutions: integrating international standards for strategic risk management in global contexts. Sapienza: International Journal of Interdisciplinary Studies, 6(2), e25035, P. 1-11. e-ISSN: 2675-9780. URL:

<https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/e25035>. doi: <https://doi.org/10.51798/sijis.v6i2.1072> (Scopus)

Особистий внесок: розроблено авторську методологію розвитку цифрових технологій для спеціальної підготовки фахівців у сфері публічного управління.

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

11. **Кравцов О.В.** Напрями удосконалення підготовки державних службовців в умовах інформаційного суспільства. *Аналітика і влада : журнал експерт.-аналіт. матеріалів і наук. пр. ПІДУМС НАДУ*. 2013. № 8. С.219-229.

12. **Кравцов О.В.** Краудсорсинг в системі державного управління. *Державне управління та місцеве самоврядування*. 2014. № 4. С. 15-23.

13. **Кравцов О.В.**, Кандзюба С.П., Титаренко О.М. Методика формування простору електронної взаємодії у межах об'єднаної територіальної громади. *Аспекти публічного управління*. 2015. № 5-6. С. 76-84. URL: <https://aspects.org.ua/index.php/journal/article/view/169>. doi: <https://doi.org/10.15421/151551>.

Особистий внесок: розроблено державноуправлінські підходи щодо формування сучасного механізму електронної взаємодії на рівні органів місцевого самоврядування.

14. **Кравцов О.В.** Формування інформаційно-комунікативної компетентності публічних службовців в умовах розвитку електронного урядування: загальні підходи. Публічне адміністрування: теорія та практика. 2016. Вип. 1. (електронне видання). URL: http://nbuv.gov.ua/UJRN/Patp_2016_1_10.

15. **Кравцов О.В.,** Губа М.І., Андросович А.В. Роль цифрових технологій у покращенні доступності та якості публічних послуг в Україні. *Державне управління: удосконалення та розвиток*. 2024. № 9. (електронне видання) URL: <https://www.nayka.com.ua/index.php/dy/article/view/4612/> DOI: <http://doi.org/10.32702/2307-2156.2024.9.13>.

Особистий внесок: розроблено методологію дослідження особливих технологічних засобів та інструментів надання публічних послуг.

16. **Кравцов О.В.** Баштанник В.В. Інституціональні механізми забезпечення участі громади в муніципальному управлінні. *Публічне управління та адміністрування в Україні*. 2023. № 35. С.201-210. URL: <https://pag-journal.iei.od.ua/archives/2023/35-2023/38.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2023.35.38>.

Особистий внесок: узагальнені спеціальні механізми забезпечення участі громади в муніципальному управлінні у форматі цифрового суспільства на основі концепту національної стійкості.

17. **Кравцов О.В.,** Баштанник В.В., Порівняльний аналіз сучасних моделей участі громади в муніципальному управлінні країн ЄС та України у контексті сучасних трендів адміністрування. *Публічне управління та адміністрування в Україні*. 2023. № 37. С.202-214. URL: <https://pag-journal.iei.od.ua/archives/2023/37-2023/37.pdf> doi: <https://doi.org/10.32782/pma2663-5240-2023.37.37>.

Особистий внесок: детерміновані основні виклики для системи національної стійкості, на основі аналізу зарубіжного досвіду та особливостей його впровадження в умовах проведення реформи децентралізації.

18. **Кравцов О.** Кравцова Т.В., Лащенко О.В. Теоретичні основи впровадження антикризового менеджменту в діяльність органів публічного управління. *Аспекти публічного управління*. 2021. № 9. 64-72. URL: <https://aspects.org.ua/index.php/journal/article/view/878/> doi: <https://doi.org/10.15421/152129>.

Особистий внесок: розроблено методологію впровадження антикризового управління в діяльності органів публічного управління для забезпечення національної стійкості із застосуванням системного підходу.

19. **Кравцов О.В.,** Кравцова Т.В., Лащенко О.В. Державна політика в сфері вищої освіти України в умовах цифровізації. *Вісник національного університету цивільного захисту України: серія «Державне управління»*. 2021. Випуск 1(14). С. 73–85. URL: https://www.researchgate.net/publication/352922841_Derzavna_politika_v_sferi_v_isoi_osviti_Ukraini_v_umovah_cifrovizacii. doi: <https://doi.org/10.52363/2414-5866-2021-1-10>.

Особистий внесок: детерміновано особливості формування та реалізації державної політики в сфері вищої освіти України в умовах цифровізації, визначено освітні компоненти процесу формування цифрового суспільства.

20. Кравцова Т.В., Лащенко О.В., **Кравцов О.В.** Використання маркетингового підходу в діяльності органів публічного управління медичною сферою. *Аспекти публічного управління*. 2021. Т. 9. № 4. С. 72–84. URL: <https://aspects.org.ua/index.php/journal/article/view/890>. doi: <https://doi.org/10.15421/152139>.

Особистий внесок: систематизовано сучасні адміністративні підходи щодо використання маркетингового підходу в діяльності органів публічного управління медичною сферою на основі застосування цифрових технологій.

21. **Кравцов О.В.** Роль соціально-ментальних чинників становлення національної ментальної стійкості в умовах цифрового суспільства. *Публічне управління та адміністрування в Україні*. 2023. Випуск 34. С. 212-218. URL:

<https://pag-journal.iei.od.ua/archives/2023/34-2023/39.pdf>.

doi:

<https://doi.org/10.32782/pma2663-5240-2023.34.39>.

22. **Кравцов О.В.** Інституціональний зміст сучасного механізму національної стійкості. *Публічне управління та адміністрування в Україні*. 2023. Випуск 38. С. 293-299. URL: <https://pag-journal.iei.od.ua/archives/2023/38-2023/52.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2023.38.52>.

23. **Кравцов О.В.** Концептуалізація моделі державотворчих процесів в Україні на основі проблемного підходу: феномен цифрової резильєнтності державних структур. *Держава і регіони*. 2023. № 1. URL: http://pa.stateandregions.zp.ua/archive/1_2023/1_2023.pdf. doi: http://pa.stateandregions.zp.ua/archive/1_2023/1_2023.pdf

24. **Кравцов О.В.** Формування особливих механізмів національного розвитку на основі цифровізації в умовах правового режиму воєнного стану. *Публічне управління та місцеве самоврядування*. 2024. Випуск 3. С. 26-33. URL: <https://journals.politehnica.dp.ua/index.php/public/article/view/666>. doi: <https://doi.org/10.32782/2414-4436/2024-3-4>.

25. **Кравцов О.В.** Роль державного управління в розбудові національної моделі стійкості в цифровому суспільстві. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. №4. С. 7-12. URL: <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/631>. doi: <https://doi.org/10.51547/ppp.dp.ua/2024.4.1>.

26. **Кравцов О.В.** Децентралізація і локалізація в контексті формування цифрової моделі стійкості. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. №5. С. 71-78. URL: <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/659>.doi: <https://doi.org/10.51547/ppp.dp.ua/2024>.

27. Прокопчук І., Воронкова А., **Кравцов О.** Дослідження впровадження інноваційних цифрових технологій в державному управлінні. *Успіхи і досягнення у науці*. Серія «управління та адміністрування». 2024. №

10. С. 714-728. URL: <http://perspectives.pp.ua/index.php/sas/article/view/18067>.
doi: [https://doi.org/10.52058/3041-1254-2024-10\(10\)-714-728](https://doi.org/10.52058/3041-1254-2024-10(10)-714-728).

Особистий внесок: проаналізовано динаміку індексу запровадження електронного врядування в діяльності органів влади, досліджено критерії оцінки ефективності впровадження цифрових технологій в управлінському середовищі.

28. **Кравцов О.В.** Упровадження моделі «раціональної інформаційної стабільності» як основи формування національної ментальної системи (НМС) 3.0. *Публічне управління та адміністрування в Україні*. 2024. № 39. С.278-285. URL:<https://pag-journal.iei.od.ua/archives/2024/39-2024/54.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2024.39.52>.

29. Ковальов В., **Кравцов О.** Діджиталізація публічних послуг для внутрішньо переміщених осіб: огляд, виклики, перспективи. *Публічне управління і адміністрування в Україні*. 2025. №46. С. 156-161. URL: <https://pag-journal.iei.od.ua/archives/2025/46-2025/29.pdf>. doi: <https://doi.org/10.32782/pma2663-5240-2025.46.27>.

Особистий внесок: розроблено авторську методологію надання публічних послуг у цифровому форматі, запропоновано авторський підхід до класифікації наявних електронних послуг, а також наведено алгоритми удосконалення механізмів надання послуг внутрішньо переміщеним особам.

30. Філатов В., **Кравцов О.** Публічна діджиталізація та Е-демократія: сучасні інструменти, проблеми і моделі регулювання. *Вчені записки Таврійського національного університету ім. В.Вернадського. Серія «Публічне управління та адміністрування»*. 2024. Т.35 (74). № 6. С.219-225. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2024/6_2024/6_2024.pdf. doi: <https://doi.org/10.32782/TNU-2663-6468/2024.6/37>.

Особистий внесок: обґрунтовано феномен публічної діджиталізації в суспільних відносинах, охарактеризовано механізми публічного управління в контексті феномену Е-демократії.

Праці, які додатково відображають наукові результати дисертації (апробація матеріалів дисертації на наукових конференціях) за науковою спеціальністю 25.00.01 – теорія та історія державного управління

31. **Кравцов О.В.** Удосконалення інформаційного наповнення сайтів ОТГ. *Новітні інформаційно-комунікаційні технології в модернізації публічного управління: зарубіжний і вітчизняний досвід* : матеріали VII наук.-практ. семінару, 25 липня 2019 р., м. Дніпро. Дніпро: ДРІДУ НАДУ. 2019. URL: https://dridu.dp.ua/konf/konf_dridu/Seminar%20ITIC%2007.2019.pdf.

32. **Кравцов О.В.** Актуальні проблеми розвитку штучного інтелекту в Україні. *Сталий розвиток територій: проблеми та шляхи вирішення* : матеріали X міжнар. наук.-практ. конф., м. Дніпро. 25 жовт. 2019 р., Дніпро : ДРІДУ НАДУ. 2019. С. 305–308. URL: http://dridu.dp.ua/konf/konf_dridu/2019_10_25_material_erep.pdf.

33. **Кравцов О.В.** Напрями удосконалення підготовки публічних службовців з питань інформаційної безпеки. *Інноваційний розвиток і підвищення рівня спроможності об'єднаних територіальних громад*: матеріали наук.-практ. конф. за міжнар. участю. м. Дніпро. 30 жовтня – 29 листопада 2019 р. Дніпро: ДРІДУ НАДУ. 2019. С. 354-356. URL: http://www.dridu.dp.ua/konf/konf_dridu/2019_11_29_materialy_mup.pdf.

34. **Кравцов О.В.** Соціальні ефекти інформаційної безпеки. *Проблеми управління соціальним і гуманітарним розвитком*: матеріали XIV наук.-практ. конф. за міжнар. участю. Дніпро : ДРІДУ НАДУ, 2020. С. 166-170. URL: http://dridu.dp.ua/konf/konf_dridu/2020_Material_Social_develop.pdf.

35. **Кравцов О.В, Кравцова Т.В., Маматова Т.В.** Формування цифрових компетентностей публічних службовців. *Науково-практичне забезпечення надання публічних послуг в умовах децентралізації*: матеріали науково-практичної інтернет-конференції за міжнародної участі, м. Київ, 20 квітня 2021 р., Інститут підготовки кадрів Державної служби зайнятості України. Київ: ІПК ДСЗУ, 2021 С. 125–130. URL: https://ipk.edu.ua/wp-content/uploads/2021/09/Konf21_04_2021.pdf.

36. **Кравцов О.В.**, Кравцова Т.В., Лащенко О.В. Цифровізація вищої освіти України в умовах пандемії. *Актуальні проблеми європейської інтеграції та євроатлантичного співробітництва України*: матеріали XVIII регіон. наук.-практ. конф., м. Дніпро. 13 трав. 2021 р. Дніпро : ДРІДУ НАДУ, 2021. С. 117-120. URL:http://www.dridu.dp.ua/konf/konf_dridu/_2021_05_13_pei_material.pdf.

37. Кравцова Т.В., **Кравцов О.В.**, Лащенко О.В. Сутність та зміст державної політики і управління в галузі освіти. *Формування дієвих механізмів державного управління з забезпечення державної безпеки*: круглий стіл за міжнар. участю, м. Харків, 14 трав. 2021 р. Харків: Нац. ун-т цивільного захисту України, 2021. С. 45–47. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12968/3/ZBNMKS_2021.pdf.

38. **Кравцов О.В.**, Кравцова Т.В. Розвиток цифрових навичок: досягнення та перспективи. *Східна політика Європейського Союзу: здобутки, виклики та перспективи / Wschodnia Polityka Unii Europejskiej: osiagniecia, wyzwania i perspektywy*: Materiały VI Polsko-Ukraińskiego Forum Naukowego (27-28 maja 2021, Lwów). Львів-Olsztyn: «ROMUS-POLIGRAF», 2021. 256 s. URL: https://palsg.nmu.org.ua/ua/Sci/Publ_postgrad/Drobakhina-2021.pdf.

39. **Кравцов О.В.**, Кравцова Т.В. Цифровізація медицини – запорука ефективного здоров'язбереження. *Трансформація системи публічного управління створенням здоров'язбережувального та безпечного простору України (модернізація, інновації, розвиток)*: II Міжнародна науково-практична конференція, м. Переяслав, 11 червня 2021 року. Переяслав : Університет Григорія Сковороди, 2021. 245 с. С. 141-148. URL:<https://uhsp.edu.ua/event/ii-mizhnarodna-naukovo-praktychna-konferenciya>.

40. Кравцова Т.В., **Кравцов О.В.**, Кіреєва О.Б. Інформаційне забезпечення органів місцевого самоврядування в сфері надання адміністративних послуг: проблеми та пріоритетні напрями вдосконалення.

Modern scientific research: achievements, innovations and development prospects. Abstracts of the I International scientific and practical conference, July 4-6, 2021, Berlin, Germany. MDPC Publishing. Berlin, Germany. 2021. Pp. 217-223. URL: <https://sci-conf.com.ua/wp-content/uploads/2021/07/MODERN-SCIENTIFIC-RESEARCH-ACHIEVEMENTS-INNOVATIONS...-4-6.07.21.pdf>.

41. Кравцова Т.В., **Кравцов О.В.** Комплекс пріоритетів здоров'язбереження територіальної громади у поствоєнний період. *Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні* : матеріали Всеукр. наук.-практ. конф. м. Київ, ДЗВО «Університет менеджменту освіти» НАПН України, 15-28 квітня 2022 р. Київ : ДЗВО «УМО» НАПН України, 2022. С. 146–150. URL: https://palsg.nmu.org.ua/ua/Sci/konf/Збірник_тез_Том_I.pdf

42. Кравцова Т.В., Лащенко О.В., **Кравцов О.В.** Муніципальний маркетинг як інструмент забезпечення ревіталізації та розвитку територіальних громад. *Міжнародні економічні відносини. Сталий розвиток України в умовах глобалізації та європейської економічної інтеграції: проблеми, перспективи, ефективність.* Фенікс-2022»: матеріали міжнародної науково-практичної конференції, м. Харків, 31 травня 2022 р. Харків. С. 144–146. URL: https://palsg.nmu.org.ua/ua/Sci/konf/Збірник_тез_ФЕНІКС-2022.pdf

43. **Кравцов О.В.** Цифрова трансформація публічного управління в Україні. *Актуальні проблеми європейської та євроатлантичної інтеграції України* : матеріали XIX-ї регіон. наук.-практ. конф. 16 червня 2022 р., Дніпро / за заг. ред. Л.Л. Прокопенка. Д : НТУ ДП, 2022. С. 112–115. URL: https://palsg.nmu.org.ua/ua/Sci/konf/Material_conference_16_06_2022.pdf.

44. **Кравцов О.В.** Цифровізація територіальних громад в Україні. *Digital transformation and technologies for sustainable development all branches of modern education, science and practice.* International Scientific and Practical Conference Proceeding, January 26, 2023. International Academy Applied Sciences in Lomza (Poland) - State Biotechnological University (Ukraine). Publishing house: MANS w Łomży, Lomza, Poland, 2023. Part 2. С. 154-157.

URL:

https://www.researchgate.net/publication/373070515_Digital_transformation_and_technologies_for_sustainable_development_all_branches_of_modern_education_s_cience_and_practice_Electronic_resource_International_Scientific_and_Practical_Conference.

45. **Кравцов О.В.** Дезінформація, маніпуляція та фейки як загрози інформаційної безпеки органів публічного управління в умовах європейської інтеграції. *Національна безпека: загрози та виклики*: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 квітня – 12 травня 2024 року. Львів – Торунь : Liha-Pres, 2024. С. 98-101. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/22907/1/%D0%90dvanced_training_UzhNU.pdf.

Додаток Б

Додаток Б1



ХЕРСОНСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ

пл. Свободи, 1, м. Херсон, 73003, тел. +38 (099) 632 97 36

e-mail: kanc@khoda.gov.ua, www.khoda.gov.ua

Код ЄДРПОУ 00022645

№ _____ На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Кравцова Олега Валентиновича

«Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства»

Матеріали аналітичних довідок та пропозиції щодо удосконалення управлінської діяльності органів влади на території Херсонської області, підготовлені за результатами дисертаційного дослідження Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства» на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління використовуються в діяльності Херсонської обласної державної адміністрації у процесі виконання обласної Цільової програми сприяння розвитку громадянського суспільства на 2022 – 2026 роки, затвердженої рішенням Х сесії Херсонської обласної ради VIII скликання від 07 грудня 2021 року № 399, у тому числі стосовно створення належних умов для впровадження цифрових технологій в діяльності органів виконавчої влади; забезпечення ефективних процедур участі громадянськості в умовах цифровізації у формуванні та реалізації державної регіональної політики, вирішенні напрямів реалізації Національної моделі стійкості для соціально-економічного розвитку області.

Наукові результати дисертаційного дослідження О.В. Кравцова впроваджені у діяльності органів влади Херсонської області у частині визначення адміністративних режимів цифрового врядування. О.В. Кравцов підготував комплекс наукових праць за напрямом формування управлінських моделей стійкості на центральному та регіональному рівні.

Результати дисертаційного дослідження О.В. Кравцова у вигляді авторських пропозицій і рекомендацій щодо функціонування системи публічного адміністрування в умовах правового режиму воєнного стану розглянуті і будуть впроваджені в діяльності органів виконавчої влади Херсонської області.

Заступник голови обласної
державної адміністрації,
кандидат наук з державного
управління, доцент

Володимир КЛЮЦЕВСЬКИЙ



СЕД АСКОД Херсонська ОВА

№ 01-01-58-1101/0/25/05-02 від 28.01.2025

Підписувач Ключевський Володимир Іванович

Сертифікат 3FAA9288358EC0030400000003ABE37001DB8C400

Дійсний з 20.10.2023 0:00:00 по 19.10.2025 23:59:59

Херсонська обласна військова адміністрація
№ 01-01-58-1101/0/25/05-02 від 28.01.2025

Додаток Б2



**ДЕРЖАВНЕ АГЕНТСТВО ВОДНИХ РЕСУРСІВ УКРАЇНИ
(ДЕРЖВОДАГЕНТСТВО)**

вул. Велика Васильківська, 8, м. Київ, 01024, тел./факс: (044) 235-31-92, тел. (044) 235-61-46

E-mail: davr@davr.gov.ua, сайт: davr.gov.ua, код згідно з ЄДРПОУ 37472104

ДОВІДКА

про впровадження результатів дисертаційного дослідження на тему:
**«Теоретико-методологічні засади формування національної моделі
стійкості у форматі цифрового суспільства»**
КРАВЦОВА ОЛЕГА ВАЛЕНТИНОВИЧА

на здобуття наукового ступеня доктора наук з державного управління за
спеціальністю 25.00.01 – теорія та історія державного управління

Матеріали наукових розробок, аналітичних довідок та пропозиції щодо удосконалення управлінської діяльності органів влади в умовах цифровізації, підготовлені за результатами дисертаційного дослідження Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства» на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління використовуються в діяльності Державного агентства водних ресурсів України в частині впровадження цифрових технологій, запровадження алгоритмів е-врядування на рівні суб'єктів державного управління у сфері водних ресурсів, реалізації сучасних управлінських проектів у межах програми діджиталізації публічного управління.

Результати дисертаційного дослідження О.В. Кравцова будуть враховані при розробці відкритих інформаційних платформ даних з управління водними ресурсами та запровадження публічних консультацій, розвитку інноваційних методів управління водними ресурсами шляхом партнерства з науковими установами та приватним сектором.

**Т.в.о. Голови,
доктор технічних наук**



Ігор ГОПЧАК

Державне агентство водних ресурсів України
№ 819/9/13/11-25 від 11.02.2025



Додаток БЗ

ГРОМАДСЬКА НАУКОВА ОРГАНІЗАЦІЯ «ФУНДАЦІЯ ПУБЛІЧНО-ПРАВОВИХ ІНІЦІАТИВ»

код ЄДРПОУ 43232102,
49000, Дніпропетровська обл., місто Дніпро, пл. Соборна, 1-Б, оф. 301,
засоби для зв'язку: +38(063)-774-40-31, email: gno_fppi@ukr.net



від 28.08.2024 № 20-21/28-1

ДОВІДКА

про впровадження результатів Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства»

Матеріали аналітичних довідок та пропозицій щодо формування інституціональних засад реалізації державної влади у сфері свободи слова в Україні, підготовлені за результатами дисертаційного дослідження Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства» на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління використовуються в діяльності в діяльності Громадської організації «ГНО «Фундація публічно-правових ініціатив» у контексті формування нової державної політики, забезпечення функціонування цифрових управлінських платформ, формування інформаційних електронних платформ в умовах цифрового суспільства.

Отримані О.В. Кравцовим наукові результати дисертаційного дослідження враховані у діяльності Громадської організації «ГНО «Фундація публічно-правових ініціатив» у частині розробки науково-практичних пропозицій щодо формування національної моделі стійкості, змін до законодавчих актів, формування наукової основи цифрової трансформації.

Результати дисертації О.В. Кравцова, зокрема, розробленої на основі звернення Громадської організації «ГНО «Фундація публічно-правових ініціатив» «Концепції формування засад національної моделі стійкості в умовах цифрового суспільства» впроваджені у діяльності організації, а також впроваджені в діяльності органів місцевого самоврядування Дніпропетровської області – партнерів ГО ГНО «Фундація публічно-правових ініціатив».

Керівник ГО



Н.О. Бойко

Додаток Б4

АДВОКАТСЬКЕ ОБ'ЄДНАННЯ «ПАНТЕОН.»

код ЄДРПОУ 43582693, 49005, м. Дніпро, пл. Соборна, 1 Б, оф. 301,
+38(096)63-49-330; pantheon-group@ukr.net

28.10.2024 № 112/28-11

ДОВІДКА

про впровадження результатів Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства»

Матеріали аналітичних довідок та пропозицій щодо формування інституціональних засад реалізації державної влади у сфері свободи слова в Україні, підготовлені за результатами дисертаційного дослідження Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства» на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління використовуються в діяльності Адвокатського об'єднання «Пантеон.» у процесі здійснення професійної адвокаційної діяльності щодо дотримання нормативних актів з питань організації управлінської діяльності, у сфері цифрової трансформації. О.В. Кравцовим запропоновано нову методологію раціоналізації діяльності органів влади цифровому форматі, наведено авторські пропозиції щодо формування і функціонування національної моделі стійкості. Варто відзначити здійснений автором теоретичний аналіз концепту резильєнтності у контексті організації правової та методичної допомоги територіальним громадам.

Наукові результати дисертаційного дослідження О.В. Кравцова впроваджені у діяльності Адвокатського об'єднання «Пантеон.», аналітичні матеріали застосовувалися при аналізі конкретних ситуацій, розгляді, заяв і звернень громадян з питань юридичного обслуговування осіб, що стосувалися цифровізації суспільних відносин.

Адвокат АО «Пантеон»



Ф.В. Раїмов

Додаток Б5



**ПЕРЕЩЕПИНСЬКА МІСЬКА РАДА
САМАРІВСЬКОГО РАЙОНУ ДНІПРОПЕТРОВСЬКОЇ
ОБЛАСТІ**

вул. Шевченка, 43, м. Перещепин, Самарівський район, Дніпропетровська область, 51220, тел. 9-14-09, факс (05693) 9-14-09. E-mail: info@pereshepynske.org.dp.gov.ua, web: https://pereshepynske.org.dp.gov.ua код ЄДРПОУ 04338463

28.01.2025 № 215-55 На № _____ від _____

ДОВІДКА

Про впровадження результатів дисертаційного дослідження Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства» на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління

Результати дисертаційного дослідження Кравцова Олега Валентиновича «Теоретико-методологічні засади формування національної моделі стійкості у форматі цифрового суспільства» на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління впроваджуються в діяльності Перещепинської міської ради у межах розробки та впровадження цифрової інтегрованої інформаційно-аналітичної системи «Єдина платформа житлово-комунальних послуг», затвердженої рішенням Перещепинської міської ради від 27.12.2024 р. №10.

Отримані у дисертації О.В. Кравцова наукові результати забезпечують методологічну та організаційно-правову основу для побудови цифрової резильєнтності органів місцевого самоврядування шляхом впровадження архітектури інтегрованого управління на рівні громади, що поєднує єдині реєстри, процесну модель та центри відповідальності; створення наскрізних процесів планування, надання та моніторингу ЖКП на базі цифрової платформи, застосування методики оцінювання цифрової стійкості для регулярного аудиту спроможностей, ризиків та планування безперервності надання послуг.

Результати дисертаційного дослідження О.В. Кравцова у сфері формування національної моделі стійкості важливі у практичній реалізації для органів місцевого самоврядування, підтверджують їх дієвість для підвищення інституційної та цифрової стійкості громади, забезпечують якість публічних послуг і спроможність самоврядних структур до кризового реагування.

В.о. начальника відділу з питань житлово-комунального господарства, комунальної власності, цивільного захисту та благоустрою



Сергій СОЛОГУБ

Додаток В

Проект
Розглянуто і рекомендовано до впровадження ГО ГНО
Фундація публічно-правових ініціатив
(довідка від 10.06.2025 року
№ 10-06/25-4)

Концепція
формування засад національної моделі стійкості в умовах цифрового
суспільства

1. Вступ та актуальність

Сучасний етап розвитку української державності характеризується поєднанням трьох взаємопов'язаних процесів: повномасштабної збройної агресії РФ, глибинних інституційних трансформацій системи публічного управління та прискореного становлення цифрового суспільства. Війна одночасно загострила наявні структурні вразливості української держави й продемонструвала нові можливості для її оновлення, консолідації та розвитку. В цих умовах перед системою органів державної влади постає не лише завдання забезпечення поточної ефективності управління чи надання базових публічних послуг, але й фундаментальніше завдання – збереження самої можливості існування держави як політичного та правового суб'єкта, спроможного до тривалого опору, відновлення та стратегічного розвитку в умовах тривалих криз, гібридних загроз і радикальної глобальної невизначеності. Йдеться не лише про фізичне виживання державних інституцій, а й про збереження й розвиток української політичної нації, національної ідентичності, суверенного контролю над власним інформаційним і цифровим простором.

Досвід воєнного стану, децентралізації, масових внутрішніх і зовнішніх переміщень населення, руйнування критичної інфраструктури, а також форсованої цифрової трансформації (розвиток систем е-врядування, національних платформ на кшталт «Дія», появи галузових цифрових екосистем, застосунків для взаємодії громадян із сектором безпеки й оборони) засвідчує: традиційні моделі організації органів державної влади, побудовані на логіці відносної стабільності, жорсткій ієрархії, лінійному плануванні та процедурно орієнтованому управлінні, виявляються концептуально та інструментально недостатніми. Вони не забезпечують необхідної швидкості, гнучкості й узгодженості рішень у ситуаціях, коли загрози мають комплексний характер, розгортаються одночасно у військовій, інформаційній, економічній, гуманітарній та цифровій площинах і супроводжуються цілеспрямованими спробами противника підірвати довіру до державних інституцій, дискредитувати український політичний суб'єкт,

нав'язати альтернативні, ворожі ідентичнісні та ціннісні наративи.

Поряд із новими можливостями цифрові технології створюють додаткові вразливості – від кіберзагроз до критичних державних систем і реєстрів до складних дезінформаційних кампаній, спрямованих на деморалізацію населення, розкол суспільства, дискредитацію керівництва держави та союзників. Залежність від цифрової інфраструктури стає одночасно умовою модернізації та джерелом уразливості: порушення роботи цифрових сервісів може паралізувати функціонування як окремих органів влади, так і цілих секторів економіки чи безпеки. До цього додаються виклики цифрової нерівності, нерівного доступу до цифрових послуг, відмінностей у цифрових компетентностях між регіонами й соціальними групами. Цифрове суспільство в українських реаліях воєнного часу виявляється полем не лише для інновацій і самоорганізації, а й для масштабних інформаційно-психологічних операцій, маніпуляцій, атак на символічні й ідентичнісні засади української державності.

Особливістю російської збройної агресії проти України є те, що вона має виразно гібридний, цивілізаційний та ідентичнісний характер. Об'єктом атаки виступає не лише територія, економіка чи військовий потенціал, а й сама ідея української нації, її історична пам'ять, мова, культура, право на окремий політичний та цивілізаційний вибір. Концепт «руського мира» й відповідні пропагандистські практики спрямовані на делегітимацію української державності як «штучного утворення», на знецінення української ідентичності, представленій як «варіант» російської. У таких умовах стійкість органів державної влади набуває не лише інституційно-функціонального виміру, а й чітко окресленого ідентичнісного й ціннісного змісту: ідеться про спроможність державних інституцій послідовно й переконливо втілювати, захищати й відтворювати українську ідентичність у правових нормах, управлінських практиках, символічній політиці, комунікації з громадянами та світом.

У цьому контексті важливим є визначення національної моделі стійкості (НМС) як інтегральної рамки переосмислення та модернізації публічного управління, у центрі якої – система органів державної влади як «несуча конструкція» життєздатності держави, її політичної суб'єктності та демократичної легітимності. НМС трактується як багатовимірна, динамічна екосистема, що поєднує онтологічний вимір (розуміння природи стійкості як характеристики державності в умовах невизначеності), функціональний (здатність органів влади виконувати ключові функції безперервно й адаптивно), інституційний (архітектура органів, розподіл повноважень, механізми взаємодії), цифровий (інформаційно-комунікаційні платформи, дані, кібербезпека) та соціально-комунікативний (участь громадян, довіра, національна ідентичність, публічна сфера) виміри. У цифровому просторі ця модель конкретизується через National E-Resilience – національну цифрово орієнтовану концепцію інтегрованого управління, яка переводить принципи НМС у площину конкретних цифрових платформ, стандартів, сервісів та

індикаторів, забезпечуючи водночас захист інформаційного суверенітету й посилення суб'єктності України в глобальному цифровому порядку денному.

Потреба в науковій концепції для НМС в системі органів державної влади зумовлена цілою низкою чинників, які дисертаційне дослідження виокремлює й системно аналізує. По-перше, це необхідність перейти від фрагментарних, реактивних та часто ситуативних рішень (часткові інституційні реформи, поодинокі цифрові проєкти, локальні стратегії безпеки чи відновлення) до цілісної моделі стійкості національної публічної влади, спроможної поєднати безпековий, економічний, соціальний, гуманітарний і цифровий виміри політики. Відсутність єдиної екзистенційної рамки стійкості призводить до того, що окремі ініціативи слабо узгоджені між собою, дублюють або навіть взаємно нейтралізують одна одну, залишаючи критичні прогалини в управлінні ризиками та забезпеченні безперервності функцій держави й базових послуг для громадян.

По-друге, актуальною є потреба інституціоналізувати НМС як окремий, чітко окреслений напрям державної політики та галузі наукових досліджень. На сьогодні в Україні існують численні стратегії та програми – національної безпеки, кібербезпеки, цифрової трансформації, регіонального розвитку, відбудови тощо, – проте вони рідко розглядаються крізь призму єдиної концепції стійкості, що об'єднує різні політики, режими та інструменти. Без такого концептуального об'єднання органи державної влади лишаються в позиції реагування на кризи, а не їх проактивного передбачення, попередження й використання як імпульсів для трансформації. НМС покликана заповнити цю лакуну, запропонувавши цілісну науково обґрунтовану рамку, в межах якої можуть бути скоординовані реформи публічного управління, розвиток безпекового сектору та цифрової трансформації, політика відновлення й модернізації.

По-третє, нагальною є вимога гармонізувати українську систему публічного управління зі стандартами ЄС та НАТО, адаптувавши їх до екстремальних воєнних умов і одночасно зберігши власну ідентичність, ціннісні орієнтири та інституційні особливості. ЄС і НАТО упродовж останнього десятиліття розвинули власні підходи до національної стійкості, захисту критичної інфраструктури, кіберстійкості, протидії гібридним загрозам. Для України, яка веде повномасштабну війну на власній території й одночасно рухається до членства в цих об'єднаннях, постає завдання подвійної адаптації: з одного боку, інтеграції у відповідні європейські та євроатлантичні рамки, а з іншого – трансляції цього досвіду у власну НМС, що має враховувати унікальний досвід країни тривалої тотальної війни, масштабних руйнувань і відбудови, глибокої суспільної мобілізації та відпору авторитарному ревізіонізму. Важливо, що така адаптація не може бути зведена до механічного копіювання окремих інститутів чи технічних стандартів; вона вимагає сформованого національного бачення стійкості як складника модернізаційного проєкту української держави.

По-четверте, в умовах цифрового суспільства, що формується, НМС

повинна безпосередньо враховувати трансформацію самої природи публічного простору, політичної комунікації та громадянської участі. Цифрові платформи стають ключовим середовищем, де формуються й артикулюються національні ідентичності, розгортаються політичні дискусії, мобілізуються ресурси для спротиву чи, навпаки, поширюються паніка й дезінформація. Для України це має подвійний вимір: з одного боку, потужна цифрова мобілізація, волонтерські спільноти, краудфандингові кампанії, інформаційна дипломатія та публічна дипломатія в мережі істотно посилили стійкість держави й суспільства; з іншого – вразливість до зовнішніх інформаційних операцій, залежність від глобальних комерційних платформ, нерівність у доступі до цифрових сервісів створюють додаткові ризики. НМС інтегрує ці аспекти, пропонуючи концепт National E-Resilience як спосіб не лише технічно захистити цифрову інфраструктуру, а й забезпечити суб'єктну присутність української держави в цифровому просторі, її здатність активно формувати цифровий порядок денний, підтримувати комунікаційний зв'язок із громадянами, діаспорою, міжнародними партнерами, водночас протидіючи інформаційній агресії та зберігаючи простір для вільного, плюралістичного розвитку української ідентичності.

По-п'яте, агресія РФ оголила й загострила проблему внутрішньої вразливості національної ідентичності, зокрема на рівні окремих регіонів, мовних і культурних спільнот, соціальних груп. Стійкість у таких умовах означає не консервацію статус-кво, а здатність до інтеграції різноманіття в єдиний політичний та ціннісний проєкт, заснований на повазі до прав людини, демократичних інститутах, визнанні європейського цивілізаційного вибору, але при цьому – на збереженні й розвитку власних культурних кодів, мови, історичної пам'яті. Система органів державної влади в цій логіці постає не лише як адміністратор політик, а й як ключовий інструмент формування інклюзивної, але чітко окресленої української ідентичності – через освітню, культурну, інформаційну політику та політику національної пам'яті, через практики публічної комунікації, через формати співпраці з громадянським суспільством. Відтак НМС повинна включати ідентичнісний вимір як один із базових критеріїв стійкості: держава є стійкою настільки, наскільки вона здатна підтримувати відчуття приналежності своїх громадян до політичної та культурної спільноти навіть у найважчих умовах війни.

Концепція покликана структурувати науково-практичне бачення національної моделі стійкості в системі органів державної влади України в її повноті – як моделі, що одночасно враховує потреби воєнного часу й стратегічні цілі післявоєнного відновлення та розвитку. Вона виходить із того, що питання стійкості не може розглядатися як суто технічне або тактичне завдання окремих органів влади; йдеться про базову характеристику української державності, без якої неможливе ані збереження територіальної цілісності, ані європейська інтеграція, ані відтворення української політичної нації в умовах глобальних викликів цифрової епохи. Саме тому Концепція орієнтована не лише на опис поточного стану речей, а

й на формулювання цільової моделі, до якої має еволюціонувати система органів державної влади, аби забезпечити не тільки виживання, а й гідний, суб'єктний розвиток України в умовах тривалої війни, глобальної конкуренції та невизначеності, де цифрові технології, національна ідентичність і інституційна стійкість дедалі тісніше переплітаються в єдину політико-управлінську реальність.

Базові категорії національної стійкості:

національна стійкість (національна резильєнтність) – інтегральна здатність системи публічного управління забезпечувати підтримання ідентичності держави, функціональну безперервність виконання ключових публічних функцій та здатність до адаптивної трансформації в умовах тривалих потрясінь (воєнних, безпекових, економічних, соціальних, кібернетичних тощо);

суспільна стійкість – здатність суспільства як цілісної соціальної системи (громадян, спільнот, інститутів громадянського суспільства) зберігати базову згуртованість, здатність до самоорганізації, взаємної підтримки та конструктивної взаємодії з державою в умовах криз, а також відновлювати соціальні зв'язки та довіру після потрясінь;

Національна модель стійкості (НМС) – теоретично й методологічно обґрунтована, інституційно та цифрово оформлена система принципів, інструментів, організаційних механізмів та управлінських практик, спрямована на забезпечення стійкого функціонування, адаптації й відновлення держави, суспільства та територіальних громад в умовах тривалих криз і гібридних загроз. НМС виступає інтегрованою рамкою модернізації публічного управління;

екосистема національної стійкості – сукупність акторів (органи державної влади, органи місцевого самоврядування, інститути громадянського суспільства, бізнес, міжнародні партнери), інститутів, цифрових платформ, норм і практик, через взаємодію яких забезпечується формування, підтримка та розвиток національної стійкості в її онтологічному, функціональному, інституційному, цифровому та соціально-комунікативному вимірах;

національна ментальна система – концептуальна модель, що описує сукупність соціально-ментальних факторів, цінностей, установок та інформаційних практик суспільства, від яких залежить рівень ментальної стійкості, сприйняття загроз та здатність до консолідації в умовах криз. У контексті Концепції розглядається як «ментальне підґрунтя» НМС;

Цифровий вимір: суспільство, держава, стійкість

цифрове суспільство – стадія розвитку суспільства, за якої ключові соціальні, економічні, політичні й культурні процеси суттєво опосередковуються цифровими технологіями, інформаційно-комунікаційними мережами й платформами, а доступ до цифрових ресурсів стає одним із базових чинників соціальної включеності та конкурентоспроможності;

цифрова держава – модель організації публічної влади, в якій основні управлінські процеси, надання публічних послуг, взаємодія з громадянами та бізнесом, а також міжвідомча координація системно здійснюються за допомогою цифрових технологій, даних і електронних сервісів на єдиній архітектурній основі;

цифрова стійкість (цифрова резильєнтність) – здатність цифрової інфраструктури, інформаційно-комунікаційних систем, даних та пов'язаних з ними управлінських процесів витримувати вплив кібератак, технічних збоїв, фізичних руйнувань, відключень енергопостачання тощо, зберігати критичні функції та швидко відновлювати працездатність із мінімальними втратами;

цифрова стійкість держави – інтегральна здатність державних цифрових систем, реєстрів, платформ, каналів зв'язку та відповідних інституційно-управлінських механізмів забезпечувати безперервність та безпеку публічного управління й надання базових публічних послуг у цифровому форматі за будь-яких кризових сценаріїв;

цифрова інституційна спроможність публічної влади – здатність органів державної влади та місцевого самоврядування ефективно планувати, розгортати, експлуатувати й оновлювати цифрові системи, інтегрувати їх у щоденну управлінську діяльність, забезпечувати кібербезпеку, управління даними та цифрові компетентності персоналу;

цифрова політика – це цілеспрямована діяльність держави щодо формування нормативно-правових, інституційних, економічних та організаційних умов для розвитку цифрової інфраструктури, сервісів і компетентностей, а також для забезпечення цифрової безпеки, прав людини в цифровому середовищі та цифрової інклюзії;

інституціоналізація цифрової політики у форматі НМС – процес закріплення цілей, принципів та інструментів цифрової політики у правових нормах, організаційних структурах, процедурах і стандартах діяльності органів публічної влади таким чином, щоб цифрові рішення безпосередньо слугували досягненню цілей національної стійкості;

публічна діджиталізація – це системний процес переведення публічного управління, публічних послуг і публічної комунікації в цифровий формат (е-послуги, е-врядування, відкриті дані, е-демократія) із метою підвищення ефективності, прозорості, підзвітності та стійкості публічної влади;

цифрова трансформація публічного управління – глибинна зміна моделей організації, процесів, ролей і компетентностей у системі публічної влади, зумовлена впровадженням цифрових технологій і даних, що веде не лише до автоматизації процедур, а й до переосмислення функцій держави, методів управління, форматів взаємодії з суспільством.

Інтегровані цифрові моделі та інструменти НМС

National E-Resilience – національна цифрово-орієнтована модель інтегрованого управління, спрямована на забезпечення стійкості України шляхом розвитку національної цифрової інфраструктури (платформи,

реєстри, хмарні сервіси), впровадження інструментів штучного інтелекту, аналітики великих даних, блокчейн-технологій та віртуальних платформ підтримки управлінських процесів. Виступає цифровим «ядром» НМС;

Institutional SaaS-платформа (Institutional Software as a Service) – уніфікована, хмароорієнтована платформа е-адміністрування, яка виконує роль «операційної системи» публічного управління, стандартизуючи ключові управлінські процеси (планування, моніторинг, аналіз, управління ризиками, документообіг, звітність, взаємодія з громадянами) та забезпечуючи взаємодію органів влади на основі спільних стандартів даних і сервісів;

Digital E-Resilience Assessment (DEA, методологія оцінки цифрової стійкості) – це методологія комплексного оцінювання цифрової стійкості органів публічної влади, що базується на системі структурних, процесних та результативних індикаторів (стан ІКТ-інфраструктури, організація управління даними, процедури кібербезпеки, готовність до криз, фактична здатність підтримувати роботу цифрових сервісів у кризових умовах). Застосовується для моніторингу, аудитів, бенчмаркінгу, стратегічного планування та оптимізації цифрових політик;

Adaptive Institutional Trajectory Building – методика адаптивного формування цифрових інституційних траєкторій розвитку органів публічної влади. Вона передбачає діагностику поточного рівня цифрової інституційної спроможності, визначення цільового профілю, побудову поетапної траєкторії змін (організаційних, нормативних, кадрових, технологічних) і регулярне її коригування на основі даних (зокрема результатів DEA);

цифрові траєкторії (ЦТ, digital institutional trajectories) – поетапні плани цифрового та інституційного розвитку конкретних органів публічної влади, розроблені за методикою Adaptive Institutional Trajectory Building з урахуванням їхнього мандату, стартового стану, ресурсів і контексту функціонування. ЦТ слугують інструментом цілеспрямованого, а не хаотичного нарощування цифрової спроможності в руслі НМС;

смарт-резильєнтні регіональні стратегії (CPPC / SEES) – інтегровані регіональні стратегії, що поєднують інструменти стратегічного планування, просторового розвитку, цифрового врядування та локальної безпекової політики в єдину рамку забезпечення стійкості територіальних громад і регіонів. Орієнтовані на використання цифрових даних, платформ і аналітики для управління ризиками та планування відновлення;

кластери інституційної стійкості (KIC) – міжвідомчі об'єднання органів влади, організацій та експертних структур, які координують діяльність у визначених напрямках стійкості (наприклад, енергетичної, цифрової, гуманітарної), забезпечуючи узгоджене планування, взаємодію ресурсів і тиражування кращих практик;

крос-секторальна інтеграція (KCI) – узгоджене планування та реалізація політик і заходів стійкості, які одночасно охоплюють декілька секторів (безпека, економіка, цифрова інфраструктура, соціальна сфера тощо), на основі спільних цілей, спільних даних і єдиних цифрових

платформ;

Рамкова модель інтегрованого відкритого врядування (Integrated Open Governance Framework – концептуальна модель, що поєднує принципи відкритості, участі, підзвітності та інтегрованості в єдину архітектуру стійкого врядування. Передбачає використання відкритих даних, цифрових каналів участі громадян, прозорих механізмів ухвалення рішень і міжвідомчої координації в контексті НМС;

національна цифрова платформа (НЦП) – інтегрований комплекс державних цифрових реєстрів, сервісів і модулів управління, що забезпечує єдине середовище обробки даних, надання е-послуг і підтримки управлінських процесів на національному рівні. Виступає базовою інфраструктурою для реалізації NEE та Institutional SaaS;

Інституційний і територіальний виміри НМС

Система публічного управління – сукупність органів державної влади й органів місцевого самоврядування, їхніх повноважень, взаємозв'язків, процесів і механізмів, через які реалізуються публічні інтереси, формуються та виконуються політики, надаються публічні послуги;

Інституційна спроможність – здатність конкретного органу публічної влади ефективно виконувати свої функції й мандат завдяки адекватній організаційній структурі, ресурсам, процедурами, компетентностям персоналу й управлінській культурі. У контексті НМС акцент робиться на спроможності діяти в умовах криз і використовувати цифрові інструменти;

Режими надзвичайного та воєнного адміністрування – особливі режими організації публічної влади, що запроваджуються в умовах надзвичайного чи воєнного стану й передбачають зміну порядку роботи органів влади, перерозподіл повноважень, посилення ролі військових адміністрацій, спеціальні процедури прийняття рішень і обмеження прав, визначені законом;

Регіональні та місцеві центри стійкості – організаційні вузли (на базі обласних/місцевих військових адміністрацій, органів місцевого самоврядування чи спеціалізованих структур), які на територіальному рівні інтегрують функції цивільного захисту, територіальної оборони, управління критичною інфраструктурою, відбудови та цифрового моніторингу, забезпечуючи локальну реалізацію НМС;

Цифровізація територіальних громад – процес упровадження цифрових сервісів, реєстрів, платформ участі, систем управління даними та інфраструктурних рішень на рівні громад з метою підвищення якості послуг, ефективності управління, прозорості й стійкості місцевого розвитку.

Загальні (загальновизнані) поняття в контексті НМС

публічне управління – діяльність органів державної влади та місцевого самоврядування, спрямована на реалізацію публічних інтересів через формування й упровадження політик, регуляторну діяльність, надання публічних послуг та забезпечення прав і свобод людини;

критична інфраструктура (КІ, ДКІ) – об'єкти, системи й сервіси

(енергетика, транспорт, зв'язок, водопостачання, охорона здоров'я, цифрові платформи, фінансова система тощо), порушення функціонування яких може спричинити значні негативні наслідки для національної безпеки, економіки, здоров'я та безпеки населення;

кібербезпека – стан захищеності кіберпростору, інформаційно-комунікаційних систем, мереж, даних і користувачів від кіберзагроз, а також система організаційних, технічних і правових заходів, спрямованих на досягнення такого стану;

кризове управління – сукупність заходів, процедур і рішень, спрямованих на запобігання кризам, підготовку до них, своєчасне виявлення, локалізацію, мінімізацію наслідків і відновлення нормального функціонування системи публічного управління та суспільства;

управління ризиками (risk management) – систематичний процес ідентифікації, аналізу, оцінювання, пріоритезації та моніторингу ризиків із наступною розробкою та реалізацією заходів щодо їх запобігання, зниження, перенесення чи прийняття;

субсидіарність – принцип, за яким управлінські рішення мають ухвалюватися на найнижчому рівні влади, де вони можуть бути ефективно реалізовані; вищі рівні втручаються лише за умови недостатньої спроможності нижчих;

багаторівневе врядування – організація публічної влади, за якої управлінські повноваження розподілені між національним, регіональним, місцевим і наднаціональним рівнями, що взаємодіють між собою;

інформаційно-комунікаційні технології (ІКТ / ICT) – сукупність технічних, програмних та організаційних засобів, які забезпечують збирання, обробку, зберігання, передавання та використання інформації в електронній формі;

штучний інтелект (ШІ / AI) – клас цифрових технологій і систем, здатних виконувати завдання, що зазвичай потребують людського інтелекту (навчання на даних, розпізнавання образів, прогнозування, прийняття рішень), на основі алгоритмів машинного навчання та інших методів;

великі дані (Big Data) – масиви даних великого обсягу, швидкості надходження та різноманітності, обробка яких потребує спеціалізованих методів і технологій і які можуть використовуватися для аналітики, моделювання, прогнозування та підтримки управлінських рішень;

системи підтримки прийняття рішень (DSS) – інформаційні системи, що поєднують дані, аналітичні моделі й інструменти візуалізації для допомоги керівникам у прийнятті обґрунтованих управлінських рішень, зокрема в кризових ситуаціях.

2. Мета та завдання модернізації

Ключовою метою Концепції національної моделі стійкості в системі органів державної влади України є не просто підвищення ефективності

поточного управління, а формування цілісної, інституційно й цифрово вбудованої рамки функціонування публічної влади, здатної забезпечувати життєстійкість держави, суспільства й територіальних громад в умовах тривалої збройної агресії, гібридних загроз та прискореної цифровізації. Йдеться про побудову такої системи органів державної влади, яка у воєнний, перехідний і повоєнний періоди зберігає здатність підтримувати базові функції державності, захищати національну ідентичність, гарантувати права людини й водночас адаптуватися до радикально змінюваного середовища цифрового суспільства. У цьому сенсі національна модель стійкості (НМС) розглядається як інтегральний «каркас» модернізації публічного управління, що поєднує безпековий, інституційний та цифровий виміри й робить систему органів державної влади не лише виконавцем окремих політик, а ядром екосистеми National E-Resilience.

Реалізація цієї мети вимагає розв'язання комплексу взаємопов'язаних завдань, які задають логіку переходу від фрагментарних реформ до цілісної стійкісної моделі публічної влади. Першим, фундаментальним завданням є формування і вдосконалення нормативно-правової основи НМС, що охоплює як «звичайні» режими функціонування держави, так і спеціальні режими – воєнний стан, надзвичайні стани, кризове управління. Йдеться не лише про доповнення чинного законодавства окремими актами про стійкість, а про системну кодифікацію принципів, повноважень і процедур, які визначають, як саме органи державної влади мають діяти в умовах тривалих потрясінь. У цьому контексті ключовим є узгодження українського законодавства зі стандартами ЄС і НАТО в частині захисту критичної інфраструктури, кіберстійкості, інформаційної безпеки, цифрових прав людини, але з обов'язковою адаптацією до реалій повномасштабної війни. Модернізація адміністративних процесів у нормативному вимірі означає впорядкування правових підстав для режимів обмеження прав, делегування повноважень, створення тимчасових кризових інституцій так, щоб вони одночасно забезпечували ефективність управління й не руйнували основ конституційного ладу.

Другим стратегічним завданням є оптимізація інституційної архітектури та управління в системі органів державної влади з погляду стійкості. Централізована, жорстко ієрархічна модель влади в умовах гібридної агресії та цифрового суспільства є недостатньою. Тому Концепція НМС передбачає перехід до адаптивніших форм організації влади: переосмислення ролі центральних органів виконавчої влади як стратегічних «центрів стійкості»; інституціоналізацію ролі обласних військових адміністрацій як ключових акторів у кризових режимах; поглиблення партнерства з органами місцевого самоврядування як «першою лінією» національної стійкості; розвиток мережових міжвідомчих форматів (ситуаційні центри, координаційні штаби) на основі рамки Integrated Open Governance Framework. Оптимізація інституційної структури тут означає не скорочення органів, а впорядкування та узгодження їх функцій, усунення

дублювань, запровадження гнучких механізмів переходу між «мирними» та «мілітарними» архітектурами управління.

Третьою ключовою групою завдань є цифрова трансформація як архітектурний принцип НМС. На основі National E-Resilience Концепція орієнтує систему органів державної влади на побудову єдиної, захищеної, інтероперабельної цифрової інфраструктури управління. Це включає розгортання та розвиток національних цифрових платформ і реєстрів, інституціоналізацію хмароорієнтованої Institutional SaaS-платформи як «операційної системи» е-адміністрування, запровадження аналітичних інструментів на основі великих даних та штучного інтелекту для підтримки прийняття управлінських рішень. Важливим завданням є застосування методології Digital E-Resilience Assessment (DEA) як інструменту регулярного оцінювання цифрової стійкості органів влади: визначення системи індикаторів (структурних, процесних, результативних), побудова «цифрових профілів» інституцій, використання результатів оцінювання для корекції політик, планування інвестицій у цифрову інфраструктуру та компетентності. Органи державної влади мають стати не просто користувачами цифрових систем, а активними архітекторами цифрового контуру НМС, відповідальними за кібербезпеку, захист даних, цифрову інклюзію та інформаційну стійкість суспільства.

Четверте завдання стосується конструювання й підтримки механізмів крос-інституційної та крос-секторальної взаємодії в межах НМС. Адже національна стійкість у цифровому суспільстві не може бути продуктом виключно державних структур; вона базується на взаємодії держави, громадянського суспільства, бізнесу, наукових і освітніх установ, міжнародних партнерів та цифрових платформ. Тому Концепція виходить із потреби інституціоналізувати формати державно-приватного партнерства, публічно-громадського партнерства, участі ІТ-сектору в розвитку критичної цифрової інфраструктури, а також ролі волонтерських і експертних спільнот у виробленні та моніторингу політик стійкості. На рівні органів державної влади це означає створення стабільних платформ взаємодії – як офлайн, так і в цифровому середовищі, – для спільної роботи над сценаріями ризиків, планами безперервності, регіональними смарт-резильєнтними стратегіями (SRPS), формуванням і просуванням наративів національної стійкості.

П'ятим важливим завданням є забезпечення стратегічно вивіреного, прозорого та ефективного використання ресурсів, необхідних для функціонування НМС. Ресурсний вимір у Концепції не зводиться лише до фінансів, але й охоплює людські, інформаційні, організаційні, матеріально-технічні, дипломатичні ресурси. У фінансовому аспекті це означає формування умовного «бюджету стійкості»: інтеграцію критеріїв стійкості в бюджетний процес, виокремлення програм підтримки критичної інфраструктури (у тому числі – цифрової), резервування ресурсів для кризових ситуацій, забезпечення прозорих механізмів контролю й аудиту. З погляду інформаційних ресурсів і знань завданням стає створення систем

знання менеджменту, баз даних про кращі практики реагування на кризи, використання аналітики для стратегічного планування. Розподіл ресурсів має підпорядковуватися логіці ризик-орієнтованого управління: пріоритет надається інвестиціям, що підвищують здатність системи влади протистояти ударам і відновлюватися, а не лише розширюють поточні можливості.

Шосте завдання Концепції пов'язане з розвитком кадрового потенціалу й інституційної спроможності органів державної влади у вимірі НМС. Адже стійкість не може бути досягнута суто нормативними чи технічними засобами – вона укорінюється в компетентностях, цінностях і практиках державних службовців. Отже, потрібно: вибудовувати системи підготовки та перепідготовки кадрів із чіткою стійкісною компонентою (кризове управління, ризик-менеджмент, кібербезпека, робота з даними, публічні комунікації в умовах інформаційної війни); розвивати цифрові компетентності держслужбовців; формувати культуру інституційного навчання (аналіз помилок, посткризова рефлексія, обмін досвідом між інституціями та регіонами). Особливе значення має застосування методики *Adaptive Constitutional / Institutional Trajectory Building* – для поетапного зміцнення цифрової інституційної спроможності конкретних органів влади: визначення їхньої «стартової точки», формування цільових моделей спроможності, побудова індивідуальних траєкторій розвитку з урахуванням ролі в НМС.

Нарешті, сьоме завдання стосується ідентичнісно-ціннісного та комунікативного вимірів НМС, які розглядаються як складова національної стійкості в цифровому суспільстві. Система органів державної влади повинна бути здатною не лише адмініструвати політики, а й підтримувати й відтворювати українську національну ідентичність, ментальну стійкість суспільства, довіру до інституцій у ситуації постійних інформаційних атак. Це означає формування осмисленої державної політики національної пам'яті, інформаційної політики, цифрової дипломатії, системної протидії дезінформації та ворожим наративам, розвиток інструментів електронної демократії та участі громадян у виробленні рішень, що стосуються стійкості. Органи державної влади мають навчитися працювати з цифровими публічними просторами як із полем підтримки й укріплення національної єдності, а не лише як із каналом односторонніх комунікацій.

Сукупне розв'язання цих завдань дозволяє розглядати Концепцію національної моделі стійкості в системі органів державної влади України як стратегічний інструмент переходу від реактивного, фрагментарного управління до проактивної, даноцентричної й ціннісно вмотивованої моделі публічної влади, яка здатна витримувати тривалу збройну агресію, адаптуватися до викликів цифрової епохи й водночас зберігати та розвивати українську державність і національну ідентичність.

3. Основні напрями модернізації державного управління у сфері формування національної моделі стійкості

Формування національної моделі стійкості в системі органів державної влади доцільно розглядати як цілісний, багатовимірний процес трансформації публічного управління, у межах якого організаційно-процесуальні, інституційні, цифрові, ризикологічні та територіальні компоненти взаємно зумовлюють і підсилюють одна одну. У центрі цього процесу перебуває переорієнтація державного управління з інерційно-бюрократичної, нормативно перевантаженої та переважно паперово-процедурної моделі на адаптивну, даноцентричну й цифрово опосередковану систему врядування, спроможну функціонувати в умовах тривалих криз, гібридної збройної агресії та високої динаміки цифрового середовища. Одним із базових напрямів виступає процесна оптимізація та дебюрократизація, що у контексті стійкості набуває не лише організаційного, а й безпеково-інституційного змісту. Йдеться про реінжиніринг ключових адміністративних процесів – ухвалення рішень, міжвідомчої координації, управління ресурсами, звітності, кризових комунікацій – із застосуванням принципів «digital-by-default» і «resilience-by-design». Такі процеси мають проектуватися як первинно цифрові, трасовані, здатні до функціонування в умовах розірваних ланцюгів постачання, часткової втрати інфраструктури, кіберзагроз і перевантаження інформаційних систем. Перехід від процедурно орієнтованого управління до результатно-, ризик- та дано-орієнтованих підходів означає, що регламенти розглядаються не як самодостатні обмеження, а як інструменти забезпечення безперервності критичних функцій і захисту прав, свобод та безпеки громадян; при цьому вони мають бути внутрішньо сумісними з цифровими контурами управління, інтероперабельними з національними інформаційними системами і побудованими так, щоб їхня дія могла бути відтворена в автоматизованих workflow-моделях і rule-based governance. Такий підхід дає змогу не лише скоротити час реагування й знизити транзакційні витрати, а й мінімізувати зони неконтрольованої дискреції, підвищити передбачуваність рішень та їх відтворюваність у різних кризових сценаріях.

Наступним концептуальним напрямом виступає забезпечення інституційної адаптивності й формування координаційних механізмів кризового врядування. Режими надзвичайного та воєнного адміністрування, що дедалі частіше актуалізуються в умовах гібридної агресії, потребують теоретичного осмислення та нормативної стандартизації, оскільки традиційні «мирні» моделі організації публічної влади виявляються недостатньо гнучкими. Інституційна стійкість у цьому контексті означає здатність органів влади керовано переходити між різними режимами функціонування – від звичайного до воєнного чи надзвичайного – без руйнування конституційного ладу й базових гарантій прав людини, але з можливістю оперативної концентрації повноважень і ресурсів там, де це диктується безпековими потребами. Це вимагає чіткого функціонального розмежування й одночасної узгодженості повноважень між центральними органами виконавчої влади,

військовими адміністраціями та органами місцевого самоврядування, нормативного закріплення алгоритмів тимчасового перерозподілу компетенцій, порядку створення кризових штабів, ситуаційних центрів та міжвідомчих координаційних платформ. Важливою складовою є формування процедур легітимних тимчасових відхилень (*derogations*) від звичайних правил, які, з одного боку, створюють простір для оперативності й гнучкості дій, а з іншого – вбудовують запобіжники від зловживань, забезпечуючи зворотність надзвичайних режимів і повернення до стандартних механізмів управління після нормалізації ситуації. У цифровому вимірі інституційна адаптивність передбачає наявність сценаріїв підтримання функцій органів влади в умовах часткової втрати інформаційних систем, пошкодження центрів обробки даних, порушення зв'язку, що вимагає розподілених, резервованих цифрових архітектур і протоколів дій.

Органічним продовженням цих трансформацій є перехід до мережевої та інтегрованої моделі врядування, в основі якої лежить концепція інтегрованого відкритого врядування. У такій моделі органи державної влади перестають бути ізольованими вертикалями та відомчими структурами, і починають функціонувати як вузли складної багаторівневої мережі, в якій циркулюють дані, компетенції, ресурси та політичні мандати. Відкритість і прозорість управлінських процесів досягається за рахунок широкого використання відкритих даних, публічних електронних реєстрів, онлайн-дашбордів, що відображають ключові показники стійкості, а також уніфікованих процедур доступу до інформації й цифрових каналів комунікації з громадянами. Принцип участі реалізується через інституціалізацію механізмів залучення громадянського суспільства, бізнесу, місцевих спільнот та експертних груп до вироблення, реалізації й оцінювання політик у сфері стійкості, зокрема через інструменти електронної демократії, консультаційні платформи, краудсорсингові механізми та корпоративний дизайн управлінських рішень. Підзвітність забезпечується створенням чітких процедур і критеріїв оцінки діяльності органів влади, у тому числі у сфері управління ризиками, кризового реагування та цифрової безпеки, а також розвитком цифрових інструментів аудиту й громадського контролю за діями посадових осіб. Інтегрованість, своєю чергою, виражається в горизонтальній і вертикальній координації між інституціями, секторами та рівнями влади, у побудові інтероперабельних цифрових екосистем, що уможливають безшовний обмін даними й сумісність управлінських процесів. У результаті відбувається перехід від жорстко ієрархічної до екосистемної логіки, у якій стійкість розглядається як результат взаємодії численних суб'єктів, об'єднаних спільними стандартами, цілями та цифровою інфраструктурою.

Ще одним визначальним напрямом є інституціоналізація ризик-орієнтованого та сценарного управління як базового управлінського підходу в межах національної моделі стійкості. У цьому ракурсі управлінські рішення розглядаються не як реакція на вже реалізовані загрози, а як елемент безперервного циклу виявлення, оцінювання, моніторингу та пом'якшення

ризиків у безпековій, економічній, соціальній, інформаційній, кібернетичній та інституційній сферах. Ключовим стає використання методів сценарного моделювання, включно із застосуванням штучного інтелекту, аналізу великих даних, симуляційних систем для прогнозування можливих траєкторій розвитку подій – як у воєнному, так і в повоєнному вимірах – та формування відповідних управлінських стратегій. Національна модель стійкості вимагає побудови систем раннього попередження, що спираються на «сигнальні індикатори» у різних секторах (коливання соціальних настроїв, збої в цифрових системах, аномальні інформаційні потоки, навантаження на інфраструктуру), інтегровані через національні цифрові платформи. Органи державної влади в такій архітектурі перестають бути інструментами реалізації статично визначених повноважень і перетворюються на активних акторів управління ризиками, які володіють необхідними даними, алгоритмами, компетентностями та мандатами для своєчасного коригування політик, процедур і ресурсного розподілу в умовах невизначеності.

Нарешті, національна модель стійкості вимагає чіткого врахування регіонального та муніципального вимірів як простору, де стійкість або вразливість держави набувають конкретної соціальної, економічної та інфраструктурної форми. Територіальні громади, міста, регіони, особливо прикордонні, прифронтові чи постраждалі від бойових дій території, є тими ланками, на яких безпосередньо перевіряється життєздатність державних стратегій. Саме тому доцільно розглядати смарт-резильєнтні регіональні стратегії як інструмент територіалізованого втілення НМС: вони мають інтегрувати стратегічне та просторове планування, політики відбудови, розвиток критичної та цифрової інфраструктури, безпеку громад, соціальну згуртованість і місцеву економічну стійкість.

Органи місцевого самоврядування та військові адміністрації виступають у цій логіці «першою лінією» національної стійкості, відповідальною за забезпечення базових послуг, організацію цивільного захисту, підтримку вразливих груп, адаптацію населення до нових умов. Водночас центральні органи влади мають гарантувати методичну, фінансову, кадрову й цифрову підтримку територій, створюючи механізми координації, передання знань, розбудови локальних спроможностей. Особливої ваги набуває запровадження єдиних підходів до оцінювання стійкості громад і регіонів, розгортання регіональних цифрових платформ управління, створення навчальних програм для місцевих управлінців, спрямованих на формування компетентностей у сфері кризового менеджменту, цифрового врядування й участі громадян.

У сукупності процесна оптимізація, інституційна адаптивність, інтегроване відкрите врядування, ризик-орієнтований підхід і регіонально-муніципальний вимір утворюють взаємопов'язану систему напрямів, через яку національна модель стійкості наповнюється реальним інституційним, процедурним та цифровим змістом, перетворюючись із декларативної конструкції на дієздатну екосистему публічного управління,

здатну витримувати й трансформувати виклики цифрової, воєнної та політичної турбулентності.

4. Нормативно-правове забезпечення

Формування національної моделі стійкості в системі органів державної влади неможливе без цілеспрямованої, послідовної та концептуально вивіреної інституціоналізації цього феномена в правовій системі держави. Йдеться не лише про точкове ухвалення окремих актів, а про побудову цілісної нормативно-правової архітектури, яка фіксує стійкість як одну з базових характеристик сучасної української державності, встановлює чіткі правила гри для всіх суб'єктів публічної влади, визначає межі та процедури застосування спеціальних режимів управління, а також ураховує нові реалії цифрового суспільства та збройної агресії. Без належного правового підґрунтя національна модель стійкості ризикує залишитися суто декларативною конструкцією, не інтегрованою в практику публічного управління, а отже – неспроможною забезпечити реальну життєздатність інституцій у кризових ситуаціях.

Першим ключовим елементом такого нормативно-правового забезпечення є закріплення національної моделі стійкості як самостійного, чітко окресленого об'єкта державної політики. Це передбачає ухвалення рамкового акту – концептуального урядового документа високого рівня (постанови Кабінету Міністрів України), у якому були б визначені базові поняття стійкості, її принципи, цілі, суб'єкти, інструменти та механізми реалізації. Такий акт має встановлювати загальнодержавний підхід до політики стійкості, інтегруючи безпековий, інституційний, соціальний, економічний та цифровий виміри, і водночас слугувати методологічною основою для подальших галузевих і секторальних нормативних актів. Важливо, щоб національна модель стійкості не залишалася ізольованою в межах окремого документа, а була органічно інтегрована в чинні та майбутні стратегії національної безпеки й оборони, цифрової трансформації, регіонального розвитку, відновлення та модернізації країни. Така інтеграція забезпечить узгодженість цілей і засобів різних політик, запобігатиме дублюванню або взаємному нівелюванню ініціатив і, головне, перетворюватиме стійкість на наскрізний принцип державного управління, а не на окремий тематичний блок.

Другим системоутворювальним напрямом є нормативне упорядкування та узгодження спеціальних режимів управління з позицій стійкості. Українська держава функціонує в умовах повномасштабної збройної агресії, що зумовлює регулярне застосування воєнного стану, надзвичайних режимів та інших кризових форматів адміністрування. Наявні норми нерідко створювалися фрагментарно, у відповідь на конкретні виклики, і не завжди враховують довгострокову перспективу, баланс між ефективністю реагування та збереженням демократичних інститутів. Відтак виникає

потреба в детальній нормативній регламентації цих режимів саме крізь призму національної стійкості: має бути чітко визначено порядок і межі обмеження прав і свобод, процедури тимчасового делегування або концентрації повноважень, створення та функціонування тимчасових інституційних конструкцій (кризових штабів, ситуаційних центрів, спеціальних координаційних органів).

Таке врегулювання має забезпечувати, з одного боку, можливість оперативних та рішучих дій у ситуаціях екзистенційної загрози, а з іншого – не допускати розмивання основ правової держави, нормалізації надзвичайних практик і втрати легітимності інституцій. В умовах цифрового суспільства додатково постає завдання нормативного вбудовування в ці спеціальні режими сучасних цифрових інструментів – систем електронного документообігу, реєстрів, платформ кризового моніторингу й інформування населення, а також процедур прозорості та контролю, які дозволяють забезпечити підзвітність владних рішень навіть у надзвичайних обставинах.

Третім невід’ємним чинником нормативної інституціоналізації національної моделі стійкості є гармонізація національного законодавства з європейським та євроатлантичним правом. Враховуючи конституційно закріплений курс України на членство в ЄС і НАТО, формування стійкісної політики не може відбуватися у відриві від відповідних стандартів і підходів цих об’єднань. Йдеться про адаптацію норм і рекомендацій щодо захисту критичної інфраструктури, кібербезпеки, захисту персональних і службових даних, безпеки ланцюгів постачання, безперервності функціонування державних служб. Важливо не лише формально перенести норми європейських директив чи політичних рамок НАТО, а й глибоко осмислити їх у контексті української реальності повномасштабної війни, територіальних втрат, масових переміщень населення та тривалого ресурсного виснаження. Імплементация підходів до національної стійкості, розроблених у рамках ЄС та НАТО, має враховувати, що Україна виступає своєрідним форпостом безпеки на східному фланзі європейського простору, а отже, її досвід і потреби мають бути не лише об’єктом пристосування, а й джерелом збагачення європейського *acquis* у сфері стійкості. Така двостороння гармонізація вимагає постійного моніторингу розвитку відповідних міжнародних стандартів, докладного порівняльно-правового аналізу, виявлення прогалин і суперечностей у національному праві, а також створення дієвих механізмів імплементації, включно з інституційною відповідальністю за впровадження норм на рівні центральних органів виконавчої влади та місцевого самоврядування.

Четвертим, надзвичайно актуальним у цифрову епоху, напрямом є формування нормативної підтримки цифрової стійкості як складника загальної національної моделі стійкості. Цифровий вимір державності – інформаційні системи, електронні реєстри, національні платформи е-урядування, хмарні сервіси, телекомунікаційна інфраструктура – перетворився на повноцінний елемент критичної інфраструктури, від

функціонування якого залежить здатність держави надавати послуги, здійснювати управління, забезпечувати оборону та безпеку. Відповідно, необхідно на нормативному рівні закріпити статус ключових цифрових компонентів як об'єктів критичної цифрової інфраструктури, із визначенням особливих вимог до їхнього захисту, резервування, управління доступом, режимів роботи в умовах надзвичайних ситуацій і воєнного стану. Це стосується як державних реєстрів і платформ, так і хмарних рішень, що використовуються органами влади, у тому числі в рамках публічно-приватних партнерств. Не менш важливим є розроблення та впровадження комплексного правового регулювання у сфері кіберстійкості: встановлення стандартів виявлення, реагування й відновлення після кібератак; правил резервного копіювання й географічного рознесення даних; вимог до розподілених дата-центрів; порядку використання технологій штучного інтелекту в управлінні публічними справами з урахуванням етичних, правозахисних і безпекових аспектів. У цьому контексті цифрова стійкість постає не просто як технічна характеристика ІТ-систем, а як комплексна правова категорія, що поєднує питання інформаційного суверенітету, приватності, захисту персональних даних, прозорості алгоритмів і відповідальності за цифрові управлінські рішення.

Таким чином, лише комплексне вдосконалення нормативно-правової бази за цими взаємопов'язаними напрямками – закріплення стійкості як об'єкта державної політики, узгодження спеціальних режимів управління, гармонізація з європейськими та євроатлантичними стандартами, а також розбудова правових основ цифрової стійкості – здатне створити реальне, а не декларативне підґрунтя для функціонування національної моделі стійкості. Саме така правова архітектура дає змогу перетворити стійкість із політичного гасла на структурну характеристику української держави, забезпечуючи безперервність її функцій, захист прав і свобод, збереження національної ідентичності та спроможність до розвитку в умовах тривалих загроз і турбулентності.

5. Організаційні зміни в системі національної стійкості

Глибока перебудова організаційної архітектури публічної влади є ключовою передумовою реалізації національної моделі стійкості, оскільки саме структура та внутрішня логіка функціонування органів державної влади визначають їх здатність діяти узгоджено, швидко й передбачувано в умовах тривалих криз, війни та радикальної невизначеності. Йдеться не лише про формальне перерозподілення повноважень між інституціями, а про зміну самої моделі організації влади – від інерційної, відомчо-фрагментованої та надмірно ієрархізованої до мережевої, інтегрованої та орієнтованої на стійкість. Організаційні зміни в цій логіці мають вибудовуватися як цілісний процес, що охоплює центральний, регіональний і місцевий рівні, забезпечує інституційну диференціацію функцій та створює стійкі «опорні точки» в

системі публічної влади.

На центральному рівні ключовим вектором організаційних змін є посилення стратегічної ролі Уряду як центру інтегрованого управління стійкістю. Це означає, що Уряд має виконувати не лише координаційно-розпорядчі функції в рамках поточної політики, а й виступати головним архітектором і модератором НМС: формувати загальнодержавне бачення стійкості, узгоджувати пріоритети між секторами, забезпечувати баланс між безпековими, економічними, соціальними та цифровими imperatives. Для цього необхідне створення або перепозиціонування спеціалізованих координаційних структур – міжвідомчих рад, урядових комітетів, ситуаційних та аналітичних центрів – із чітким мандатом щодо формування, реалізації та моніторингу політики стійкості. Такі структури мають працювати на постійній основі, спираючись на дані, сценарний аналіз і системи раннього попередження, а не лише збиратися ad hoc у відповідь на чергову кризу. Важливим напрямом є подолання хронічної відомчої фрагментації, коли кожне міністерство чи відомство розглядає стійкість виключно у власній вузькій сфері відповідальності. Для цього доцільно формувати міжгалузеві «кластери стійкості» – безпековий, енергетичний, цифровий, гуманітарний, економічний тощо, – які об'єднуватимуть відповідні органи влади довкола спільних цілей і спільних індикаторів, забезпечуватимуть горизонтальну координацію політик і спільне планування ресурсів. Такий підхід дозволяє перейти від реактивного погодження позицій між відомствами до проактивного спільного управління ризиками та стійкістю на рівні всієї державної машини.

На регіональному рівні центральну роль у реалізації національної моделі стійкості відіграють обласні військові адміністрації, військові адміністрації інших адміністративно-територіальних одиниць та регіональні органи виконавчої влади. Концепція передбачає формування на рівні областей регіональних центрів стійкості, які інтегрують функції територіальної оборони, цивільного захисту, управління відбудовою, планування розвитку критичної інфраструктури й координації дій із громадами. Такі центри мають стати «нервовими вузлами» НМС на регіональному рівні, де збирається, аналізується й використовується інформація про ризики, ресурси, потреби населення, логістичні й безпекові обмеження. Особливе значення має розгортання в регіонах складників цифрової інфраструктури National E-Resilience: регіональних ситуаційних центрів, аналітичних платформ, єдиних реєстрів ресурсів, систем моніторингу стану інфраструктури, безпеки, соціально-економічних показників. Це дозволяє органам влади на місцях діяти не ізольовано, а як частина єдиного цифрового простору управління, де рішення на регіональному рівні узгоджуються з національними пріоритетами, а інформація рухається в обох напрямках – знизу вгору і зверху вниз. Така організаційна модель підсилює суб'єктність регіонів, роблячи їх не лише виконавцями вказівок «з центру», а й активними акторами формування та

реалізації політики стійкості.

Місцеве самоврядування в рамках національної моделі стійкості розглядається як ключова опора життєздатності держави на рівні громад. Саме органи місцевого самоврядування найближчі до населення, найкраще розуміють локальні потреби, мають прямий контакт із реальними наслідками війни, економічних криз, міграційних процесів. Тому важливим організаційним принципом є визнання їх ключовими суб'єктами стійкості громад – не лише в деклараціях, а й через реальне закріплення ролей, повноважень і ресурсів. Це означає, що громади повинні мати можливість розробляти й реалізовувати власні стратегії стійкості, плани цивільного захисту, програми підтримки вразливих груп, заходи з локальної енергетичної, продовольчої та цифрової безпеки. Водночас така відповідальність неможлива без цілеспрямованої підтримки їхньої інституційної спроможності з боку держави. Концепція передбачає розгортання системних методичних, фінансових і цифрових інструментів підтримки громад: розроблення типових методик оцінки стійкості, надання доступу до державних цифрових платформ, субвенцій на розбудову критичної та цифрової інфраструктури, програм навчання місцевих кадрів у сфері кризового управління, цифрового врядування та участі громадян. У підсумку громади мають перетворитися з об'єктів допомоги на повноцінних партнерів у реалізації НМС, що підвищує гнучкість і стійкість усієї держави.

Завершальним, але не менш важливим напрямом організаційних змін є інституційна диференціація та спеціалізація в системі органів державної влади. Сучасні виклики – від гібридних загроз до складних цифрових трансформацій – вимагають не лише «більше ресурсів» чи «кращої координації», а й наявності в державному апараті спеціалізованих функцій стратегічного передбачення, аналізу даних, управління ризиками й цифрового супроводу рішень. Концепція передбачає виокремлення й інституційне закріплення таких функцій як у центральних, так і в регіональних органах влади: створення підрозділів або окремих структур, відповідальних за аналіз сценаріїв, моделювання наслідків управлінських рішень, розробку планів безперервності діяльності, координацію заходів з кібер- та інформаційної безпеки. Паралельно доцільним є формування стабільних «центрів компетенцій» зі стійкості та цифрового управління – організацій, які акумулюють експертизу, розробляють методики, навчають кадри, супроводжують впровадження нових інструментів у різних секторах і на різних рівнях влади. Такі центри можуть функціонувати як у межах державних органів, так і у форматах державно-громадського чи державно-приватного партнерства, але в усіх випадках вони мають бути інтегровані в загальну архітектуру НМС. Інституційна диференціація в цьому контексті не означає розростання бюрократії; навпаки, вона покликана забезпечити, щоб складні спеціалізовані завдання – робота з великими масивами даних, побудова систем раннього попередження, розробка цифрових стандартів – виконувалися професійно, системно й відповідально, а не за залишковим

принципом «між іншим» у межах традиційних управлінських структур.

Узгоджена реалізація цих взаємопов'язаних організаційних змін – перебудови центрального рівня, посилення регіональної ланки, утвердження місцевого самоврядування як опори стійкості та створення спеціалізованих центрів компетенцій – формує нову організаційну конфігурацію державної влади, здатну підтримувати функціонування національної моделі стійкості не епізодично, а на постійній основі. Саме така конфігурація перетворює НМС із теоретичної конструкції на практичну інфраструктуру виживання, відновлення та розвитку української держави в умовах тривалих викликів.

6. Фінансове забезпечення реалізації Концепції

Реалізація національної моделі стійкості неможлива без цілеспрямованого, системного та довгострокового ресурсного підкріплення. Йдеться не лише про збільшення обсягів фінансування, а насамперед про зміну логіки планування, розподілу й використання ресурсів – від реагування «по факту кризи» до проактивних інвестицій у запобігання, готовність, адаптацію та відновлення. Концепція передбачає формування цілісної системи ресурсного забезпечення НМС, що включає спеціальні бюджетні інструменти, диверсифікацію джерел фінансування, а також жорсткі вимоги до прозорості, підзвітності та антикорупційного контролю.

1. «Бюджет стійкості» як інструмент пріоритезації та планування

Мета: інтегрувати принципи стійкості в бюджетний процес таким чином, щоб державні та місцеві фінанси системно підтримували розвиток і захист критичних спроможностей держави, а не лише покривали поточні видатки чи ліквідовували наслідки криз.

Ключові елементи:

1) **інтеграція критеріїв стійкості у бюджетний процес.** Усі ключові державні й регіональні програми, особливо у сферах безпеки, інфраструктури, цифрової трансформації, соціальної політики, мають оцінюватися не тільки за економічними показниками, а й за внеском у національну стійкість: здатність зменшувати вразливість, посилювати адаптивність, прискорювати відновлення після шоків. Для цього запроваджуються спеціальні критерії та індикатори, які враховуються під час формування та затвердження бюджетів;

2) **формування умовного «бюджету стійкості».** У межах державного та місцевих бюджетів доцільно виокремлювати напрями, безпосередньо пов'язані з НМС: розвиток і захист критичної інфраструктури (енергетичної, транспортної, комунальної, цифрової), створення резервів (матеріальних, фінансових, інформаційних), підтримку систем цивільного захисту, кібербезпеки, кризового управління. Це може набувати форми окремих бюджетних програм, спеціальних фондів або захищених статей видатків;

3) **підтримка критичної цифрової інфраструктури як окремого напрямку.** У рамках «бюджету стійкості» виділяються ресурси на розгортання та супровід національних цифрових платформ, державних

реєстрів, хмарних рішень, систем кіберзахисту й резервування даних, адже їх виведення з ладу внаслідок атак чи аварій може паралізувати роботу держави не меншою мірою, ніж фізичне руйнування об'єктів;

4) програмно-цільовий підхід і багаторічне планування. Фінансування заходів стійкості має здійснюватися не в режимі разових «антикризових вливань», а в контексті багаторічних програм з чіткими цілями, показниками результативності та етапністю реалізації. Це передбачає інтеграцію НМС у середньострокове бюджетне планування та державні цільові програми;

5) закріплення мінімальних фінансових гарантій. Для окремих критично важливих напрямів (резерви, цивільний захист, кібербезпека, підтримка ключових елементів критичної інфраструктури) можуть бути встановлені мінімальні відсоткові частки від ВВП або від загального обсягу бюджету, що гарантуватиме захист цих видатків навіть в умовах жорсткої конкуренції за ресурси.

2. Диверсифікація джерел ресурсів і стратегічна мобілізація фінансування

Мета: забезпечити стійкість фінансування самої НМС шляхом поєднання різних джерел і інструментів – державних, місцевих, міжнародних, приватних – та спрямувати їх використання на довгострокове посилення спроможностей, а не лише на короткострокове «латання дір» під час криз.

Ключові елементи:

1) поєднання державного та місцевих бюджетів. Держава визначає загальну рамку та ключові напрямки фінансування стійкості, тоді як органи місцевого самоврядування й регіональні органи влади забезпечують співфінансування заходів на своїй території (захисні споруди, локальні системи оповіщення, резервні джерела енергопостачання, підготовка добровольчих формувань, локальні ЦНАПи в умовах надзвичайних ситуацій тощо);

2) системне залучення міжнародної допомоги. Міжнародні фінансові організації, донорські уряди, гуманітарні та розвиткові агенції розглядаються не лише як джерело екстреної підтримки під час війни, а як партнери у формуванні довгострокових спроможностей стійкості: відновлення та модернізація критичної й цифрової інфраструктури, посилення інституційної спроможності органів влади, розвиток систем управління ризиками й кризового врегулювання;

3) фокус донорських програм на стійкості, а не лише на гуманітарній підтримці. Донорські ресурси мають цілеспрямовано спрямовуватися на такі напрями, як будівництво або зміцнення захищених об'єктів, резервні та альтернативні інфраструктурні рішення (розподілені енергетичні системи, мобільні зв'язкові комплекси, резервні дата-центри), підготовка персоналу, цифровізація кризового управління. Гуманітарна

допомога лишається важливою, але поступово доповнюється й заміщується інвестиціями в системні спроможності;

4) розвиток державно-приватного партнерства (ДПП) у сферах, пов'язаних із НМС. Для об'єктів і сервісів, де це доцільно (енергетика, логістика, цифрова інфраструктура, соціальні послуги), доцільне використання механізмів ДПП: концесії, спільне будівництво та управління, сервісні контракти. При цьому в кожному проєкті має бути чітко визначена «компонента стійкості» – вимоги до резервування, захисту, безперервності надання послуг, а також справедливий розподіл ризиків між державою та приватним партнером.

5) використання інноваційних фінансових інструментів. Доцільно розглядати можливості цільових облігацій (наприклад, «облігацій стійкості» або «облігацій відновлення»), спеціальних кредитних ліній від міжнародних фінансових інституцій, механізмів змішаного фінансування (blended finance), де грантові кошти поєднуються з кредитами і приватними інвестиціями для зменшення ризиків та збільшення масштабів проєктів стійкості.

3. Прозорість, підзвітність і антикорупційні механізми у використанні ресурсів стійкості

Мета: забезпечити максимальну відкритість інформації про рух і використання ресурсів, призначених для НМС, а також мінімізувати корупційні ризики у сферах відбудови, закупівель, цифрових проєктів і управління критичною інфраструктурою. Без цього ані внутрішня довіра громадян, ані зовнішня довіра донорів і партнерів не можуть бути збережені.

Ключові елементи:

1) відкриті дані про ресурси стійкості. Вся інформація про бюджетні програми стійкості, проєкти відбудови, розвиток критичної та цифрової інфраструктури, залучену міжнародну допомогу (обсяги, джерела, цільове призначення), а також про ключові договори та підрядників має публікуватися у форматі відкритих даних. Це дає можливість незалежного аналізу, журналістських розслідувань, громадського моніторингу;

2) цифрові дашборди та карти проєктів. Створення інтерактивних онлайн-ресурсів, які в зручній формі відображають інформацію про реалізацію проєктів стійкості: об'єкти відбудови, модернізації інфраструктури, створення захисних споруд, розгортання цифрових систем, використання донорських коштів. Такі дашборди мають оновлюватися в режимі, наближеному до реального часу, та бути зрозумілими як фахівцям, так і громадянам;

3) інструменти громадського контролю та участі. Запровадження механізмів подання скарг і повідомлень про зловживання в питаннях використання ресурсів стійкості (онлайн-платформи, гарячі лінії), залучення громадських рад, профільних громадських організацій, експертних спільнот до моніторингу великих проєктів, проведення публічних слухань щодо пріоритетів відбудови та фінансування;

4) посилення прозорості та конкуренції в публічних закупівлях. Усі закупівлі, пов'язані зі стійкістю (будівництво та відновлення об'єктів, створення цифрової інфраструктури, постачання обладнання та матеріалів для резервів), мають здійснюватися через електронні системи публічних закупівель із максимальним рівнем конкуренції, відкритим доступом до тендерної документації та результатів. Для проєктів, що фінансуються з міжнародних джерел, доцільно інтегрувати національні вимоги прозорості з правилами донорів;

5) антикорупційні механізми в сферах відбудови та цифрових проєктів. Потрібен цілеспрямований аналіз корупційних ризиків у проєктах відбудови інфраструктури, реконструкції об'єктів критичної інфраструктури, закупівлі IT-рішень, створення цифрових платформ. За результатами аналізу запроваджуються спеціальні запобіжники: незалежний технічний нагляд, зовнішні аудити, обов'язкова перевірка підрядників, механізми попередження конфлікту інтересів, жорстка відповідальність за нецільове використання коштів;

6) розвиток інституцій фінансового контролю. Важливо посилити спроможність органів внутрішнього аудиту в міністерствах та інших ЦОВВ, а також незалежних контролюючих органів (Рахункова палата, антикорупційні інституції, правоохоронні органи) саме у сфері моніторингу ресурсів стійкості. Це включає спеціалізовані методики аудиту проєктів стійкості, ризик-орієнтований підхід до перевірок, використання цифрових інструментів аналізу транзакцій та контрактів.

Такі взаємопов'язані напрями формують комплексну фінансово-ресурсну основу національної моделі стійкості, дозволяючи поєднати ефективне використання наявних ресурсів із стратегічним залученням нових, забезпечити довіру громадян та партнерів і спрямувати кожен витрачений гривню на реальне посилення здатності держави витримувати, переживати та трансформувати кризи.

7. Управління персоналом: розвиток та мотивація до резильєнтності

Людський капітал є ключовою опорою національної моделі стійкості в системі органів державної влади, а успіх її впровадження безпосередньо залежить від того, наскільки державні службовці та інші посадові особи володіють відповідними компетентностями, мотивацією та здатністю до навчання й адаптації. В умовах повномасштабної війни, гібридних загроз, швидкої цифрової трансформації та високого рівня невизначеності кадровий вимір набуває критичного значення. Це вимагає переходу від формального підходу до підготовки й використання кадрів до стратегічного управління людськими ресурсами в публічному секторі, орієнтованого на стійкість, цифрові спроможності та інституційне навчання.

1. Компетентності стійкості й цифрового управління

Цей напрям фокусується на формуванні у державних службовців та

посадових осіб органів місцевого самоврядування таких знань, умінь і установок, які дозволяють ефективно діяти в кризових умовах, управляти ризиками, працювати з даними та цифровими інструментами, необхідними для функціонування НМС.

Мета – забезпечити, щоб на всіх рівнях влади були кадри, здатні не лише виконувати поточні адміністративні функції, а й мислити сценарно, працювати з невизначеністю, використовувати цифрові платформи для прийняття рішень і взаємодії з громадянами.

Ключові елементи:

- формування компетенцій кризового менеджменту, управління ризиками, безперервності діяльності (business continuity), роботи в умовах стресу й інформаційного перевантаження;
- розвиток навичок роботи з даними (data literacy): розуміння джерел даних, основ аналітики, інтерпретації показників стійкості, використання інформації для прийняття рішень;
- оволодіння цифровими інструментами управління: національними та відомчими цифровими платформами, системами електронного врядування, інструментами моніторингу, ситуаційними дашбордами;
- інтеграція модулів зі стійкості, кризового управління, цифрового врядування в програми підготовки та підвищення кваліфікації державних службовців (як базові, так і спеціалізовані);
- розробка типових профілів компетентностей для посад, критичних з точки зору НМС (керівники органів влади, фахівці з цифрової трансформації, аналітики, фахівці з цивільного захисту, кібербезпеки тощо) та прив'язка до них процедур підбору й оцінювання персоналу.

2. Управління інституційними траєкторіями (*Adaptive Institutional Trajectory Building*).

Цей напрям стосується не лише окремих працівників, а й інституційної спроможності органів влади в цілому. Ідеться про системний, поетапний підхід до зміцнення цифрової та організаційної спроможності органів влади за допомогою спеціальної методики Adaptive Institutional Trajectory Building, яка дозволяє будувати індивідуалізовані траєкторії розвитку кожного органу з урахуванням його стартового стану, ресурсів і ролі в НМС.

Мета – забезпечити, щоб розвиток органів влади в напрямі стійкості й цифровізації не був хаотичним або лише «проектно-грантовим», а здійснювався за усвідомленими, дано-орієнтованими траєкторіями, які поступово підвищують їхню інституційну спроможність.

Ключові елементи:

- використання методики Adaptive Institutional Trajectory Building для діагностики поточного стану цифрової інституційної спроможності (структури процесів, кадрового потенціалу, ІТ-інфраструктури, управлінських практик) в конкретному органі влади;
- розробка індивідуальних цифрових траєкторій розвитку для міністерств, інших ЦОВВ, ОВА/МВА та органів місцевого самоврядування з

урахуванням їхнього мандату в НМС (центральна координація, регіональна безпека, управління даними, критична інфраструктура тощо);

- поетапне планування змін: визначення коротко-, середньо- та довгострокових кроків (кадрових, організаційних, технологічних), необхідних для переходу від поточного до цільового рівня спроможності;

- інтеграція результатів Adaptive Institutional Trajectory Building - оцінювання в управлінські рішення щодо розподілу ресурсів, навчання кадрів, створення нових підрозділів або трансформації існуючих;

- залучення керівників органів влади та ключових фахівців до процесу формування та реалізації інституційних траєкторій, щоб зміни не сприймалися як «нав'язані зверху», а були результатом спільного планування й рефлексії.

3. Культура навчальної й рефлексивної держави

Третій напрям пов'язаний із формуванням такої організаційної культури, у якій державні інституції здатні вчитися зі свого досвіду, аналізувати помилки, ділитися кращими практиками та постійно вдосконалюватися. У контексті НМС це означає перехід від реактивної, формально-бюрократичної логіки до моделі «навчальної держави», яка системно рефлексує над власними діями й адаптується до нових викликів.

Мета – зробити інституційне навчання й рефлексію невід'ємною частиною повсякденної роботи органів влади, щоб кожна криза, інцидент або проєкт давали не лише тактичні уроки, а й стратегічні висновки для посилення стійкості.

Ключові елементи:

- запровадження механізмів постійного інституційного навчання: регулярний аналіз дій після кризових подій (after action review), розбір інцидентів, навчань і тренувань з фіксацією висновків та рекомендацій;

- створення внутрішніх та міжвідомчих майданчиків для обміну кращими практиками у сфері управління стійкістю, цифрового врядування, кризового менеджменту (семінари, спільноти практики, електронні бази знань);

- розвиток системи внутрішнього консалтингу й наставництва, коли органи з більш розвиненими практиками стійкості допомагають іншим інституціям (особливо на регіональному та місцевому рівнях) адаптувати аналогічні рішення;

- заохочення лідерства, орієнтованого на стійкість: керівники мають демонструвати готовність брати відповідальність за довгострокові результати, підтримувати ініціативи персоналу, що спрямовані на посилення спроможностей, а не лише вимагати швидких формальних показників;

- інтеграція рефлексивних механізмів у цикли публічної політики: оцінювання реалізованих програм і проєктів з точки зору їхнього внеску в НМС, коригування стратегій на основі отриманих уроків.

Комплексний підхід до кадрового виміру НМС, що поєднує розвиток компетентностей стійкості й цифрового управління, поетапне інституційне

нарощування спроможності за допомогою методики Adaptive Institutional Trajectory Building та формування культури навчальної й рефлексивної держави, створює основу для того, щоб національна модель стійкості була не лише концептуальною рамкою, а реальною практикою щоденної роботи органів державної влади.

8. Цифровий вимір: National E-Resilience, Institutional SaaS та DEA

Цифровий вимір відіграє ключову, системоутворюючу роль у формуванні національної моделі стійкості, забезпечуючи інструменти для безперервності управління, оперативного прийняття рішень, координації між інституціями та швидкої адаптації до кризових ситуацій. Ідеться не просто про інформатизацію окремих процесів, а про побудову цілісної цифрової екосистеми, в якій дані, платформи, сервіси та методики оцінювання інтегровані в єдине «цифрове ядро» публічної влади. У цьому контексті National E-Resilience виступає цифровою надбудовою національної моделі стійкості, Institutional SaaS – її «операційною системою» е-адміністрування, а методологія Digital E-Resilience Assessment (DEA) – інструментом постійного вимірювання та коригування цифрової стійкості.

Розбудова єдиної цифрової інфраструктури управління в рамках National E-Resilience

Національна цифрова інфраструктура управління розглядається як фундаментальний компонент НМС, що забезпечує узгоджену, надійну та захищену роботу органів влади на всіх рівнях. У межах National E-Resilience пріоритетом є створення та розвиток національних цифрових платформ, реєстрів і хмарних сервісів, які покривають ключові управлінські функції – від документообігу, реєстрації прав та ресурсів до кризового моніторингу, аналітики й комунікації з громадянами. При цьому критично важливо забезпечити надійність, масштабованість, стійкість і резервування цих компонентів, включно з використанням розподілених дата-центрів, національних «govcloud»-рішень, резервних каналів зв'язку. Необхідною умовою ефективності National E-Resilience є уніфікація стандартів даних (формати, довідники, класифікатори), протоколів обміну інформацією, а також вимог до кібербезпеки й захисту інформації. Йдеться про створення єдиного контексту даних, у якому різні органи влади, інформаційні системи та сервіси «говорять однією мовою», що уможливорює безшовну інтероперабельність, комплексний аналіз ситуації та побудову інтегрованих дашбордів для управлінських рішень. Важливим аспектом є також забезпечення географічної та організаційної розподіленості цифрової інфраструктури, що підвищує її живучість у разі фізичних атак, кібератак, перебоїв енергопостачання та інших деструктивних впливів.

9. Впровадження Institutional SaaS як «операційної системи» е-адміністрування

Institutional SaaS (Software as a Service) розглядається як

хмароорієнтована «операційна система» публічного управління, яка надає органам влади стандартизований набір модулів і сервісів для виконання повсякденних управлінських функцій. На відміну від фрагментарного підходу, коли кожен орган створює власні унікальні системи, Institutional SaaS пропонує єдину платформу, на якій розгортаються типові рішення для планування, моніторингу, аналізу, управління ризиками, взаємодії з громадянами, звітності тощо. Це дозволяє суттєво знизити транзакційні витрати (розробка, підтримка, інтеграція), уникнути дублювання функціоналу, забезпечити інтероперабельність між інституціями та рівнями влади. Важливо, що така платформа створюється як хмарний сервіс із високим рівнем захисту, масштабованістю та можливістю швидкого розгортання нових модулів чи оновлень, що особливо важливо в умовах криз і війни. Institutional SaaS має підтримувати гнучкість налаштувань під специфіку різних органів влади, залишаючись при цьому стандартизованою за базовими процесами та структурами даних. Це відкриває можливості для тиражування кращих управлінських і цифрових практик – від центральних органів до регіональних і місцевих, а також для швидкого залучення новостворених або реорганізованих інституцій у єдиний цифровий простір управління. З часом така платформа стає не лише технічним, а й організаційним каркасом для уніфікації процесів, підвищення прозорості, підзвітності та стійкості всієї системи публічної влади.

10. Розвиток методології оцінки цифрової стійкості (Digital E-Resilience Assessment, DEA)

Методологія DEA виступає інструментом системного вимірювання, моніторингу та управління цифровою стійкістю органів публічної влади. Вона базується на наборі індикаторів, що охоплюють структурні аспекти (наявність і стан IT-інфраструктури, резервних потужностей, захищених каналів зв'язку, цифрових платформ), процесні характеристики (якість управління даними, процедур кібербезпеки, регламентів роботи в кризових умовах, рівень інтеграції цифрових сервісів у повсякденну діяльність) та результативні показники (здатність зберігати функціонування під час інцидентів, швидкість відновлення після збоїв, ефективність використання цифрових інструментів у кризовому управлінні). DEA застосовується як для внутрішніх аудитів і самооцінювання окремих органів, так і для зовнішнього моніторингу та бенчмаркінгу між різними інституціями й рівнями влади. На основі результатів оцінювання формуються цифрові «профілі стійкості» органів влади, виявляються критичні вразливості, сильні сторони та пріоритетні напрями розвитку. Це дозволяє використовувати DEA як інструмент стратегічного планування цифрових трансформацій: розробляти поетапні плани підвищення спроможності, обґрунтовано розподіляти ресурси, визначати вимоги до нових проєктів і реформ. Крім того, інтеграція результатів DEA в національні цифрові платформи та Institutional SaaS створює можливості для побудови дашбордів цифрової стійкості в режимі, наближеному до реального часу, що посилює проактивність управлінських

рішень та дозволяє оперативно реагувати на зміни в ризиковому середовищі.

У сукупності National E-Resilience як єдина цифрова інфраструктура, Institutional SaaS як стандартизована «операційна система» е-адміністрування та методологія DEA як інструмент оцінки й управління цифровою стійкістю формують цифрове «ядро» національної моделі стійкості. Без цього ядра неможливо забезпечити справжню безперервність, прозорість та адаптивність сучасної держави в умовах війни, гібридних загроз і швидких технологічних змін.

9. Принципи реалізації Концепції

Реалізація національної моделі стійкості (НМС) у системі органів державної влади здійснюватиметься на основі принципів:

1. Людиноцентричність і правозахисний характер

Цей принцип є засадничим і означає, що стійкість держави не може досягатися за рахунок руйнування або системного обмеження прав і свобод людини. У центрі НМС перебуває захист життя, гідності, базових прав і свобод громадян, навіть в умовах війни, надзвичайних ситуацій та інших кризових обставин. Усі політики, інституційні реформи та оперативні рішення в межах НМС мають проєктуватися та оцінюватися крізь призму їхнього впливу на людину: недопущення свавільних обмежень, збереження доступу до базових послуг, гарантування мінімальних соціальних стандартів і недискримінації. Це вимагає чіткого нормативного регулювання режимів воєнного та надзвичайного стану, прозорих процедур обмеження прав, ефективних механізмів судового та адміністративного захисту, а також реальної підзвітності органів влади за порушення прав людини, вчинені під приводом «забезпечення стійкості».

2. Системність та інтегрованість

НМС розглядається не як набір розрізнених заходів, а як цілісна екосистема, у якій безпекові, цифрові, соціальні, економічні, гуманітарні та інші компоненти перебувають у постійній взаємодії. Принцип системності означає, що будь-які зміни або інвестиції в одному секторі (наприклад, в енергетиці чи цифровій інфраструктурі) мають оцінюватися з точки зору їхнього впливу на інші сектори та на загальну стійкість держави. Інтегрованість передбачає міжвідомчу координацію, спільне планування, використання єдиних підходів до управління ризиками, а також застосування крос-секторальних інструментів – наприклад, спільних цифрових платформ, інтегрованих систем моніторингу й аналізу даних. У практичному вимірі це означає перехід від «відокремленого» управління до моделі, де рішення в галузі безпеки, економіки, цифрової трансформації, соціальної політики та регіонального розвитку узгоджуються з урахуванням цілей НМС.

3. Адаптивність і сценарність

Цей принцип відображає усвідомлення того, що майбутнє України, особливо в умовах повномасштабної війни, гібридних загроз і глобальної

нестабільності, характеризується високим рівнем невизначеності. НМС має будуватися так, щоб інституції, політики, процедури та інфраструктури могли змінюватися й переналаштовуватися залежно від розвитку подій. Адаптивність означає здатність органів влади своєчасно переглядати плани, алгоритми дій, структуру повноважень, ґрунтуючись на результатах моніторингу, нових даних і зміні зовнішнього середовища. Сценарність передбачає використання сценарного аналізу, моделювання можливих кризових ситуацій (ескалація війни, енергетичні шоки, кібератаки, міграційні кризи тощо) і завчасну підготовку набору варіантів реагування. У результаті політика стійкості не постає жорстким планом «раз і назавжди», а функціонує як гнучка рамка з вбудованими механізмами коригування.

4. Відкритість і прозорість

Принцип відкритості та прозорості означає, що реалізація НМС має відбуватися у режимі максимальної публічності, доступності інформації та участі громадян. Широке використання відкритих даних про ризики, інфраструктуру, проєкти відбудови, використання ресурсів стійкості, а також інструментів електронної демократії (е-консультації, е-петиції, платформи для зворотного зв'язку) сприяє підвищенню довіри до рішень влади та зменшує ризики зловживань. Важливим елементом є залучення громадян, громадських організацій, місцевих спільнот і бізнесу до ухвалення рішень у сфері стійкості – від планування укриттів та локальних систем оповіщення до пріоритетів відбудови й розвитку цифрової інфраструктури. Прозорість також передбачає зрозумілу комунікацію ризиків: держава не приховує загроз, а чесно інформує суспільство про можливі сценарії, необхідні обмеження та спільні дії, що формує зрілу культуру безпеки й співвідповідальності.

5. Субсидіарність і багаторівневність

НМС спирається на принцип субсидіарності, згідно з яким рішення мають ухвалюватися на тому рівні влади, де їх можна найбільш ефективно реалізувати, за умови достатньої спроможності цього рівня. Це означає чіткий, юридично та організаційно закріплений розподіл повноважень між центральними органами влади, регіональними структурами (ОВА/МВА, територіальні органи ЦОВВ) і органами місцевого самоврядування. Багаторівневність передбачає, що стійкість будується одночасно «згори вниз» (через національні стратегії, стандарти, ресурси) і «знизу вгору» (через ініціативи громад, місцеві плани безпеки й відновлення). У кризових умовах це дає можливість гнучко перерозподіляти функції та ресурси – наприклад, тимчасово підсилювати місцевий рівень за рахунок державного або навпаки. Важливо, щоб при цьому не виникало дублювання або «провалів» у відповідальності, коли критичні завдання нібито належать усім і водночас нікому конкретно.

6. Наукова обґрунтованість і доказовість

Цей принцип означає, що розробка й реалізація політик стійкості мають базуватися на сучасних наукових підходах, емпіричних даних та

верифікованих методах аналізу, а не лише на інтуїції, політичній доцільності або ситуативних міркуваннях. Використання результатів досліджень у галузі безпеки, державного управління, ризик-менеджменту, цифрового врядування, соціології, економіки, а також даних з державних реєстрів, статистики, цифрових платформ моніторингу дозволяє обґрунтовано визначати пріоритети, оцінювати ефективність заходів і коригувати політику. Важливою складовою є впровадження доказових підходів (evidence-based policy), включно з експериментальними та пілотними проектами, оцінюванням впливу регулювань, використанням цифрових аналітичних інструментів, методик на кшталт DEA (Digital E-Resilience Assessment) тощо. Наукова обґрунтованість також передбачає постійну взаємодію держави з академічною спільнотою, аналітичними центрами, експертами та залучення їх до процесу стратегічного планування.

7. Євроінтеграційна орієнтація

Європейська та євроатлантична інтеграція є стратегічним вибором України, тому НМС орієнтується на стандарти, підходи та практики ЄС і НАТО в сфері національної стійкості, захисту критичної інфраструктури, кібербезпеки, цивільного захисту, управління кризами. Водночас цей принцип не означає механічного копіювання зовнішніх моделей. Йдеться про творчу адаптацію – глибоке вивчення відповідних документів (рамкових концепцій, керівних принципів, стандартів), аналіз умов їхнього застосування в країнах-партнерах та співвіднесення з українськими реаліями повномасштабної війни, масштабних руйнувань і трансформації інституцій. Євроінтеграційна орієнтація передбачає поступову гармонізацію законодавства, управлінських практик, технічних стандартів і процедур із нормами ЄС і НАТО, а також активну участь України в спільних ініціативах, навчаннях і програмах з національної та цифрової стійкості. Таким чином, НМС стає не лише інструментом внутрішньої модернізації, а й важливим кроком до глибшого включення України в європейський та євроатлантичний безпековий простір.

ОЧІКУВАНІ РЕЗУЛЬТАТИ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ

Успішне впровадження національної моделі стійкості (НМС) в системі органів державної влади за даною Концепцією має призвести до досягнення низки суттєвих, вимірних результатів, які змінять характер функціонування української держави в умовах війни, тривалих криз та цифрової трансформації:

1. Забезпечення безперервності виконання ключових функцій держави

Йдеться про здатність держави виконувати свої базові функції – гарантування безпеки, підтримання правопорядку та правосуддя, надання ключових публічних послуг (адміністративних, соціальних, освітніх, медичних), організацію управління кризами – навіть у разі тривалих шоків: воєнних дій, масованих кібератак, енергетичних криз, природних чи

техногенних катастроф. Реалізація НМС забезпечить створення резервних управлінських контурів (альтернативні центри управління, резервні цифрові платформи та канали зв'язку), механізмів планування безперервності діяльності (business continuity planning) для органів влади, а також процедур пріоритизації функцій у надзвичайних умовах. Це дозволить уникнути паралічу державного управління, хаосу та втрати керованості територіями, навіть якщо окремі елементи інфраструктури чи інституції зазнають ударів або тимчасово виходять з ладу.

2. Підвищення інституційної та цифрової спроможності органів влади до дій в умовах комплексних загроз

Результатом упровадження НМС стане суттєве посилення здатності органів державної влади функціонувати в умовах одночасної дії воєнних, кібернетичних, інформаційних, економічних та соціальних загроз. Інституційна спроможність посилюватиметься через чіткіші мандати, оптимізовані організаційні структури, кращу координацію між відомствами, наявність підготовленого персоналу, стандартів кризового управління та навченої управлінської вертикалі. Цифрова спроможність зростатиме завдяки розвитку National E-Resilience (єдиної цифрової інфраструктури управління), впровадженню захищених хмарних сервісів, ситуаційних центрів, систем моніторингу та аналітики, інструментів кіберзахисту й резервування даних. У сукупності це означатиме, що органи влади будуть не лише формально наділені повноваженнями, а й реально забезпечені ресурсами, технологіями та компетентностями для ефективних дій у стресових умовах.

3. Скорочення розриву між стратегіями та реальною практикою управління

НМС передбачає опору на конкретні інструменти, що зменшують типовий для публічного управління розрив між декларативними стратегіями та повсякденною практикою. Серед таких інструментів – методологія оцінки цифрової стійкості (DEA), платформа Institutional SaaS як «операційна система» е-адміністрування, методика Adaptive Institutional Trajectory Building для поетапного інституційного розвитку, а також інші розробки (зокрема, CPPC – системи підтримки рішень у сфері стійкості / кризового планування). Їх використання дозволить переводити стратегічні цілі в чіткі показники, цифрові дашборди, поетапні плани розвитку органів влади, стандартизовані процеси та алгоритми дій у різних сценаріях. У результаті стратегії НМС перестають бути абстрактними документами й стають операційними рамками, які щодня «працюють» у діяльності центральних, регіональних і місцевих інституцій.

4. Зростання довіри громадян до держави

Ефективна реалізація НМС має привести до відчутного посилення довіри громадян до публічної влади, насамперед завдяки прозорості дій, передбачуваності рішень та здатності держави відповідально діяти у кризових ситуаціях. Використання відкритих даних, публічних цифрових дашбордів щодо реалізації проєктів стійкості та відбудови, прозорі механізми

розподілу ресурсів і допомоги, належна комунікація ризиків та рішень, а також реальні приклади ефективного кризового реагування формуватимуть у громадян відчуття, що держава не приховує проблем, чесно говорить про загрози й демонструє спроможність діяти. Додатковим чинником зміцнення довіри стане відчутне покращення взаємодії «держава – громада» на місцевому рівні: залучення громадян до планування стійкості, публічні консультації, підтримка місцевих ініціатив, швидкий і прозорий зворотний зв'язок у кризових ситуаціях.

5. Інтеграція України в європейську систему стійкості й безпеки

Упровадження НМС відповідно до європейських та євроатлантичних підходів до національної та цифрової стійкості сприятиме посиленню залучення України до спільних механізмів безпеки, кризового управління та відбудови. Це означатиме гармонізацію національних стандартів захисту критичної інфраструктури, кібербезпеки, цивільного захисту, планування безперервності, а також інституційних рамок з відповідними підходами ЄС та НАТО. На практиці це відкриє можливості для участі в спільних ініціативах, програмах підтримки стійкості, регіональних платформах обміну даними й досвідом, спільних навчаннях та тренуваннях, механізмах взаємодопомоги у випадку великих криз. Україна перестане бути лише «одержувачем допомоги» і поступово стає повноцінним учасником європейської системи стійкості, який вносить власний унікальний досвід протидії гібридній агресії та тривалій війні.

6. Перетворення держави на динамічну, навчальну та самовідновну систему

Найбільш глибоким результатом упровадження НМС має стати трансформація української держави з переважно реактивної, бюрократичної системи на динамічну, навчальну й самовідновну інституційну екосистему. Це означає формування культури, у якій кризи розглядаються не лише як загрози, а й як джерела уроків і імпульси для розвитку; де існують сталі механізми інституційного навчання (аналіз досвіду, *post-action review*, обмін кращими практиками), постійне оновлення політик і процедур на основі даних, а також гнучкі інструменти зміни організаційних структур, цифрових рішень і кадрових стратегій. Така держава здатна не просто «виживати» в умовах тривалої війни, глобальної конкуренції та швидких технологічних змін, а й використовувати ці виклики для модернізації, підвищення ефективності, розширення прав і можливостей громадян та посилення свого суб'єктного становища у світі.

У такій інтерпретації національна модель стійкості в системі органів державної влади постає не як разова програма чи тимчасовий «антикризовий» пакет, а як довгострокова інституційно-цифрова рамка існування й розвитку української держави в цифрову епоху. Вона задає новий стандарт того, як держава планує, організовує та здійснює своє функціонування в умовах постійних ризиків і невизначеності, перетворюючи стійкість на невід'ємну характеристику сучасного українського

державотворення.

Додаток Д1

АНКЕТА ЕКСПЕРТНОГО ОПИТУВАННЯ «НАЦІОНАЛЬНА МОДЕЛЬ СТІЙКОСТІ В УМОВАХ ЦИФРОВОГО СУСПІЛЬСТВА»

Опитування проводиться ГО ГНО «Фундація публічно-правових ініціатив у межах наукового дослідження, присвяченого теоретико-методологічним засадам формування національної моделі стійкості (НМС) України у форматі цифрового суспільства.

Респондентами є експерти у сфері публічного управління, державні службовці, представники обласних та місцевих військових адміністрацій, органів місцевого самоврядування, фахівці з цифрової трансформації, представники громадянського суспільства, науковці та ін.

Мета опитування: виявити експертні оцінки стану та перспектив формування НМС в Україні, зокрема цифрової стійкості публічної влади, інституційної спроможності органів влади, ролі децентралізації та воєнного стану, а також можливостей адаптації досвіду ЄС і НАТО у сфері національної стійкості.

Інструкція:

Просимо Вас відповісти на запитання, обравши один або кілька варіантів відповідей (як це зазначено біля кожного запитання). У разі вибору варіанту «Інше» – коротко конкретизуйте свою думку. Ваші відповіді є конфіденційними та будуть використані лише в узагальненому вигляді. Орієнтовний час заповнення анкети: 15–25 хвилин.

I. ЗАГАЛЬНА ОЦІНКА СТАНУ НАЦІОНАЛЬНОЇ СТІЙКОСТІ

1. Як Ви в цілому оцінюєте поточний рівень національної стійкості України в умовах повномасштабної війни та цифровізації? (Один варіант відповіді).

1.1. Високий рівень: система загалом стійка, спроможна витримувати тривалі шоки.

1.2. Помірно достатній рівень: ключові функції зберігаються, але із суттєвими напруженнями.

1.3. Обмежений рівень: стійкість забезпечена лише в окремих секторах (оборона, окремі цифрові сервіси тощо).

1.4. Низький рівень: система переважно реактивна та вразлива до комплексних загроз.

1.5. Інше (вказіть): _____.

2. Наскільки, на Вашу думку, у практиці публічного управління фактично реалізується ідея національної моделі стійкості (НМС) як інтегрованої рамки модернізації держави? (Один варіант відповіді).

2.1. Значною мірою реалізується (є цілісна політика, узгоджені інструменти та інституції).

2.2. Частково реалізується (наявні окремі елементи, але відсутня цілісна рамка).

2.3. Реалізується фрагментарно, переважно в секторі безпеки та оборони.

2.4. Переважно декларативна: стійкість фігурує в стратегіях, але мало впливає на реальну практику.

2.5. Інше (вказіть): _____.

3. Які з вимірів НМС, на Вашу думку, є найбільш розвиненими в Україні сьогодні? (Можна обрати кілька варіантів).

3.1. Онтологічний (забезпечення самого існування держави як політичного суб'єкта).

3.2. Функціональний (безперервність виконання ключових публічних функцій і

базових послуг).

3.3. Інституційний (адаптивність, узгодженість, навчальна здатність органів публічної влади).

3.4. Цифровий (захищеність, гнучкість, інтероперабельність цифрової інфраструктури).

3.5. Соціально-комунікативний (довіра, участь, згуртованість, інформаційна стійкість суспільства).

3.6. Важко відповісти.

4. Як Ви оцінюєте здатність системи публічного управління забезпечувати безперервність виконання ключових функцій держави в умовах тривалих криз? (Один варіант відповіді).

4.1. Висока: є дієві механізми резервування, дублювання та кризового управління.

4.2. Середня: безперервність забезпечується, але зі значними перебоями й імпровізацією.

4.3. Низька: при серйозних кризах ключові функції часто перериваються або різко погіршуються.

4.4. Різняться залежно від рівня влади / сектора.

4.5. Інше (вказіть): _____.

II. ЦИФРОВИЙ ВИМІР НМС ТА ІНСТИТУЦІЙНА СПРОМОЖНІСТЬ

5. Як Ви оцінюєте рівень цифрової стійкості державних органів (здатність цифрових систем працювати та відновлюватися під час атак, збоїв, руйнувань інфраструктури)? (Один варіант відповіді).

5.1. Високий: є резервні центри, відпрацьовані процедури, регулярні аудити й навчання.

5.2. Середній: є окремі сильні елементи, але відсутня повна системність.

5.3. Низький: захищеність і готовність до інцидентів є недостатніми.

5.4. Цифрова стійкість суттєво різниться між окремими органами / секторами.

5.5. Важко відповісти.

6. Наскільки розвинуеною, на Вашу думку, є в Україні ідея National E-Resilience – єдиної національної цифрово-орієнтованої моделі інтегрованого управління стійкістю? (Один варіант відповіді).

6.1. Фактично реалізується: існує інтегрована цифрова інфраструктура й узгоджені рішення.

6.2. Перебуває на стадії активного формування.

6.3. Представлена окремими несинхронізованими ініціативами.

6.4. Наразі майже відсутня як цілісна концепція.

6.5. Інше (вказіть): _____.

7. Чи відомі Вам практики використання методології оцінки цифрової стійкості (Digital E-Resilience Assessment, DEA) або її аналогів в українських органах влади? (Один варіант відповіді).

7.1. Так, відомі й застосовуються системно.

7.2. Так, відомі, але застосовуються епізодично / у пілотному режимі.

7.3. Чув(ла) про подібні підходи, але не знаю про реальне застосування в Україні.

7.4. Не відомі / не застосовуються.

7.5. Інше (вказіть): _____.

8. Як Ви оцінюєте доцільність впровадження єдиної Institutional SaaS-платформи («операційної системи» е-адміністрування) для органів публічної влади? (Один варіант відповіді).

- 8.1. Вкрай доцільно: це ключова умова цифрової стійкості та уніфікації процесів.
- 8.2. Доцільно, але з урахуванням галузевої специфіки.
- 8.3. Частково доцільно: варто залишити більше автономії окремим органам
- 8.4. Недоцільно: централізована платформа створює надмірні ризики й залежності.
- 8.5. Інше (вказіть): _____.

9. З якими бар'єрами цифрової стійкості найчастіше стикаються українські органи влади? (Можна обрати кілька варіантів).

- 9.1. Фрагментація ІКТ-систем і відсутність єдиної архітектури.
- 9.2. Недостатній рівень кібербезпеки та захисту даних.
- 9.3. Відсутність резервних центрів обробки даних / планів безперервності діяльності.
- 9.4. Низький рівень цифрових компетентностей персоналу.
- 9.5. Обмежене фінансування цифрової інфраструктури та її захисту.
- 9.6. Цифрова нерівність і залежність від вразливої фізичної інфраструктури (енергетика, зв'язок).
- 9.7. Інше (вказіть): _____.

10. Наскільки, на Вашу думку, реалістичним є застосування методики Adaptive Institutional Trajectory Building або подібних підходів для поетапного розвитку інституційної спроможності органів влади? (Один варіант відповіді).

- 10.1. Реалістично й необхідно: без поетапних «цифрових траєкторій» розвиток буде хаотичним.
- 10.2. Реалістично, але потребує суттєвої адаптації до українських умов.
- 10.3. Скоріше утопічно: інституції не готові працювати з такими інструментами.
- 10.4. Важко відповісти / недостатньо інформації.
- 10.5. Інше (вказіть): _____.

III. ТЕРИТОРІАЛЬНИЙ ВИМІР НМС: ДЕЦЕНТРАЛІЗАЦІЯ, ВІЙНА, ГРОМАДИ

11. Як Ви оцінюєте вплив реформи децентралізації на стійкість територіальних громад та регіонів? (Один варіант відповіді).

- 11.1. Переважно позитивний: децентралізація підвищила здатність громад до самостійних дій у кризах.
- 11.2. Позитивний для спроможних громад, але обмежений для слабких / депресивних територій.
- 11.3. Переважно нейтральний: стійкість визначається іншими факторами (війна, ресурси, керівництво).
- 11.4. Переважно негативний: посилилася нерівність у стійкості між громадами.
- 11.5. Інше (вказіть): _____.

12. Яку роль, на Вашу думку, відіграють обласні та місцеві військові адміністрації (ОВА, МВА) у формуванні регіональної та місцевої стійкості? (Один варіант відповіді).

- 12.1. Ключову: вони є фактичними регіональними / місцевими центрами стійкості.
- 12.2. Важливу, але розділену з органами місцевого самоврядування.
- 12.3. Обмежену: їхній вплив визначається, головню, сектором безпеки й оборони.
- 12.4. Низьку: відсутня чітка роль у системі стійкості.
- 12.5. Інше (вказіть): _____.

13. Які механізми зміцнення стійкості на територіальному рівні Ви вважаєте найбільш ефективними? (Можна обрати кілька варіантів).

- 13.1. Смарт-резильєнтні регіональні стратегії (CPPC / SEES).
- 13.2. Розвиток місцевих центрів стійкості / ситуаційних центрів при ОВА та

громадах.

13.3. Міжмуніципальне співробітництво (спільні послуги, спільна IT-інфраструктура тощо).

13.4. Розвиток цифрових рішень на рівні громад (е-сервіси, цифрові карти ризиків, платформи участі).

13.5. Створення кластерів інституційної стійкості (КІС) на регіональному рівні.

13.6. Інше (вказіть): _____.

14. Які фактори найбільше обмежують стійкість територіальних громад в умовах війни? (Можна обрати кілька варіантів).

14.1. Руйнування критичної інфраструктури (енергетичної, транспортної, цифрової).

14.2. Недостатнє фінансування й нерівномірний розподіл ресурсів.

14.3. Кадровий дефіцит (особливо в малих та прифронтових громадах).

14.4. Низька цифрова спроможність громад (відсутність фахівців, ІКТ-інфраструктури).

14.5. Недостатня координація між державними органами та місцевим самоврядуванням.

14.6. Низький рівень довіри та взаємодії з громадянами.

14.7. Інше (вказіть): _____.

IV. ЄВРОПЕЙСЬКИЙ ТА ЄВРОАТЛАНТИЧНИЙ ДОСВІД

15. Досвід яких інституцій або країн Ви вважаєте найбільш релевантним для побудови НМС в Україні? (Можна обрати кілька варіантів).

15.1. Європейського Союзу (загальні рамки національної та цифрової стійкості).

15.2. НАТО (концепції національної та суспільної резильєнтності, захисту критичної інфраструктури).

15.3. Естонії (модель цифрової держави та кіберстійкості).

15.4. Скандинавських країн (поєднання соціальної держави, безпеки й цифровізації).

15.5. Польщі та країн Центрально-Східної Європи (досвід трансформації в умовах зовнішніх загроз).

15.6. Інше (вказіть): _____.

16. Які елементи європейського та євроатлантичного досвіду стійкості, на Вашу думку, найпростіше адаптувати в Україні? (Можна обрати кілька варіантів).

16.1. Стандарти захисту критичної інфраструктури (у т.ч. цифрової).

16.2. Підходи до кібербезпеки та кіберстійкості державних систем.

16.3. Моделі багаторівневого врядування та субсидіарності в кризах.

16.4. Системи раннього попередження та кризового моніторингу.

16.5. Інструменти участі громадян і відкритого врядування у сфері стійкості.

16.6. Інше (вказіть): _____.

17. Які основні перешкоди, на Вашу думку, заважають імплементації європейських стандартів національної та цифрової стійкості в Україні? Можна обрати кілька варіантів).

17.1. Недосконалість і фрагментарність законодавчої бази.

17.2. Інституційний опір змінам та інерція управлінської культури.

17.3. Обмежені фінансові ресурси й конкуренція пріоритетів у воєнний час.

17.4. Низька інституційна та цифрова спроможність частини органів влади.

17.5. Відсутність системної координації між різними відомствами та рівнями влади.

17.6. Низька поінформованість і недостатня підготовка кадрів до використання європейських практик.

17.7. Інше (вказіть): _____.

18. Які формати співпраці з ЄС і НАТО в сфері національної та цифрової стійкості Ви вважаєте найбільш пріоритетними? (Можна обрати кілька варіантів).

18.1. Спільні навчання, тренування та моделювання кризових ситуацій.

18.2. Участь у європейських програмах підтримки стійкості та кібербезпеки.

18.3. Створення спільних центрів компетенцій / центрів стійкості.

18.4. Обмін даними та спільні аналітичні платформи щодо загроз і ризиків.

18.5. Підтримка в розбудові національної цифрової інфраструктури (хмари, реєстри, платформи).

18.6. Інше (вказіть): _____.

V. ІНСТИТУЦІЇ, ПРИНЦИПИ УПРАВЛІННЯ ТА ДОВІРА

19. Наскільки, на Вашу думку, у поточній політиці та практиці управління реалізуються ключові принципи НМС (людиноцентричність, адаптивність, відкритість, субсидіарність, наукова обґрунтованість, євроінтеграційність)? (Один варіант відповіді).

19.1. У значній мірі: більшість із цих принципів реально впливають на рішення.

19.2. Частково: окремі принципи реалізуються, інші залишаються декларативними.

19.3. Переважно декларативно: принципи фігурують у документах, але мало проявляються в практиці.

19.4. Реалізація принципів суттєво різниться між секторами та рівнями влади.

19.5. Інше (вказіть): _____.

20. Які фактори, на Ваш погляд, найбільше впливають на інституційну стійкість органів публічної влади? (Можна обрати кілька варіантів).

20.1. Якість лідерства та управлінських команд.

20.2. Чіткість мандату, регламентів і процедур кризового управління.

20.3. Рівень цифрової інституційної спроможності (цифровізація процесів, дані, аналітика).

20.4. Кадровий потенціал і система підготовки / підвищення кваліфікації.

20.5. Міжвідомча координація та мережеві форми взаємодії.

20.6. Рівень довіри та співпраці з громадянським суспільством і бізнесом.

20.7. Інше (вказіть): _____.

21. Як Ви оцінюєте рівень довіри громадян до дій держави у кризових ситуаціях (з точки зору Вашого професійного досвіду)? (Один варіант відповіді).

21.1. Високий: суспільство переважно підтримує й довіряє рішенням публічної влади.

21.2. Середній: довіра зберігається, але є суттєві зони скепсису та критики.

21.3. Низький: домінують недовіра, підозри й відчуття непрозорості рішень.

21.4. Суттєво різниться між секторами / регіонами / групами населення.

21.5. Важко оцінити.

22. Які інноваційні підходи Ви вважаєте найбільш перспективними для подальшого розвитку НМС в Україні? (Можна обрати кілька варіантів).

22.1. Регулярне використання DEA для оцінки цифрової стійкості органів влади.

22.2. Масштабне впровадження Institutional SaaS-платформи як «операційної системи» е-адміністрування.

22.3. Побудова смарт-резильєнтних регіональних стратегій (SRPS) для всіх регіонів.

22.4. Створення кластерів інституційної стійкості (КІС) у ключових секторах (безпека, енергетика, цифрова інфраструктура тощо).

22.5. Розвиток рамкової моделі інтегрованого відкритого врядування (відкриті дані, участь, підзвітність).

22.6. Інше (вказіть): _____.

VI. ОСОБИСТА ІНФОРМАЦІЯ

23. Ваш стаж професійної діяльності в сфері, дотичній до публічного управління / безпеки / цифровізації:

23.1. До 3 років

23.2. 3–10 років.

23.3. 11–20 років.

23.4. Понад 20 років.

24. Стать:

24.1. Чоловіча.

24.2. Жіноча.

24.3. Відмова відповідати.

25. Вік (повних років): _____

26. Ваша перша вища освіта (спеціальність / галузь):

27. Основний вид Вашої діяльності (Один варіант відповіді):

27.1. Державний службовець центрального органу виконавчої влади.

27.2. Представник обласної / місцевої військової адміністрації.

27.3. Посадова особа органу місцевого самоврядування.

27.4. Працівник органу, що надає публічні послуги (ЦНАП, соціальні служби тощо).

27.5. Фахівець з цифрових технологій / цифрової трансформації.

27.6. Представник громадського сектору / неурядової організації.

27.7. Науковець / викладач.

27.8. Інше (вказіть): _____.

28. Ви мешкаєте переважно:

28.1. У великому місті (понад 500 тис. населення).

28.2. У середньому місті (50–500 тис.).

28.3. У малому місті (до 50 тис.).

28.4. У селі / селищі.

28.5. Інше (вказіть): _____.

29. Область (регіон) Вашого проживання / основної професійної діяльності:

Дякуємо за участь в опитуванні та внесок у розбудову національної моделі стійкості України в умовах цифрового суспільства!

Додаток Д2

Аналіз результатів опитування

1. Результати опитування

Анкета експертного опитування щодо національної моделі стійкості в умовах цифрового суспільства охопила 127 респондентів – представників центральних органів виконавчої влади, обласних та місцевих військових адміністрацій, органів місцевого самоврядування, фахівців з цифрової трансформації, представників громадянського суспільства та науковців.

Опитування містило 22 запитання, що дозволило сформулювати узагальнену картину стану та перспектив формування національної моделі стійкості (НМС), зокрема її цифрового, інституційного та територіального вимірів, а також рівня адаптації європейського та євроатлантичного досвіду.

Загалом результати свідчать про те, що:

- 1) респонденти визнають поступове формування НМС,
- 2) відзначають нерівномірність цифрової та інституційної стійкості між секторами та рівнями влади,
- 3) підтримують розвиток цифрових інструментів стійкості (NEE, DEA, Institutional SaaS, смарт-резильєнтні регіональні стратегії),
- 4) фіксують серйозні бар'єри законодавчого, ресурсного та інституційного характеру.

2. Аналіз питань анкети

1. Загальний рівень національної стійкості

Питання 1. Як Ви в цілому оцінюєте поточний рівень національної стійкості України в умовах повномасштабної війни та цифровізації?

Високий рівень – 11%

Помірно достатній рівень – 46%

Обмежений рівень (стійкість лише в окремих секторах) – 31%

Низький рівень – 7%

Важко відповісти / інше – 5%

Близько 57% (високий + помірно достатній) вважають, що базові засади стійкості забезпечені, проте понад третина бачить її як секторно обмежену. Це узгоджується з тим, що стійкість краще проявлена в оборонному та окремих цифрових секторах, але залишається вразливою у соціальній, інфраструктурній та територіальній площині.

2. Реалізація ідеї НМС

Питання 2. Наскільки у практиці публічного управління фактично реалізується ідея НМС як інтегрованої рамки модернізації держави?

Значною мірою реалізується – 12%

Частково реалізується – 44%

Реалізується фрагментарно, переважно в секторі безпеки та оборони – 28%

Переважно декларативна – 11%

Інше – 5%

56% (значною мірою + частково) визнають наявність елементів НМС,

однак 39% наголошують на фрагментарності чи декларативності, що вказує на відсутність єдиної, повністю оформленої моделі.

3. Найбільш розвинені виміри НМС

Питання 3. Які з вимірів НМС є найбільш розвиненими? (кілька відповідей)

Функціональний – 58%

Цифровий – 54%

Онтологічний – 41%

Інституційний – 37%

Соціально-комунікативний – 33%

Найчастіше відзначають функціональний та цифровий виміри, що свідчить про відносно кращу здатність забезпечувати базові функції та цифрові сервіси навіть в умовах війни. Водночас інституційний та соціально-комунікативний виміри помітно відстають, що корелює з наявністю інституційних «вузьких місць» та проблемою довіри.

4. Безперервність виконання ключових функцій

Питання 4. Як Ви оцінюєте здатність системи публічного управління забезпечувати безперервність виконання ключових функцій держави в умовах тривалих криз?

Висока – 18%

Середня – 48%

Низька – 13%

Різниться залежно від сектора / рівня влади – 16%

Інше – 5%

Переважає оцінка «середня» (48%), при цьому 29% прямо вказують на низьку або різко нерівномірну спроможність, що підкреслює актуальність механізмів резервування, дублювання функцій і кризового управління.

5. Рівень цифрової стійкості органів влади

Питання 5. Рівень цифрової стійкості державних органів?

Високий – 15%

Середній – 49%

Низький – 14%

Суттєво різниться між органами / секторами – 17%

Важко відповісти – 5%

Більшість (64%) фіксує середній або високий рівень цифрової стійкості, проте 31% наголошують на низькому або дуже нерівномірному рівні, що підтверджує нерівномірний розвиток та потребу в уніфікації стандартів і архітектури.

6. Стан розвитку National E-Resilience

Питання 6. Наскільки розвинена ідея National E-Resilience?

Фактично реалізується як інтегрована модель – 9%

На стадії активного формування – 43%

Представлена окремими несинхронізованими ініціативами – 34%

Майже відсутня як цілісна концепція – 9%

Інше – 5%

Понад 3/4 респондентів (77%) вважають, що National E-Resilience або формується, або вже частково реалізується, але переважно у вигляді окремих, не до кінця узгоджених ініціатив.

7. Використання DEA або аналогів

Питання 7. Чи відомі Вам практики використання методології оцінки цифрової стійкості (DEA) або її аналогів?

Застосовуються системно – 7%

Застосовуються епізодично / пілотно – 29%

Чув(ла), але без відомих прикладів застосування – 26%

Не відомі / не застосовуються – 33%

Інше – 5%

Лише 36% вказують на певне застосування (системне чи пілотне), тоді як 59% фактично не ідентифікують DEA або подібні методики в практиці. Це аргументує потребу в інституціоналізації системного оцінювання цифрової стійкості.

8. Доцільність Institutional SaaS-платформи

Питання 8. Як Ви оцінюєте доцільність впровадження єдиної Institutional SaaS-платформи?

Вкрай доцільно – 46%

Доцільно, з урахуванням галузевої специфіки – 35%

Частково доцільно – 9%

Недоцільно – 4%

Інше – 6%

Отже, 81% підтримують ідею централізованої Institutional SaaS як операційної системи е-адміністрування, при цьому більшість наполягає на можливості адаптації під галузеві та регіональні особливості.

9. Бар'єри цифрової стійкості

Питання 9. З якими бар'єрами цифрової стійкості найчастіше стикаються органи влади? (кілька відповідей)

Фрагментація ІКТ-систем і відсутність єдиної архітектури – 63%

Недостатній рівень кібербезпеки – 52%

Відсутність резервних центрів / планів безперервності – 49%

Низький рівень цифрових компетентностей персоналу – 44%

Обмежене фінансування – 57%

Цифрова нерівність і вразливість фізичної інфраструктури – 38%

Домінують структурно-організаційні та ресурсні бар'єри (фрагментація, фінансування, резервування), що демонструє необхідність архітектурної уніфікації та бюджетування стійкості.

10. Реалістичність використання Adaptive Institutional Trajectory Building

Питання 10. Наскільки реалістичним є застосування Adaptive Institutional Trajectory Building?

Реалістично й необхідно – 41%

Реалістично, але потребує адаптації – 33%

Скоріше утопічно – 11%

Важко відповісти – 10%

Інше – 5%

74% респондентів розглядають поетапні «цифрові траєкторії» як реальний інструмент розвитку, що підтверджує запит на інструменти планового, а не хаотичного нарощування спроможності.

11. Вплив децентралізації на стійкість територій

Питання 11. Як Ви оцінюєте вплив децентралізації на стійкість територіальних громад та регіонів?

Переважно позитивний – 38%

Позитивний для спроможних громад – 32%

Нейтральний – 12%

Переважно негативний – 10%

Інше – 8%

70% вказують на позитивний ефект децентралізації (прямо чи для спроможних громад), але підкреслюють нерівність стійкості між різними типами громад.

12. Роль ОВА та МВА

Питання 12. Яку роль відіграють ОВА та МВА у формуванні регіональної та місцевої стійкості?

Ключову – 44%

Важливу, розділену з ОМС – 37%

Обмежену – 8%

Низьку – 4%

Інше – 7%

Понад 80% розглядають військові адміністрації як ключові або дуже важливі «центри стійкості» на територіальному рівні.

13. Механізми зміцнення стійкості на місцях

Питання 13. Які механізми зміцнення стійкості на територіальному рівні є найбільш ефективними? (кілька відповідей)

Смарт-резильєнтні регіональні стратегії (CPPC / SEES) – 47%

Регіональні / місцеві центри стійкості, ситуаційні центри – 59%

Міжмуніципальне співробітництво – 41%

Цифрові рішення на рівні громад – 53%

Кластери інституційної стійкості (KIC) – 38%

Найбільшу підтримку отримали центри стійкості та локальні цифрові рішення, що відображає практичну орієнтацію на інституціоналізацію й цифровізацію територіального управління.

14. Обмеження стійкості громад в умовах війни

Питання 14. Які фактори найбільше обмежують стійкість громад? (кілька відповідей)

Руйнування критичної інфраструктури – 68%

Недостатнє фінансування – 57%

Кадровий дефіцит – 49%

Низька цифрова спроможність громад – 44%

Недостатня координація між рівнями влади – 39%

Низький рівень довіри / взаємодії з громадянами – 27%

Найчастіше згадуються інфраструктурні втрати, ресурсні обмеження та кадрові проблеми, що відповідає реаліям воєнного часу та підкреслює важливість комплексної політики відновлення.

15. Релевантні зарубіжні джерела досвіду

Питання 15. Досвід яких інституцій або країн є найбільш релевантним для побудови НМС? (кілька відповідей)

Європейський Союз як цілісна рамка – 52%

НАТО – 48%

Естонія – 61%

Скандинавські країни – 39%

Польща та країни ЦСЄ – 45%

Інше – 12%

Найчастіше респонденти звертаються до Естонії (цифрова держава) та Польщі / ЦСЄ (перехідні моделі в умовах загроз), а також ЄС і НАТО як рамкових інституцій стійкості.

16. Елементи досвіду, які найлегше адаптувати

Питання 16. Які елементи європейського й євроатлантичного досвіду стійкості найлегше адаптувати? (кілька відповідей)

Стандарти захисту критичної інфраструктури – 51%

Підходи до кібербезпеки й кіберстійкості – 57%

Моделі багаторівневого врядування – 43%

Системи раннього попередження та кризового моніторингу – 38%

Інструменти участі громадян – 36%

Домінує увага до технічних і управлінських стандартів безпеки, але також відзначено значення багаторівневого врядування та участі громадян.

17. Перешкоди імплементації стандартів стійкості

Питання 17. Які основні перешкоди заважають імплементації європейських стандартів національної та цифрової стійкості? (кілька відповідей)

Недосконалість і фрагментарність законодавства – 66%

Інституційний опір змінам – 54%

Обмежені фінансові ресурси – 59%

Низька інституційна та цифрова спроможність частини органів влади – 51%

Відсутність системної координації – 48%

Низька поінформованість та підготовка кадрів – 42%

Відповіді вказують на комплексний характер бар'єрів – одночасно правових, організаційних, ресурсних та кадрових.

18. Пріоритетні формати співпраці з ЄС і НАТО

Питання 18. Які формати співпраці з ЄС і НАТО у сфері стійкості є

пріоритетними? (кілька відповідей)

Спільні навчання, тренування, моделювання криз – 63%

Участь у програмах підтримки стійкості й кібербезпеки – 58%

Створення спільних центрів компетенцій / центрів стійкості – 49%

Обмін даними та спільні аналітичні платформи – 41%

Підтримка розбудови національної цифрової інфраструктури – 52%

Респонденти орієнтуються на практичні та інституційні формати співпраці, що забезпечують передачу знань, технологій та спільну підготовку до криз.

19. Реалізація принципів НМС

Питання 19. Наскільки реалізуються ключові принципи НМС (людиноцентричність, адаптивність, відкритість, субсидіарність тощо)?

У значній мірі – 17%

Частково – 49%

Переважно декларативно – 19%

Суттєво різняться між секторами / рівнями – 11%

Інше – 4%

Дві третини (66%) визнають хоча б часткову реалізацію принципів, однак понад 30% говорять про їхню декларативність або різку нерівномірність у практиці.

20. Фактори інституційної стійкості

Питання 20. Які фактори найбільше впливають на інституційну стійкість органів публічної влади? (кілька відповідей)

Якість лідерства та управлінських команд – 71%

Чіткість мандату, регламентів і процедур кризового управління – 58%

Рівень цифрової інституційної спроможності – 62%

Кадровий потенціал і система підготовки – 55%

Міжвідомча координація та мережеві взаємодії – 49%

Довіра та співпраця з громадянським суспільством і бізнесом – 44%

Провідну роль відіграють лідерство, цифрова спроможність та інституційно оформлене кризове управління, що підтверджує необхідність поєднання «людського» й цифрового вимірів стійкості.

21. Рівень довіри громадян у кризах

Питання 21. Як Ви оцінюєте рівень довіри громадян до дій держави у кризових ситуаціях?

Високий – 14%

Середній – 46%

Низький – 18%

Суттєво різняться між секторами / регіонами – 17%

Важко оцінити – 5%

Переважає оцінка «середній», однак 35% респондентів відзначають низький чи різко диференційований рівень довіри, що актуалізує соціально-комунікативний вимір НМС.

22. Перспективні інноваційні підходи до розвитку НМС

Питання 22. Які інноваційні підходи є найбільш перспективними для розвитку НМС? (кілька відповідей)

Регулярне використання DEA – 48%

Масштабне впровадження Institutional SaaS – 52%

Смарт-резильєнтні регіональні стратегії (CPPC) – 45%

Кластери інституційної стійкості (KIC) – 39%

Рамкова модель інтегрованого відкритого врядування – 43%

Найбільшу підтримку мають цифрові та інституційні інструменти (Institutional SaaS, DEA, CPPC), що орієнтовані на поєднання цифрової, інституційної та територіальної стійкості.

3. Загальний висновок

Отримані результати демонструють, що:

1) національна стійкість сприймається як частково сформована, із суттєвими секторальними й територіальними розривами;

2) цифровий вимір стійкості розвивається динамічно, але супроводжується фрагментацією систем, браком ресурсів і нерівномірністю спроможностей;

3) існує широка підтримка цифрових інструментів НМС (NEE, DEA, Institutional SaaS, CPPC, KIC), однак їх практичне застосування ще обмежене;

4) децентралізація й діяльність військових адміністрацій розглядаються як ключові чинники територіальної стійкості, водночас зберігається значна асиметрія між громадами;

5) впровадження європейських і євроатлантичних стандартів стримується недосконалістю законодавства, інституційним опором і дефіцитом ресурсів, що потребує цілеспрямованих реформ.

Таким чином, опитування підтверджує необхідність подальшого формування національної моделі стійкості як інтегрованої інституційно-цифрової рамки модернізації публічного управління, із пріоритетом цифрової стійкості, інституційної спроможності та багаторівневого врядування.

