

Електронне
наукове видання

«ПУБЛІЧНЕ
АДМІНІСТРУВАННЯ
ТА НАЦІОНАЛЬНА
БЕЗПЕКА»

ISSN 2617-572X
DOI: 10.25313/2617-572X-2025-5



№ 5 (58) / 2025



**Електронне наукове видання
«ПУБЛІЧНЕ АДМІНІСТРУВАННЯ
ТА НАЦІОНАЛЬНА БЕЗПЕКА»**

**Electronic scientific publication
«PUBLIC ADMINISTRATION
AND NATIONAL SECURITY»**

НАУКОВЕ ФАХОВЕ ВИДАННЯ

№ 5 (58)

Київ 2025

ББК 66.061.43

УДК 351

П88



Електронне наукове видання «Публічне адміністрування та національна безпека» зареєстровано в міжнародних каталогах наукових видань та наукометричних базах даних: Index Copernicus International (ICI); Polish Scholarly Bibliography; Google Scholar; Наукова періодика України; ResearchBib; Electronic Journals Library; Bielefeld Academic Search Engine (BASE); CrossRef.

НАУКОВЕ ФАХОВЕ ВИДАННЯ

Видання включено до Переліку наукових фахових видань
МОН України (категорія В) з державного управління (спеціальність 281),
на підставі Наказу Міністерства освіти та науки України
№ 358 від 15.03.2019.

У виданні опубліковані наукові статті з висвітленням теоретичних та практичних аспектів у сфері публічного управління та національної безпеки. Для наукових працівників, викладачів, студентів, фахівців у сфері національної безпеки, працівників державних установ, юридичних компаній, судів, правоохоронних органів й інших зацікавлених осіб.

Матеріали публікуються мовою оригіналу в авторській редакції.

Редакція не завжди поділяє думки і погляди автора. Відповідальність за достовірність фактів, імен, географічних назв, цитат, цифр та інших відомостей несуть автори публікацій.

У відповідності із Законом України «Про авторське право і суміжні права», при використанні наукових ідей і матеріалів цієї збірки, посилання на авторів та видання є обов'язковими.

© Автори статей, 2025

© Електронне наукове видання
«Публічне адміністрування
та національна безпека», 2025

ISSN 2617-572X Elektronne naukove vidannâ "Publične administruvannâ ta nacional'na bezpeka"

Редакція
Головний редактор

Головний редактор — **Романенко Євген Олександрович**, доктор наук з державного управління, професор, проректор з наукової роботи Національного авіаційного університету, академік Української Технологічної Академії, академік Міжнародної Кадрової Академії та Академії наук публічного управління, Заслужений юрист України (Київ, Україна)

Заступники головного редактора

Непомнящий Олександр Михайлович — доктор наук з державного управління, професор, академік Академії будівництва України, професор кафедри публічного адміністрування Міжрегіональної Академії управління персоналом (Київ, Україна)

Жукова Ірина Віталіївна — кандидат наук із державного управління, доцент, заступник директора з навчально-виховної роботи Навчально-наукового інституту менеджменту та психології ДЗВО «Університет менеджменту освіти», виконавчий директор президії громадської організації «Всеукраїнська асамблея докторів наук з державного управління» (Київ, Україна)

Редакційна колегія

Арошидзе Паата — доктор економічних наук, професор, Асоційований професор Державного університету імені Шота Руставелі (Грузія)

Ахметова Лайла Сейсембековна — професор політології, доктор історичних наук, професор кафедри ЮНЕСКО, міжнародної журналістики і медіа в суспільстві факультету журналістики Казахського Національного університету (КазНУ) ім. аль-Фарабі (Казахстан)

Бурик Зоряна Михайлівна — доктор наук з державного управління, старший викладач кафедри регіонального управління та місцевого самоврядування Львівського регіонального інституту державного управління Національної академії державного управління при Президентові України (Львів, Україна)

Гечбаія Бадрі Нодаровіч — доктор економічних наук, професор, Асоційований професор Батумського державного університету ім. Шота Руставелі (Грузія)

Гурковський Володимир Ігорович — доктор наук з державного управління, старший дослідник, професор кафедри інформаційної політики та цифрових технологій Національної академії державного управління при Президентові України, перший заступник директора ВГО «Центр дослідження проблем публічного управління» (Київ, Україна)

Гвожджевiч Сильвія — кандидат наук, кафедра адміністрації та національної безпеки Державної професійної вищої школи ім. Якуба з Парадижу в Гожуві-Великопольському (Польща)

Дегтяр Андрій Олегович — завідувач кафедри менеджменту та адміністрування Харківської державної академії культури Міністерства культури України, доктор наук з державного управління, професор, заслужений діяч науки і техніки України (Харків, Україна)

Дегтяр Олег Андрійович — доктор наук з державного управління, доцент, доцент кафедри менеджменту і адміністрування Харківського національного університету міського господарства ім. О. М. Бекетова (Харків, Україна)

Драган Іван Олександрович — доктор наук з державного управління, старший науковий співробітник, професор кафедри економічної безпеки, публічного управління та адміністрування Житомирського державного технологічного університету МОН України (Житомир, Україна)

Іваницька Ольга Михайлівна — доктор наук з державного управління, професор, професор кафедри теорії та практики управління Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського» (Київ, Україна)

Кіслов Денис Васильович — доктор наук з державного управління, доцент, академік Української академії наук, Академік Національної Академії наук вищої освіти України, професор кафедри публічного адміністрування Міжрегіональної Академії управління персоналом (Київ, Україна)

Козаков Володимир Миколайович — доктор наук з державного управління, професор, професор кафедри державної політики та суспільного розвитку Національної академії державного управління при Президентові України (Київ, Україна)

Кринична Ірина Петрівна — доктор наук з державного управління, професор, професор кафедри державного управління та місцевого самоврядування Дніпропетровського регіонального інституту державного управління Національної академії державного управління при Президентові України (Дніпро, Україна)

Мідельський Сергій Людвигович — професор, Академік, Президент Регіональної Академії Менеджменту (Казахстан)

Мотренко Тимофій Валентинович — доктор філософських наук, професор, професор кафедри публічного адміністрування Міжрегіональної Академії управління персоналом, Академік Національної академії педагогічних наук України (Київ, Україна)

Новак-Каляева Лариса Миколаївна — доктор наук з державного управління, професор, професор кафедри державного управління Львівського регіонального інституту державного управління Національної академії державного управління при Президентові України (Львів, Україна)

Пархоменко-Куцевіл Оксана Ігорівна — доктор наук з державного управління, завідувач кафедри публічного адміністрування Міжрегіональної Академії управління персоналом (Київ, Україна)

Радченко Олександр Віталійович — доктор наук з державного управління, професор, професор Університету Яна Длугоша в Ченстохові (Польща)

Ромат Євгеній Вікторович — доктор наук з державного управління, завідувач кафедри маркетингу та реклами Київського національного торговельно-економічного університету (Київ, Україна)

Ситник Григорій Петрович — доктор наук з державного управління, кандидат технічних наук, професор, заслужений діяч науки і техніки України, професор кафедри державного управління Київського національного університету імені Тараса Шевченка (Київ, Україна)

Сурай Інна Геннадіївна — доктор наук з державного управління, доцент, професор кафедри публічного управління та публічної служби Національної академії державного управління при Президентові України (Київ, Україна)

Кухарчук Петро Михайлович — кандидат наук з державного управління, доцент, професор кафедри суспільно-гуманітарних дисциплін Комунального закладу «Житомирський обласний інститут післядипломної педагогічної освіти» Житомирської обласної ради (Житомир, Україна)

Шмагун Антоніна Вікторівна — кандидат наук з державного управління, доцент кафедри публічного управління і проектного менеджменту Навчально-наукового інституту менеджменту та психології ДЗВО «Університет менеджменту освіти» (Київ, Україна)

Якимчук Аліна Юріївна — доктор економічних наук, професор, професор кафедри державного управління, документознавства та інформаційної діяльності Національного університету водного господарства та природокористування (Рівне, Україна)

Яровой Тихон Сергійович — кандидат наук з державного управління, доцент, доцент кафедри публічного адміністрування Міжрегіональної Академії управління персоналом (Київ, Україна)

Агнешка Кістер — доцент, доктор наук, Факультет економіки, Університет Марії Склодовської Кюрі (Польща)

Недбалек Карел — доктор філософії (PhD) в галузі права, доцент, професор Європейського професійного докторату, MBA, адвокат (Чехія)

ЗМІСТ

ГУМАНІТАРНА І ПОЛІТИЧНА БЕЗПЕКА ДЕРЖАВИ

Стоволос Надія Борисівна ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ЯК ОСНОВНОЇ СКЛАДОВОЇ ПУБЛІЧНОГО УПРАВЛІННЯ	9
Верховцева Ірина Геннадіївна, Шестаков Валерій Іванович, Гребенюк Віталій Миколайович, Гайдук Олег Васильович НОВІТНЯ ТЕРМІНОЛОГІЯ У ДИПЛОМАТИЧНИХ ПРАКТИКАХ ЯК МАРКЕР КІБЕРВПЛИВІВ: ЦИФРОВА ДИПЛОМАТІЯ, КІБЕРДИПЛОМАТІЯ	15
Кондратюк Сергій Володимирович, Верховцева Ірина Геннадіївна, Закіров Марат Борисович, Кондратенко Олег Юрійович, Любченко Андрій Володимирович, Хорватова Оксана Олегівна ЗМІЩЕННЯ ІНСТИТУЦІЙНИХ І ЗАКОНОДАВЧИХ ОСНОВ ЄВРОПЕЙСЬКОЇ КІБЕРДИПЛОМАТІЇ В УМОВАХ ЕСКАЛАЦІЇ РОСІЙСЬКИХ ГІБРИДНИХ ЗАГРОЗ.....	23
Литвиненко Євгенія Віталіївна КОМПАРАТИВНИЙ АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ МІЖВІДОМЧОЇ ВЗАЄМОДІЇ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В КРАЇНАХ, ЩО ПЕРЕБУВАЮТЬ У СТАНІ КОНФЛІКТУ АБО ПОСТКОНФЛІКТНОГО ВІДНОВЛЕННЯ	34
Шемаєв Володимир Миколайович, Єрьоміна Людмила Валеріївна «PORCUPINE STRATEGY» ДЛЯ УКРАЇНИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ	41

ДОСЛІДЖЕННЯ, РОЗРОБКИ, ПРОЕКТИ З ПИТАНЬ ПУБЛІЧНОГО УПРАВЛІННЯ
ТА АДМІНІСТРУВАННЯ

Горбачук Назарій Вікторович ПОЛЬСЬКИЙ ДОСВІД РЕГУЛЯЦІЇ РКР ЯК МОДЕЛЬ ДЛЯ ВДОСКОНАЛЕННЯ ПОЛІТИКИ ДЕРЖАВНОГО НАГЛЯДУ	48
Корсун Андрій Васильович, Бабій Вадим Юрійович БЕЗПЕРЕРВНА ОСВІТА МЕДИКІВ В ЕПОХУ ЦИФРОВІЗАЦІЇ: ФОКУС НА УПРАВЛІННІ КЛІНІЧНИМИ РИЗИКАМИ	57
Михайлов Сергій Юрійович ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ В ПУБЛІЧНОМУ УПРАВЛІННІ УКРАЇНИ: ЄВРОПЕЙСЬКІ ОРІЄНТИРИ.....	66
Прокопчук Ілля Петрович, Вознюк Наталія Іванівна, Супруненко Світлана Анатоліївна ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОПТИМІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ У ПЕРІОД ПІСЛЯВОЄННОГО ВІДНОВЛЕННЯ	75

Франчук Володимир Сергійович

ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ: ПОТЕНЦІАЛ ТА РИЗИКИ ...83

ІНСТИТУЦІЙНИЙ РОЗВИТОК ГРОМАД У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ**Короляк Остап Орестович**ІНСТИТУЦІЙНА СПРОМОЖНІСТЬ ТЕРИТОРІАЛЬНИХ ГРОМАД ЯК ЧИННИК
ЕКОНОМІЧНОГО РОЗВИТКУ УКРАЇНИ90**ПРАКТИЧНІ АСПЕКТИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ****Матвійшин Євген Григорович, Маринчук Олександр Васильович**РОЗВИТОК СИСТЕМ НАДАННЯ ПОСЛУГ ВОДОПОСТАЧАННЯ З ВИКОРИСТАННЯМ
МЕХАНІЗМУ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА98**РЕГІОНАЛЬНЕ УПРАВЛІННЯ ТА МІСЦЕВЕ САМОВРЯДУВАННЯ****Марискевич Андрій Тарасович**

ПУБЛІЧНЕ УПРАВЛІННЯ СТАЛИМ РОЗВИТКОМ РЕГІОНІВ 106

СОЦІАЛЬНА І ГУМАНІТАРНА ПОЛІТИКА**Івлієва Ольга Михайлівна, Мізюк Вікторія Анатоліївна, Драгієва Людмила Василівна**СОЦІАЛЬНО-ГУМАНІТАРНІ АСПЕКТИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ВИКЛАДАЧІВ
МАТЕМАТИЧНИХ ДИСЦИПЛІН У КОНТЕКСТІ СУЧАСНОЇ ОСВІТНЬОЇ ПОЛІТИКИ 112**ФІЛОСОФІЯ, МЕТОДОЛОГІЯ, ТЕОРІЯ ТА ІСТОРІЯ ОСНОВ НАЦІОНАЛЬНОЇ
БЕЗПЕКИ ДЕРЖАВИ****Тесніков Олександр Михайлович, Фурсова Вікторія Анатоліївна**УПРАВЛІННЯ ВІЙСЬКОВОЮ ЛОГІСТИКОЮ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ:
ДОСВІД УКРАЇНИ ТА ІЗРАЇЛЮ 118**ФУНКЦІОНУВАННЯ І РОЗВИТОК МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ****Залізняк Вікторія Петрівна**ІННОВАЦІЙНІ ПІДХОДИ ДО ПУБЛІЧНОГО АДМІНІСТРУВАННЯ СФЕРИ СОЦІАЛЬНОГО
ЗАХИСТУ: ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ 126**Луковський Роман Ігорович, Парійчук Вікторія Анатоліївна**ПРОЦЕСИ ДІДЖИТАЛІЗАЦІЇ ПІД ЧАС ЗАПРОВАДЖЕННЯ ПРАВОВОГО РЕЖИМУ
ВОЄННОГО СТАНУ ЯК ВАЖЛИВИЙ ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО
ПУБЛІЧНОГО УПРАВЛІННЯ 134**Стеців Ірина Семенівна, Козопас Андрій Володимирович**ІНСТИТУЦІЙНІ МЕХАНІЗМИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІННОВАЦІЙНОГО
ПІДПРИЄМНИЦТВА В УМОВАХ ТРАНСФОРМАЦІЙНОЇ ЕКОНОМІКИ УКРАЇНИ 143

CONTENTS

HUMANITARIAN AND POLITICAL SECURITY OF THE STATE

Stovolos Nadiya

ENSURING NATIONAL SECURITY AS A MAIN COMPONENT OF PUBLIC ADMINISTRATION..... 9

Verkhovtseva Iryna, Shestakov Valerii, Grebenyuk Vitaliy, Gaiduk Oleg

THE LATEST TERMINOLOGY IN DIPLOMATIC PRACTICES AS A MARKER OF CYBER
INFLUENCE: DIGITAL DIPLOMACY, CYBER DIPLOMACY 15

Kondratiuk Serhii, Verkhovtseva Iryna, Zakirov Marat,

Kondratenko Oleh, Lyubchenko Andrii, Horvatova Oksana

STRENGTHENING THE INSTITUTIONAL AND LEGISLATIVE FOUNDATIONS OF EUROPEAN
CYBER DIPLOMACY IN THE FACE OF ESCALATING RUSSIAN HYBRID THREATS 23

Lytvynenko Yevheniia

COMPARATIVE ANALYSIS OF EXISTING MODELS OF INTERAGENCY COOPERATION
IN THE FIELD OF NATIONAL SECURITY IN COUNTRIES IN CONFLICT
OR POST-CONFLICT RECOVERY 34

Shemayev Volodymyr, Yeromina Lyudmila

"PORCUPINE STRATEGY" FOR UKRAINE IN THE CONTEXT OF ENSURING NATIONAL
SECURITY 41

RESEARCH, DEVELOPMENT, PROJECTS ON PUBLIC ADMINISTRATION AND ADMINISTRATION

Horbachuk Nazarii

POLISH EXPERIENCE OF PKP REGULATION AS A MODEL FOR IMPROVING STATE
SUPERVISION POLICY 48

Korsun Andrii, Babii Vadym

CONTINUING EDUCATION OF PHYSICIANS IN THE AGE OF DIGITALIZATION: FOCUS
ON CLINICAL RISK MANAGEMENT 57

Mykhailov Serhii

INSTITUTIONAL SUPPORT FOR DIGITAL SOVEREIGNTY IN PUBLIC ADMINISTRATION
OF UKRAINE: EUROPEAN GUIDELINES 66

Prokopchuk Illia, Vozniuk Nataliia, Suprunenko Svitlana

USING ARTIFICIAL INTELLIGENCE TO OPTIMIZE PUBLIC ADMINISTRATION IN UKRAINE
DURING THE POST-WAR RECOVERY PERIOD 75

Franchuk Volodymyr

ARTIFICIAL INTELLIGENCE IN THE PUBLIC ADMINISTRATION SYSTEM: POTENTIAL
AND RISKS 83

**INSTITUTIONAL DEVELOPMENT OF COMMUNITIES IN THE PUBLIC ADMINISTRATION
SYSTEM****Koroliak Ostop**INSTITUTIONAL CAPACITY OF TERRITORIAL COMMUNITIES AS A FACTOR OF ECONOMIC
DEVELOPMENT OF UKRAINE90**PRACTICAL ASPECTS OF ECONOMIC SECURITY OF THE STATE****Matviishyn Yevhen, Marynychuk Oleksandr**DEVELOPMENT OF WATER SUPPLY SERVICE SYSTEMS USING THE PUBLIC-PRIVATE
PARTNERSHIP MECHANISM98**REGIONAL MANAGEMENT AND LOCAL SELF-GOVERNMENT****Maryshevych Andrii**

PUBLIC MANAGEMENT OF SUSTAINABLE DEVELOPMENT OF REGIONS 106

SOCIAL AND HUMANITARIAN POLICY**Ivliieva Olga, Miziuk Viktoriia, Drahieva Liudmyla**SOCIAL AND HUMANITARIAN ASPECTS OF PROFESSIONAL TRAINING OF TEACHERS OF
MATHEMATICAL DISCIPLINES IN THE CONTEXT OF MODERN EDUCATIONAL POLICY 112**PHILOSOPHY, METHODOLOGY, THEORY AND HISTORY OF THE FOUNDATIONS
OF NATIONAL SECURITY OF THE STATE****Tesnikov Oleksandr, Fursova Viktoriya**MANAGEMENT OF MILITARY LOGISTICS IN THE NATIONAL SECURITY SYSTEM:
THE EXPERIENCE OF UKRAINE AND ISRAEL..... 118**FUNCTIONING AND DEVELOPMENT OF PUBLIC ADMINISTRATION MECHANISMS****Zalizniuk Viktoriia**INNOVATIVE APPROACHES TO PUBLIC ADMINISTRATION OF SOCIAL PROTECTION:
IMPLEMENTATION OF DIGITAL TECHNOLOGIES 126**Lukovsky Roman, Pariichuk Viktoriia**DIGITALIZATION PROCESSES DURING THE IMPLEMENTATION OF THE LEGAL
REGIME OF MARTYR STATE AS AN IMPORTANT TOOL FOR ENSURING EFFECTIVE
PUBLIC ADMINISTRATION 134**Stetsiv Iryna, Kozopas Andrii**INSTITUTIONAL MECHANISMS OF STATE REGULATION OF INNOVATIVE
ENTREPRENEURSHIP IN THE CONTEXT OF UKRAINE'S TRANSFORMATIONAL ECONOMY...143

Stovolos Nadiya

*Candidate of Economic Sciences, Associate Professor
Sumy National Agrarian University*

Стоволос Надія Борисівна

кандидат економічних наук, доцент

Сумський національний аграрний університет

ORCID: 0000-0002-9581-4087

DOI: 10.25313/2617-572X-2025-5-10992

ENSURING NATIONAL SECURITY AS A MAIN COMPONENT OF PUBLIC ADMINISTRATION

ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ЯК ОСНОВНОЇ СКЛАДОВОЇ ПУБЛІЧНОГО УПРАВЛІННЯ

Summary. Introduction. The basic priority of life activity is the preservation of the qualitative certainty of statehood and the functioning that corresponds to its nature, and national security reflects the degree of protection of the material and spiritual values of man, society and state institutions from dangers or their absence and the related basic priorities for ensuring the positive dynamics of statehood development. Therefore, the choice of specific ways, means, and methods of ensuring national security is determined by the need to take timely measures, adequate to the nature and scale of threats to statehood.

Purpose. The purpose of this article is to analyze the provision of national security in Ukraine, which is regulated by the regulatory framework, and to substantiate the feasibility of improving state policy in the field of national security, taking into account the martial law in Ukraine.

Materials and methods. The materials of the study are: 1) regulatory and legal support for public management of national security; 2) works of domestic and foreign authors who conduct their scientific and practical research in the field of state-management activities in the field of national security.

In the process of conducting the research, the following scientific methods were used: theoretical generalization and grouping to characterize the components of national security, as well as analysis of the current legislation of Ukraine, which allows us to conclude that the objects on which the managerial influences of subjects of state and administrative activity is directed are: constitutional rights and freedoms of man and citizen; spiritual, moral and ethical, cultural, historical, intellectual and material values of society; constitutional order, sovereignty, territorial integrity and inviolability; information and natural environment; natural resources.

Results. In the article, the problems of ensuring national security in Ukraine are analyzed in detail. It is noted that their specific diversity and complexity are constantly increasing, which is a natural consequence of the threatening situation in almost all spheres of state and public life. At the same time, national specificity regarding the sources and manifestations of threats is revealed.

The analysis of information sources shows that there are different definitions of the concept of threats to national interests, and the concept of "threat" is general and is widely used in the analysis of phenomena, actions, inaction, events that can cause harm to a person, society, state. At the same time, it should be emphasized that the threat may arise with one or another degree of probability under certain conditions that are not always easy to foresee.

Discussion. The choice of ways, means and methods of ensuring national security is determined by the need for timely adoption of measures adequate to the nature and scale of dangers to statehood.

Therefore, we believe that there is a need to analyze and use international experience in ensuring the national security state policy, taking into account their specific conditions and new challenges. It remains important to develop and implement effective measures aimed at real solutions to the main problems of ensuring the national security of our country.

Key words: national security, threats, public administration.

Анотація. Вступ. Фундаментальне значення життя полягає у підтримці якості державності та функціонування відповідно до її природи, а національна безпека відображає рівень захищеності матеріальних і духовних цінностей особистості, суспільства та державних інституцій від небезпек або їх відсутності та пов'язані з цим фундаментальні пріоритети для забезпечення розвитку держави. Отже, вибір конкретних методів, засобів та прийомів забезпечення національної безпеки визначається необхідністю своєчасного вжиття заходів, адекватних характеру та масштабам загрози державі.

Мета. Метою даної статті є аналіз забезпечення національної безпеки в Україні, що регулюється нормативно-правовою базою та обґрунтування доцільності вдосконалення державної політики в сфері національної безпеки з урахуванням воєнного стану в Україні.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення щодо публічного управління національною безпекою; 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження у царині державно-управлінської діяльності у сфері національної безпеки.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування для характеристики складових національної безпеки, а також аналіз чинного законодавства України, котрий дозволяє дійти висновку, що предметами, на які спрямовуються управлінські впливи суб'єктів державно-управлінської діяльності, є: конституційні права і свободи людини і громадянина; духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності суспільства; конституційний лад, суверенітет, територіальна цілісність і недоторканість; інформаційне і навколишнє природне середовище; природні ресурси.

Результати. У статті детально аналізуються проблеми забезпечення національної безпеки в Україні. Відзначено, що їх видова різноманітність та складність постійно збільшується, що є закономірним наслідком загрозливої ситуації майже в усіх сферах державного і суспільного життя. При цьому виявляється національна специфіка щодо джерел та проявів загроз.

Аналіз джерел показує, що існують різні визначення поняття загрози національним інтересам, а поняття "загроза" є поширеним та широко використовується при аналізі явищ, дій, бездіяльності, подій, які здатні завдати шкоди окремій особі, суспільству чи країні. Слід наголосити, що загрози, з різним ступенем ймовірності, можуть виникати за певних обставин, які не завжди легко передбачити.

Перспективи. Вибір шляхів, засобів і способів забезпечення національної безпеки зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам небезпек для державності. Тому вважаємо, що є необхідність аналізу та використання міжнародного досвіду у забезпеченні державної політики національної безпеки, з урахуванням їхніх специфічних умов та нових викликів. Важливим залишається розробка та впровадження ефективних заходів, спрямованих на реальне вирішення основних проблем забезпечення національної безпеки нашої країни.

Ключові слова: національна безпека, загрози, публічне управління.

Problem statement. The basic priority of life activity is the preservation of the qualitative certainty of statehood and the functioning that corresponds to its nature, and national security reflects the degree of protection of the material and spiritual values of man, society and state institutions from dangers or their absence and the related basic priorities for ensuring the positive dynamics of statehood development. Therefore, the choice of specific ways, means, and methods of ensuring national security is determined by the need to take timely measures, adequate to the nature and scale of threats to statehood.

Analysis of recent research and publications. Certain aspects of ensuring national security as an important component of public administration were studied by such scholars as S. Barabash and T. Lutsenko [11], S. Ryabov [10], G. Sytnyk [3,8], V. Tsvetkov [9] and others.

Formulation of the article's objectives. The purpose of this article is to analyze the provision of national security in Ukraine, which is regulated by the regulatory framework, and to substantiate the feasibility of improving state policy in the field of national security, taking into account the martial law in Ukraine.

Presentation of the main material. In Ukraine, according to the Law [1] "national security" is a set of

legislative and organizational measures aimed at the constant protection of the vital interests of a person and a citizen, society and the state, which ensures the sustainable development of society, timely identification, prevention and neutralization of real and potential threats to national interests in the areas of law enforcement, the fight against corruption, border activities and defense, migration policy, healthcare, education and science, scientific, technical and innovation policy, cultural development of the population, ensuring freedom of speech and information security, social policy and pension provision, housing and communal services, financial services market, protection of property rights, stock markets and securities circulation, tax-budgetary and customs policy, trade and entrepreneurial activity, the market of banking services, investment policy, audit activity, monetary and currency policy, information protection, licensing, industry and agriculture, transport and communication, information technologies, energy and energy conservation, the functioning of natural monopolies, the use of subsoil, land and water resources, minerals, protection of ecology and the environment, and other areas of public administration in the event of negative trends that create potential or real threats to national interests.

The Law of Ukraine "On National Security of Ukraine" of 2018 provides the following definition of national security: "...it is the protection of state sovereignty, territorial integrity, democratic constitutional order and other national interests of Ukraine from real and potential threats" [2].

It should also be noted that national security is not only an assessment of certain security of the specified system against potential and real threats. It also reflects, in particular, the results of the influence of development trends and conditions of life of society, its institutions, which are determined by the relevant guidelines (political, legal and others), which ensure the preservation of the qualitative certainty of the social system and the free functioning that corresponds to its nature.

The national security of Ukraine is ensured by carrying out a balanced state policy in accordance with the doctrines, concepts, strategies and programs adopted in the established order in the political, economic, social, military, environmental, scientific and technological, information and other spheres. The choice of specific means and ways of ensuring Ukraine's national security is determined by the need to take timely measures, adequate in nature and scale of threats to national interests.

Powers of national security subjects. According to the Constitution of Ukraine and the laws of Ukraine:

1. The President of Ukraine, as the head of state, guarantor of state sovereignty, territorial integrity of Ukraine, observance of the Constitution of Ukraine, human and civil rights and freedoms, Supreme Commander-in-Chief of the Armed Forces of Ukraine and Chairman of the National Security and Defense Council of Ukraine, exercises general leadership in the areas of national security and defense of Ukraine;

2. The Verkhovna Rada of Ukraine, within the powers defined by the Constitution of Ukraine, determines the principles of domestic and foreign policy, the foundations of national security, forms the legislative framework in this area, approves decisions on the introduction of a state of emergency and martial law, mobilization, determination of the general structure, number, and functions of the Armed Forces of Ukraine and other military formations created in accordance with the laws of Ukraine;

3. The National Security and Defense Council of Ukraine coordinates and controls the activities of executive bodies in the areas of national security and defense; taking into account changes in the geopolitical situation, submits proposals to the President of Ukraine on clarifying the National Security Strategy of Ukraine and the Military Doctrine of Ukraine;

4. The Cabinet of Ministers of Ukraine, as the highest body in the system of executive bodies, ensures the state sovereignty and economic independence of Ukraine, takes measures to ensure the rights and freedoms of man and citizen, defense capability, na-

tional security of Ukraine, public order and the fight against crime;

5. The National Bank of Ukraine, in accordance with the basic principles of monetary and credit policy determines and implements monetary and credit policy in the interests of the national security of Ukraine;

6. Ministries, other central bodies of executive power, Service Security of Ukraine and the Foreign Intelligence Service of Ukraine, within the limits of their powers, ensure the fulfillment of the tasks stipulated by the Constitution of Ukraine and the laws of Ukraine, acts of the President of Ukraine, the Cabinet of Ministers of Ukraine, implement concepts and programs in the field of national security, maintain readiness for the use of force and means of ensuring national security;

7. Local state administrations and local self-government bodies ensure the resolution of issues in the field of national security, assigned by law to their competence;

8. The military organization of the state ensures the defense of Ukraine, the protection of its sovereignty, territorial integrity and inviolability of borders; counteracts external threats of a military nature;

9. Law enforcement agencies fight crime and counter terrorism, ensure the protection and rescue of the population in the event of man-made and natural emergencies;

10. Courts of general jurisdiction conduct proceedings in cases of crimes that harm the national security of Ukraine;

11. The Prosecutor's Office of Ukraine exercises powers in the field of national security of Ukraine in accordance with the Constitution of Ukraine and the Law of Ukraine "On the Prosecutor's Office of Ukraine" [4];

12. Citizens of Ukraine, through participation in elections, referendums and other forms of direct democracy, as well as through the state authorities and local self-government bodies they elect, implement national interests, voluntarily and in accordance with their constitutional duties, carry out measures specified by the legislation of Ukraine to ensure its national security; both directly and through associations of citizens, draw the attention of public and state institutions to dangerous phenomena and processes in various spheres of life of the country; in a legal manner and by legal means, protect their own rights and interests, as well as their own security.

Public administration in the field of national security as a system and a specific type of state administrative activity is an integral part of public administration, covering the social, economic, humanitarian and political spheres of life of society and the state.

There are at least two different approaches to understanding the content of public administration [9]. In the first of them, the so-called American one, focused on all processes and functions of management

in the spectrum of state powers, public administration is viewed as a field that encompasses many disciplines and includes the legislative, executive and judicial branches of government, and in the second, the so-called European one, public administration is viewed as a sub-branch of law. In other words, the first approach involves combining political, legal and administrative functions, and the second involves separating them, that is, defining public administration as all non-legislative and non-judicial activities of the state or as subordinate executive and administrative activities of state bodies.

The main goal of state management activity in the field of national security is forecasting, timely detection, prevention and neutralization of threats to the sustainable development of people, society and the state (primarily to their vital interests).

It should be noted that since in the classical sense, public management is a search for the best way to use resources to achieve priority goals of state policy [7], the logical question arises of identifying the main criteria for assessing the effectiveness of state management activities in the field of national security.

It should be noted that modern internal threats in Ukraine are more dangerous, as they are more difficult to recognize. They can appear unexpectedly as a result of some uncertain economic, social, environmental and other processes, as a result of underestimation or overestimation of certain factors as natural and therefore no less dangerous, consequences of defects in social, political, administrative structures, etc.

Internal threats make Ukraine more vulnerable to external threats and they are the main object of public administration. Analysis of the state of national security of Ukraine in recent years [8] shows that internal threats posed the greatest danger to the development of the state. They were simultaneously associated with several national interests and had a tendency to grow.

Many of them are quite dangerous and relatively long-lasting. Their total potential is concentrated mainly in the economic, socio-political, international, military, informational and environmental spheres. This also includes the sphere of regional relations.

According to the degree of their negative impact on national security [3], they can be classified as follows:

1. A potential challenge is a situation where there is a possibility of the occurrence of conditions under which the potential for countering the realization of national interests may be formed. In this case, the main function of state authorities is to assess the risks of damage in a particular area of national security in the event of conditions under which the potential for counteraction to the realization of national interests may be formed and to implement preventive measures to block the occurrence of these conditions. In other words, this is a situation when a certain potential for counteraction to the realization of national interests may accumulate;

2. A real challenge is a situation when the formation of prerequisites (accumulation of potential) for counteraction to the realization of national interests has been completed, but there is still no counteraction to the achievement of national goals in the form of official statements, political, economic or other actions. Under these conditions, the main function of state authorities is:

- timely identification of the situation and the main subjects (objects) that can realize the specified potential, that is, counteract the realization of national interests;
- clarification of possible losses in a particular area of national security (which are assessed as a low risk for ensuring national security);
- implementation of a number of adequate preventive measures (to block its transformation into a potential threat). That is, this is a situation when the potential has been accumulated, sufficient to counteract the implementation of national interests, but there are no official statements from certain entities or other actions directed against their implementation;

3. Potential threat — a situation where there is an obvious opposition to the achievement of national goals, an obvious intention to cause harm (damage) to national security in the form of official political, economic or other actions without the use of armed struggle, when we can already talk about causing certain harm (damage) to national security. However, its scale does not under any circumstances affect vital national interests (sovereignty, territorial integrity, etc.). The losses (damage) are mainly local in nature, that is, they are a set of conditions that certainly require a response (specific measures) to prevent their negative impact on national security. In the event of a potential threat, state authorities must resort to measures to directly counter the threat in order to prevent its transformation into a real threat. These measures should be adequate to the level of the threat, but in any case, the use of armed force in the combination of means and methods used to protect national interests should be excluded;

4. A real threat is a situation where there is not only an obvious opposition to the achievement of national goals, but also an obvious intention to cause harm (damage) to vital national interests in the form of official or unofficial political, economic and other actions, but without the use of armed means. At the same time, the threat of an armed attack is quite high. We can already talk about causing significant harm (damage) to national security, the scale of which affects vital national interests, but, as a rule, is local in nature. That is, this is a set of conditions that definitely require an immediate response (specific measures) to prevent their further negative impact on national security. In the event of a real threat, state authorities must take active and decisive measures to directly counter the threat in order to prevent it from develop-

ing into a real danger. These measures must be comprehensive, involve all means and methods available to the authorities, but be adequate to the level of the threat and, as a rule, exclude the need to use armed force to protect vital interests.

In the event of a real threat, the harm (losses) to vital national interests does not reach the level where, for example, the integrity of the social, economic or political system is violated or the ability to perform vital functions is lost. Thus, in a situation of a real threat, there is opposition to the implementation of vital national interests, but it is selective and without the use of armed force. At the same time, the threat of using armed means of struggle is quite high (weapons can be used at any moment). There is damage to the implementation of vital interests, but its scale is local;

5. Real danger is a situation where conditions have arisen under which the immediate danger of causing damage (harm) to vital national interests and national values is a reality. In view of this, the state must use all means at its disposal to protect these interests, in particular, means of armed struggle. The integrity of the social system and the state is violated and the possibility of their performance of certain vital functions (partially or completely) is lost.

At the same time, the proposed classification not only identifies any phenomenon (event, process, situation) as a potential or real challenge, a potential or real threat or real danger to national interests and, accordingly, plans and implements a set of measures to form and ensure the effective functioning of the national security system, but can also be used in modeling the process of ensuring national security. It is also important in defining and clarifying the set of national goals and allows us to abandon the traditional attribution to basic regulatory documents in the field of ensuring national security of a rather hypothetical list of potential and real threats to national security, without drawing a clear line between them.

Ensuring national security is one of the main components of public management and administration. The structure of ensuring national security is formed by a set of interconnected and interdependent sub-

jects of ensuring national security (state officials, state authorities and local self-government bodies, state institutions and institutions, forces and means of the security sector, civil society institutions, individual citizens) and mechanisms (institutional, organizational, legal and others) that ensure their coordinated activities on the basis of current legislation [6].

The main goal of ensuring national security is the transformation of national security policy into purposeful coordinated activities of state authorities, public administration, local self-government, and components of the security sector, aimed at realizing national interests, society, and the state.

It is worth noting that even in developed democratic countries, where a significant role in the development and implementation of state and administrative decisions in the security sphere is played by civil society institutions, non-governmental structures that emphasize their main tasks in the sphere of national security, and the media, the main subject in ensuring national security remains state authorities. This is due to the fact that it is the bodies of the legislative, executive and judicial branches of government, using the resources at their disposal, that exercise a legally authoritative influence on public relations that arise in connection with the implementation of national interests.

Conclusions. So, the social phenomenon denoted by the concept of national security is a specific property of the being (existence) of statehood, which reflects the quantitative and qualitative dynamics of its development and at the same time is an integral criterion of its protection from dangers. The choice of ways, means and methods of ensuring national security is determined by the need for timely adoption of measures adequate to the nature and scale of dangers to statehood.

Therefore, we believe that there is a need to analyze and use international experience in ensuring the national security state policy, taking into account their specific conditions and new challenges. It remains important to develop and implement effective measures aimed at real solutions to the main problems of ensuring the national security of our country.

Література

1. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-ІУ1. URL: <https://zakon.rada.gov.ua/laws/show/964-15> (дата звернення: 02.05.2025).
2. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469–19. URL: <https://zakon2.rada.gov.ua/laws/show/2469-19> (дата звернення: 02.05.2025).
3. Ситник Г. П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади) : підруч. Київ : НАДУ, 2012. 544 с.
4. Національна безпека України. *Wikipedia: вебсайт*. URL: <https://uk.wikipedia.org/wiki> (дата звернення: 07.05.2025).
5. Конституція України: станом на 1 верес. 2016 р. *Верховна Рада України*. Харків : Право, 2016. 82 с.
6. Про Раду національної безпеки і оборони України : Закон України від 5 берез. 1998 р. № 183/98-БП1. URL: <https://zakon2.rada.gov.ua/laws/show/183/98-BP1>. (дата звернення: 11.05.2025).

7. Стратегія національної безпеки України : Указ Президента України № 287/2015 від 26 трав. 2015 р. URL: <https://zakon2.rada.gov.ua/laws/show/287/2015>. (дата звернення: 03.05.2025).
8. Ситник Г.П. Формування державно-управлінських рішень: проблеми теорії, методології, практики : монографія. Київ : УАДУ, 2000. 328 с.
9. Цветков В.В. Державне управління: основні фактори ефективності (політико-правовий аспект) : навч. посіб. Харків : Право, 1996. 164 с.
10. Рябов С.Г. Політологічна теорія держави: навч. посіб., 2-е вид. Київ : Тандем, 1996. 240 с.
11. Барабаш Г.О., Луценко Т.О. Організаційно-правові основи державного управління : конспект лекцій. Харків : НУЦЗУ, 2016. 40 с.

References

1. Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy vid 19 cherv. 2003 r. № 964-IU1. URL: <https://zakon.rada.gov.ua/laws/show/964-15>.
2. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21 cherv. 2018 r. № 2469-19. URL: <https://zakon2.rada.gov.ua/laws/show/2469-19>.
3. Sytnyk H.P. Derzhavne upravlinnia u sferi natsionalnoi bezpeky (kontseptualni ta orhanizatsiino-pravovi zasady): pidruch. Kyiv: NADU, 2012. 544 s.
4. Natsionalna bezpeka Ukrainy. *Wikipedia: vebsait*. URL: <https://uk.wikipedia.org/wiki>.
5. Konstytutsiia Ukrainy: stanom na 1 veres. 2016 r. *Verkhovna Rada Ukrainy*. Kharkiv: Pravo, 2016. 82 s.
6. Pro Radu natsionalnoi bezpeky i oborony Ukrainy: Zakon Ukrainy vid berez. 1998 r. № 183/98-VR1. URL: <https://zakon2.rada.gov.ua/laws/show/183/98-VR1>.
7. Stratehiia natsionalnoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy № 287/2015 vid 26 trav. 2015 r. URL: <https://zakon2.rada.gov.ua/laws/show/287/2015>.
8. Sytnyk H.P. Formuvannia derzhavno-upravlinskykh rishen: prob lemy teorii, metodolohii, praktyky: monohrafiia. Kyiv: UADU, 2000. 328 s.
9. Tsvietkov V.V. Derzhavne upravlinnia: osnovni faktory efektyvnosti (polityko-pravovyi aspekt): navch. posib. Kharkiv: Pravo, 2016. 164 s.
10. Riabov S.H. Politolohichna teoriia derzhavy: navch. posib., 2-e vyd. Kyiv: Tandem, 2016. 240 s.
11. Barabash H.O., Lutsenko T.O. Orhanizatsiino-pravovi osnovy derzhavnoho upravlinnia. navch. posib. Kharkiv: NUTsZU, 2016. 40 s.

Стаття надійшла до редакції 26.05.2025

УДК 321:327

Верховцева Ірина Геннадіївна

*доктор історичних наук, професор,
професор кафедри публічного управління та адміністрування
Державний університет інформаційно-комунікаційних технологій*

Verkhovtseva Iryna

*Doctor of Historical Sciences, Professor,
Professor of the Department of Public Management and Administration
State University of Information and Communication Technologies*

ORCID: 0000-0002-5682-993X

Шестаков Валерій Іванович

*доктор технічних наук, доцент, директор
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій
Національна академія Служби безпеки України*

Shestakov Valerii

*Doctor of Technical Sciences, Associate Professor,
Director of the Educational and Research Institute of
Information Security and Strategic Communications
National Academy of the Security Service of Ukraine*

ORCID: 0000-0002-5918-5121

Гребенюк Віталій Миколайович

*доктор юридичних наук, старший дослідник,
директор Центру стратегічних комунікацій
Національна академія Служби безпеки України*

Grebenyuk Vitaliy

*Doctor of Law, Senior Researcher,
Director of the Centre for Strategic Communications
National Academy of the Security Service of Ukraine*

ORCID: 0000-0002-5169-8694

Гайдук Олег Васильович

*радник
Міністерство закордонних справ України*

Gaiduk Oleg

*Advisor
Ministry of Foreign Affairs of Ukraine*

ORCID: 0000-0003-4740-7759

DOI: 10.25313/2617-572X-2025-5-10991

**НОВІТНЯ ТЕРМІНОЛОГІЯ У ДИПЛОМАТИЧНИХ
ПРАКТИКАХ ЯК МАРКЕР КІБЕРВПЛИВІВ:
ЦИФРОВА ДИПЛОМАТІЯ, КІБЕРДИПЛОМАТІЯ**

**THE LATEST TERMINOLOGY IN DIPLOMATIC
PRACTICES AS A MARKER OF CYBER INFLUENCE:
DIGITAL DIPLOMACY, CYBER DIPLOMACY**

Анотація. Вступ. У статті аналізується змістове наповнення термінів «цифрова дипломатія» та «кібердипломатія», що нині активно застосовуються в наукових студіях для позначення нових практик у дипломатичних комунікаціях. Звертається увага на те, що їх кіберизація створила ситуацію інтенсивного пошуку адекватних відповідників новим комунікаційним явищам та подеколи наявність суперечливих позицій дослідників у застосуванні новітньої термінології.

Мета статті: на основі змістовного аналізу термінів «цифрова дипломатія» та «кібердипломатія», що застосовуються у науковій літературі, з'ясувати їх відповідність / невідповідність та можливість взаємозамінності.

Матеріали і методи. Базою дослідження стали публікації вітчизняних науковців, у яких аналізується практика застосування термінів «цифрова дипломатія» та «кібердипломатія» в контексті кіберизації дипломатичних комунікацій. Під час студіювання проблеми автори послуговувались методами загальнонауковими (логіки, аналізу, синтезу, дедукції, індукції) та спеціальними (порівняльним, структурно-функціонального аналізу, термінологічним, нарративним тощо). Це дозволило розглянути проблему в контексті загального й частного у визначенні сфери застосування розглядуваних термінів, з'ясувати відмінності між ними у рамках змістовного наповнення кожного, виявити специфіку позначення даними термінами відповідних явищ та поєднати результати дослідження в нарратив у відповідності із логічним методом наукового пошуку.

Результати. Наголошено, що перенесення переважної більшості публічних комунікацій у кіберпростір та якісне оновлення відповідного цифрового інструментарію зумовили ситуацію інтенсивного пошуку адекватних понять і термінів для її опису. З'ясовано, що терміни «цифрова дипломатія» та «кібердипломатія» фактично позначають нові дипломатичні практики, які реалізуються за допомогою кіберкомунікацій, тобто в цифровому форматі, але в науковій літературі зустрічаються різні тлумачення цих термінів через те, що деякі дослідники ототожнюють ці поняття. Зазначено, що більшість науковців вважають, що кібердипломатія є значно ширшим поняттям, ніж цифрова дипломатія, і охоплює всю сферу дипломатичних відносин у кіберпросторі, а сфера застосування терміна «цифрова дипломатія» пов'язана з використанням цифрових інструментів у дипломатичній діяльності. Підсумовано, що, оскільки кіберкомунікації наразі є домінуючими каналами міжнародних публічних комунікацій, кібердипломатія, відповідно, представляє практично всю сферу міжнародних публічних відносин.

Перспективи. Подальше студіювання проблеми може відбуватись у напрямі деталізації застосування термінологічного методу в студіях з вивчення новітніх дипломатичних практик як складника міжнародних публічних комунікацій за умов їх кіберизації.

Ключові слова: кіберпростір, цифровізація комунікацій, кібердипломатія, цифрова дипломатія, Iphone-дипломатія.

Summary. Introduction. The article analyses the content of the terms 'digital diplomacy' and 'cyber diplomacy', which are currently actively used in academic studies to refer to new practices in diplomatic communications. The author emphasises that their cyberisation has created a situation of intensive search for adequate responses to new communication phenomena and sometimes contradictory positions of researchers in the use of the latest terminology.

The purpose of the article is to determine, on the basis of a substantive analysis of the terms 'digital diplomacy' and 'cyber diplomacy' used in the scientific literature, their correspondence/inconsistency and the possibility of interchangeability.

Materials and Methods. The research is based on the publications of domestic scholars analysing the practice of using the terms 'digital diplomacy' and 'cyber diplomacy' in the context of cyberisation of diplomatic communications. In studying the problem, the authors used general scientific methods (logic, analysis, synthesis, deduction, induction) and special methods (comparative, structural and functional analysis, terminological, narrative, etc.) This made it possible to consider the problem in the context of the general and the particular in determining the scope of the terms under consideration, to clarify the differences between them within the content of each, to identify the specifics of the relevant phenomena denoted by these terms and to combine the research results into a narrative in accordance with the logical method of scientific research.

Results. The transfer of the vast majority of public communications to cyberspace and the qualitative upgrade of the relevant digital tools have led to an intensive search for adequate concepts and terms to describe it. The terms 'digital diplomacy' and 'cyber diplomacy' actually refer to new diplomatic practices implemented through cyber communications, i.e. in a digital format. However, in the academic literature, there are different interpretations of these terms. Some researchers equate these concepts. However, the majority of scholars believe that cyber diplomacy is a much broader concept than digital diplomacy and covers the entire sphere of diplomatic relations in cyberspace. Instead, the scope of the term 'digital diplomacy' is associated with the use of digital tools in diplomatic activities. Since cyber communications are now the dominant channels of international public communications, cyber diplomacy, accordingly, represents almost the entire sphere of international public relations.

Prospects. Further study of the problem can be carried out in the direction of detailing the application of the terminological method in the study of modern diplomatic practices as a component of international public communications in the context of their cyberization.

Key words: cyberspace, digitalisation of communications, digital diplomacy, cyber diplomacy, iPhone diplomacy.

Постановка проблеми. Зумовлені якісними змінами технічного характеру та підвищенням загального рівня технологізації, а також персоналізацією і демасифікацією масових комунікацій, лег-

кість та специфіка нових дипломатичних практик останніх десятиліть якісно впливають на характер та структурні зміни взаємин між урядами, політичними акторами, наддержавними структурами, широки-

ми колами громадськості різних країн, сприяючи залученню до спілкування горизонтальних мереж користувачів. Цифровізація міжнародних комунікацій у їх дипломатичному сегменті через надання громадськості інструментів впливу на свої уряди та створенням можливостей комунікацій із зарубіжною громадськістю інших країн суттєво впливає на порядок денний світової політики. З-поміж іншого, в наукових студіях це висуває завдання термінологічного характеру, а саме: які власне терміни з різноманіття застосованих у практиці дипломатичної комунікації у віртуальному просторі (кіберпросторі) найбільше відповідають опису сучасної ситуації, зумовленої кіберизацією міжнародних публічних комунікацій. Зокрема, чи відповідниками є терміни «цифрова дипломатія» (Digital Diplomacy / ЦД) та «кібердипломатія» (Cyberdiplomacy / КД), що застосовуються в наукових студіях, або навпаки — кожним з них позначається окрема сфера дипломатичних комунікацій.

Аналіз останніх досліджень і публікацій. Стан наукової розробки проблеми свідчить про те, що розроблялась вона фрагментарно, хоча вказані нові дипломатичні практики потрапили до фокусу уваги дослідників. У цьому контексті слід вказати на розвідки вітчизняних науковців, зокрема, О. Висоцького [2; 3]; О. Гайдука [4–7]; В. Гребенюк [8]; В. Матвієнка та Г. Петушкової [9]; Т. Мірошниченко й Г. Федорової [11]; О. Полякова [12]; О. Русової [22]; О. Сегеди [13]; В.Ціватого [14], а також зарубіжних вчених А. Ататффа, К. Ренода, С. Паоліба [18], А. Баринхи й Т. Ренарда [19]; К. Б'йолі та М. Холмс [20], Г. Христосу [21]; Р. Робінсона [23]. Однак аспекти взаємовідповідності / невідповідності понять «цифрова дипломатія» та «кібердипломатія» досі не стали предметом спеціального дослідження.

Мета статті. Не претендуючи на всебічний розгляд проблеми, метою даної розвідки визначаємо: на основі змістовного аналізу термінів «цифрова дипломатія» та «кібердипломатія», що циркулюють у науковій літературі, з'ясувати їх відповідність / невідповідність та визначити причини, якими це зумовлюється.

Виклад основного матеріалу. Кіберпростір (буквально — «надпростір») є новим простором людського буття (перші чотири — земля, вода, повітря, космос), породженим техніко-технологічними новачками останнього півстоліття. Він функціонує у взаємодії з людським інтелектом та формує особливий — «інформаційний», спосіб життя. Людство вчиться розбудовувати комунікації в ньому та жити за таких нових умов загалом. Зокрема, завдяки новітнім цифровим технологіям у міжнародних комунікаціях створюються умови для інтеграції глобального інформаційного простору, урізноманітнення форм відповідної взаємодії, зумовлених, зокрема, залученням до міжнародних публічних взаємин широких кіл громадськості. Але зворотнім боком стало поширення кіберзагроз, зневажливе ставлення деяких між-

народних акторів до міжнародно-правових норм (насамперед таке характеризує автократії), загострення геополітичного суперництва тощо. Серед якісно нових явищ, що впливають на глобальні комунікації слід вказати і на широке застосування цифрових технологій у дипломатичній практиці — як традиційного формату, так і публічно-дипломатичного, відповідно [1, с. 229–232].

На позначення таких нових практик у вітчизняному науковому полі фігурують поняття «цифрова дипломатія» та «кібердипломатія» і вживаються відповідні терміни. Обидва активно застосовуватись стали порівняно нещодавно, як, власне, і самі явища, позначені цими термінами. І якщо термін «цифрова дипломатія» у науковців не викликає сумнівів щодо його потрактування — воно пов'язується із застосуванням у дипломатичній діяльності цифрового інструментарію [11, с. 59–63; 13, с. 143–144; 15, с. 108–109]), то терміном «кібердипломатія», що тільки входить до широкого вжитку й поки не отримав чіткої конфігурації, в науковій літературі можуть позначатись і явище ЦД, і інші нові формати дипломатичної діяльності: електронна дипломатія, медіадипломатія, нет-дипломатія, Iphone-дипломатія тощо [2; 3].

У вітчизняному науковому просторі одним із перших у 2020 р. надав тлумачення терміну «цифрова дипломатія» О. Висоцький. Зокрема, він вказав, що ЦД є продовженням і розширенням публічної дипломатії, але в іншому контексті реальності, в глобально-інформаційному світі мережі Інтернет. У цьому ключі дослідник наголосив на взаємозамінності, на його погляд, термінів «цифрова дипломатія» та «кібердипломатія» та на специфіці публічно-дипломатичних практик у контексті цифровізації комунікацій в світовому інформаційному просторі, розглядаючи при цьому КД як один із сегментів/варіацій публічної дипломатії [2, с. 16–17]. Практично водночас із О. Висоцьким О. Русова, застосовуючи обидва терміни під час аналізу сучасних міждержавних взаємин та вказуючи на вагомість інструментарію обох дипломатичних практик у забезпеченні цифрового суверенітету країн, відрізняє їх і наголошує на інноваційному характері КД у репрезентації національних інтересів. Дослідниця кібердипломатичну діяльність пов'язує із широким спектром публічно-політичних взаємин, а ЦД нею застосовується суто в інструментальному аспекті цих взаємин [22, с. 27–30].

Наступна хвиля прискіпливої уваги українських науковців до кібердипломатії датується 2024–2025 роками. Зумовлено це початком інтенсивної розробки вітчизняної Стратегії кібердипломатії. В. Матвієнко та Г. Петушкова в 2024 р. у своїй статті зацентрували на технологічних аспектах цифрової дипломатії й значно ширшому потрактуванні кібердипломатії як дипломатичної практики, що застосовується до кіберпростору загалом. Кібердипломатію на національному рівні ці дослідники визначають як

використання дипломатичних інструментів та ініціатив для забезпечення інтересів держави в кіберпросторі. Завданнями для дипломатичного агента в цьому контексті ці вчені визначають: встановлення зв'язку та діалогу між державними і недержавними суб'єктами на різному рівні; запобігання кібергонитві; розбудова глобальних норм у кіберпросторі тощо. З огляду на це, кібердипломатія, як вказують науковці, ґрунтується на вимірах м'якої сили та є ефективною практикою для пом'якшення невизначеності, усунення ризиків і потенційних конфліктів, що походять із кіберпростору. Фундаментальними елементами КД є збільшення кіберпотенціалу, зміцнення довіри, дотримання та розвиток кібернорм. Це, як вважають учені, зумовлює необхідність переосмислення ролі дипломатів, реорганізації департаментів і загалом міністерств закордонних справ, щоби задовольнити щораз більшу потребу у фахівцях із питань кібербезпеки в реалізації завдань зовнішньої політики та переосмислити роль нових технологій у сучасних міжнародних відносинах [9, с. 697–698].

О. Гайдук у своїх публікаціях, аналізуючи потенціал кібердипломатії, наголошує на викликах кіберпростору традиційним формулюванням поведінки держави у поводженні із ризиками та необхідності врахування кібердипломатією цих факторів. Учений вказує, що за пропозицією Міністерства закордонних справ України, визначення кібердипломатії ґрунтується на її концепті як нового виду дипломатичної діяльності, сфокусованої на просуванні та захисті національних інтересів України у кіберпросторі. КД також включає реалізацію зовнішньополітичних цілей у цифровому середовищі, встановлення й підтримку в кіберпросторі дипломатичних зв'язків з іншими державами, їх об'єднаннями та міжнародними організаціями. Вона надає традиційній дипломатії нові інструменти, охоплює міжнародну співпрацю у сфері кібербезпеки та кіберзахисту, а також розвиває нові спільні проекти, які сприяють зміцненню міжнародної стабільності й безпеки у цифровому світі. Науковець вважає, що цифрова та кібердипломатія хоч і доповнюють одна іншу, проте мають різні фокуси: перша зосереджена на комунікаційних та іміджевих завданнях дипломатії, а друга — на захисті та регулюванні кіберпростору як окремої сфери міжнародних відносин. Дослідження взаємодії між цими напрямками є важливим для формування комплексної дипломатичної стратегії держави в епоху цифрових технологій і постійно зростаючих кіберзагроз [4–7]. У цьому ж ключі в спільній розвідці О. Гайдук із В. Шульгою, С. Корченком, Є. Іванченко вказується, що КД є інструментом забезпечення міжнародної кібербезпекової стабільності в цифровому світі [15].

Інший вимір тлумачення поняття кібердипломатії представлений у розвідках О. Хіміча, С. Корченка, І. Верховцевої, які аналізують публічно-дипломатичний відподвійний сегмент і, зокрема, її

потенціал у протидії гібридним загрозам, інформаційній агресії та інформаційному насиллю. На думку вказаних науковців, КД у її соціокомунікаційних аспектах є потужним інструментом розробки відповідних стратегій протидії деструктивним масовоінформаційним впливам [1; 14; 16; 24].

Дослідник В. Гребенюк вдався до аналізу нормативно-правового забезпечення КД та наголосив, що вона призначена забезпечувати захист інтересів національних держав та сприяти глобальній стабільності й розвитку, колективній безпеці у кіберпросторі, врегульовувати міжнародні відносини у цій сфері [8].

В. Шестаков і Ю. Даник, студіюючи вектор кібердипломатичних практик, пов'язаний із застосуванням штучного інтелекту, акцентують тому, що цей напрям є інноваційним та надзвичайно актуальним [16].

Як бачимо, позиції вітчизняних дослідників щодо трактування ЦД і КД не збігаються. Є поодинокі візії щодо їх взаємозамінності, які науковою спільнотою у своїй масі не підтримуються. Натомість переважна більшість науковців розглядають ці явища та відповідні терміни як такі, що мають споріднені, проте різні сфери застосування. ЦД, за визначенням українських науковців, акцентує на комунікаційному інструментарії дипломатичних практик, а не на змісті або сфері політики. КД — поняття значно ширше та охоплює всю сферу дипломатичних взаємин у кіберпросторі. Оскільки нині саме кіберкомунікації є домінуючими каналами міжнародних публічних комунікацій, кібердипломатія, відповідно, репрезентує практично всю сферу міжнародних публічних взаємин за умов їх еіберизації.

Таке трактування принципово відповідає візіям західних дослідників на явища ЦД і КД. Приміром, за визначенням К. Б'юлі та М. Холмс (Oxford), ЦД — це використання цифрових технологій, зокрема соціальних медіа, big data, аналітики, інструментів візуалізації, штучного інтелекту тощо, для реалізації зовнішньополітичних цілей. Це продовження та трансформація публічної дипломатії (public diplomacy) із фокусуванням на інструментах комунікації та взаємодії з іноземною аудиторією, а не на змістовних аспектах політики [20]. Натомість КД, як вказано у дослідженнях Дж. Христоу, — це дипломатична сфера, що займається міжнародними аспектами кіберкомунікацій, безпекою та правовим регулюванням кіберпростору, включно із питаннями кібербезпеки, довіри, розробки норм відповідальної поведінки держав у кіберпросторі, управління Інтернетом та взаємодії в межах діяльності, приміром, таких організацій, як GGE (експертна група з питань глобальної політики), OEWE (група, що спостерігає за довкіллям), ITU (Міжнародний Союз електрозв'язку), ICANN (Корпорація з управління доменними іменами та номерами), що працюють у сфері глобальної комунікації [21].

Інший зарубіжний науковець Р. Робінсон вважає, що КД має розглядатись як рівноправна та важлива частина ширшого і цілісного інструментарію державної політики кібербезпеки. На думку цього вченого, КД є продовженням дипломатії в більш широкому сенсі, яка сама по собі є сферою, що зазнала суттєвих змін, щоби адаптуватись до нових умов і вирішити нагальні проблеми нашого часу, такі, як зміна клімату й використання космосу в рамках постліберального й дедалі більш хаотичного світового порядку за умов розширення та поглиблення процесів, масштабів і залучених акторів, а також трансформації способів дипломатії у багатосторонньому 2.0-світі XXI-го століття [23].

А. Баринха та Т. Ренард визначають КД як дипломатію в кіберпросторі або, іншими словами, виконання дипломатичних функцій із використанням дипломатичних ресурсів для забезпечення національних інтересів у кіберпросторі. При цьому домінуючими питаннями порядку денного КД є кібербезпека, кіберзлочинність, розбудова довіри, свобода Інтернету та управління Інтернетом. При цьому КД твердо позиціонується як міжнародний суспільний інститут, що передбачає взаємодію з акторами світового суспільства [19]. А. Атататфаа, К. Ренод, С. Паоліб, наголошують на тому, що кібердипломатична діяльність пов'язана з широким спектром

проблем, які вона покликана вирішувати, в тому числі із проблемами «нетехнічного» характеру [18].

Отже, КД — це предметно-орієнтована політика, що реалізовується у кіберпросторі та має як технічний, так і соціально-комунікаційний, виміри, а ЦД репрезентує суто інструментальну сферу дипломатичної діяльності.

Висновки та перспективи подальших досліджень. Узагальнюючи викладене, слід наголосити: на погляд більшості дослідників, цифрова дипломатія акцентує на технологічних аспектах комунікаційних практик публічно-дипломатичної діяльності. Кібердипломатія є поняттям значно ширшим, аніж цифрова дипломатія, та реперезентує сферу предметно-орієнтованої політики, що реалізовується у кіберпросторі та включає весь комплекс дипломатичних заходів. При цьому кібердипломатія має як технологічний вимір, так і суто публічно-дипломатичний, пов'язаний з відповідними комунікаційними соціального характеру, репрезентуючи практично всю сферу міжнародних публічних взаємин у кіберпросторі.

Подальше студіювання проблеми може відбуватись у напрямі деталізації застосування термінологічного методу в студіях з вивчення новітніх дипломатичних практик як складника міжнародних публічних комунікацій за умов їх кіберизації.

Література

1. Верховцева І. Г. Глобальний кіберпростір та опір інформаційній агресії: кібердипломатія України у протидії російській інформаційній інвазії. *Міжнародне співтовариство та Україна в процесах економічного та цивілізаційного поступу: актуальні економіко-технологічні, ресурсні, інституціональні, безпекові та соціогуманітарні проблеми* : монографія. Ryga: Baltija Publishing, 2024. С. 213–243. <https://doi.org/10.30525/978-9934-26-480-1-9>.
2. Висоцький О. Ю. Публічна дипломатія : конспект лекцій: у 2 ч. Ч. І. Дніпро : СПД «Охотнік», 2020. 56 с.
3. Висоцький О. Iphone-дипломатія президента України в контексті новацій української цифрової дипломатії під час широкомасштабної російської агресії. *Україна і світ: теоретичні та практичні аспекти діяльності у сфері міжнародних відносин* : матер. Міжнар. наук.-практ. конф., м. Київ, 11–12 квіт. 2024 р. Київ : Вид. центр КНУКіМ, 2024. С. 17–22.
4. Гайдук О. В., Зверев В. П. Ігрові індекси в інформаційних технологіях забезпечення міжнародних комунікацій: кіберстійкість, кіберпотужність та кібербезпека. *Сучасний захист інформації*. 2025. № 1(61). 44–59. DOI: 10.31673/2409-7292.2025.016955.
5. Гайдук О. В. Кібердипломатія: нові горизонти дипломатичної діяльності у цифровому світі. *Кібердипломатія*: матер. Міжнар. наук.-практ. конфер. (м. Київ, 15–16 травня 2024 року), Наук.-практ. круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року). Київ : Дип. акад. ім. Г. Удовенка; ДУІКТ, 2025. С. 6–8.
6. Гайдук О. В. Кібердипломатія: нові напрями розвитку в цифрову епоху. *Кібердипломатія*: матер. Міжнар. наук.-практ. конфер. (м. Київ, 15–16 травня 2024 року), Наук.-практ. круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року). Київ : Дип. академія ім. Г. Удовенка; ДУІКТ, 2025. С. 23–25.
7. Гайдук О. В. Кібердипломатія як парадигма нового підходу до міжнародних відносин: досвід країн світу, науково-академічні практики та кібербезпека міжнародних комунікацій. *Стратегічні комунікації в умовах війни: погляд від волонтера до науковця*: монографія. Київ : 7БЦ, 2024. С. 421–431.
8. Гребенюк В. М. Нормативно-правове забезпечення кібердипломатії: структура та основні функції. *Кібердипломатія* : матер. Міжнар. наук.-практ. конфер. (м. Київ, 15–16 травня 2024 року), Наук.-практ. круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року). Київ : Дип. академія ім. Г. Удовенка; ДУІКТ, 2025. С. 86–90.

9. Матвієнко В., Петушкова Г. Кібердипломатія в Європейському Союзі: модель естонської кібердипломатії та досвід України. *Україна дипломатична*. 2024. Вип. 24. С. 696–708.
10. МЗС розробляє Стратегію кібердипломатії України — заступник міністра. 15.05.2024. URL: <https://www.ukrinform.ua/rubric-polytics/3863944-mzs-rozroblae-strategiu-kiberdiplomatii-ukraini-zastupnik-ministra.html> (дата звернення 5.05.2025)
11. Мірошниченко Т., Федорова Г. Цифрова дипломатія як сучасний комунікаційний інструмент міжнародних відносин. *Науково-теоретичний альманах Грани*. 2022. № 24(12). С. 58–65.
12. Поляков О. М. Кібердипломатія як важливий напрямок міжнародно-правового співробітництва в умовах режиму воєнного стану. *Нове українське право*. 2024. № 6. С. 70–76.
13. Сегеда О. Цифрова дипломатія України як елемент нової публічної дипломатії. *Науковий журнал «Політикус»*. 2020. Вип. 3. С. 139–147.
14. Хімич О. М., Корченко О. Г., Верховцева І. Г. Кібердипломатія у протидії антиукраїнській пропаганді: стратегії, інструменти. *Кібердипломатія: тези Міжнар. наук.-практ. конф. (24–25 травня 2024 р.) та наук.-практ. кругл. столу «Стратегії та практики для України, Європи та світу» (28 листопада 2024 р.) / за заг. ред. О. Г. Корченка; упоряд. І. Г. Верховцева, О. В. Гайдук. К. : Дипл. акад. імені Г. Удовенка; ДУІКТ, 2025. С. 95–102.*
15. Циватий В. Цифрова дипломатія України: інноваційний, безпековий та міжнародно-політичний дискурси (синергія реального і віртуального). *Цифрова дипломатія України: синергія реального і віртуального: матер. Міжнар. наук. конфер. Львів, 24 листопада 2023 р. Львів : ЛНУ імені Івана Франка, 2023. С. 108–112.*
16. Шестаков В. І., Даник Ю. Г. Особливості оцінювання ризиків впливу штучного інтелекту на дипломатичну сферу. *Кібердипломатія: матер. Міжнар. наук.-практ. конфер. (м. Київ, 15–16 травня 2024 року), Наук.-практ. круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року). Київ: Дип. академія ім. Г. Удовенка; ДУІКТ, 2025. С. 64–66.*
17. Шульга В. П., Корченко О. Г., Іванченко Є. В., Гайдук О. В. Кібердипломатія як інструмент забезпечення міжнародної кібербезпекової стабільності в цифровому світі. *Кібердипломатія: матер. Міжнар. наук.-практ. конфер. (м. Київ, 15–16 травня 2024 року), Наук.-практ. круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року). Київ : Дип. академія ім. Г. Удовенка; ДУІКТ, 2025. С. 48–56.*
18. Attatfaa A., Renauda K., Paolib De S. Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*. 2020. Vol. 176. P. 60–69. DOI: 10.1016/j.procs.2020.08.007.
19. Barrinha A., Renard T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs*, 3(4–5), 353–364. doi: 10.1080/23340460.2017.1414924.
20. Bjola C., Holmes M. (2015). Digital Diplomacy Theory and Practice. <https://doi.org/10.4324/9781315730844>; URL: <https://www.taylorfrancis.com/books/edit/10.4324/9781315730844/digital-diplomacy-corneliu-bjola-marcus-holmes> (дата звернення 05.05.2025).
21. Christou G. (2024). Cyber Diplomacy: From Concept to Practice. *Tallinn Paper*. Vol. 14. URL: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf (дата звернення 05.05.2025).
22. Rusova O. (2020). Cyber diplomacy: an intangible reality or a fait accompli? *UA: Ukraine Analytica*. 2(20). P. 26–33.
23. Robinson, R. Cyber Diplomacy: A New Frontier in International Relations and Professional Practice. *EDRM*. URL: <https://edrm.net/2024/06/cyber-diplomacy-a-new-frontier-in-international-relations-and-professional-practice/> (дата звернення 5.05.2025).
24. Verkhovtseva I. G. Ukraine's Cyber Diplomacy In Countering Russian Informational Aggression. *Library Science. Record Studies. Informology*. 2024. Vol. 20(3). P. 21–31. <https://doi.org/10.63009/lrsi/3.2024.21>.

References

1. Verkhovtseva, I. G. (2024). Hlobal'nyy kiberprostrir ta opir informatsijnij ahresii: kiberdyplomatiia Ukrainy u protydyi rosijs'kij informatsijnij invazii ahresii [Global Cyberspace and Resistance to Information Aggression: Ukraine's Cyber Diplomacy in Countering Russian Information Invasion]. In *Mizhnarodne spivtovarystvo ta Ukraina v protsesakh ekonomichnoho ta tsyvilizatsijnoho postupu: aktual'ni ekonomiko-tehnologichni, resursni, instytutsional'ni, bezpekovi ta sotsiohumitarni problemy: monohrafiia* (pp. 213–243). Ryga: Baltija Publishing. <https://doi.org/10.30525/978-9934-26-480-1-9> [in Ukrainian].
2. Vysots'kyj, O. Yu. (2020). Publichna dyplomatiia: konspekt lektzij [Public diplomacy: lecture notes]: u 2 ch. Ch. I. Dni-pro: SPD "Okhotnik" [in Ukrainian].
3. Vysots'kyj, O. Yu. (2024). Iphone-dyplomatiia prezidenta Ukrainy v konteksti novatsij ukrains'koi tsyvrovoi dyplomatii pid chas shyrokomasshtabnoi rosijs'koi [The iPhone Diplomacy of the President of Ukraine in the Context of Innovations of Ukrainian Digital Diplomacy during the Large-Scale Russian Aggression]. In *Ukraina i svit: teoretychni ta praktychni aspekty diial'nosti u sferi mizhnarodnykh vidnosyn: mater. Mizhnar. nauk.-prakt. konf., m. Kyiv, 11–12 kvit. 2024 r. (pp. 17–22). Kyiv: Vyd. tsentr KNUKiM*. [in Ukrainian].
4. Hajduk O. V., Zvieriev V. P. (2025). Ihrovi indeksy v informatsijnykh tekhnolohiiakh zabezpechennia mizhnarodnykh komunikatsij: kiberstijkist', kiberpotuzhnist' ta kiberbezpeka [Game indices in information technologies for inter-

national communications: cyber resilience, cyber power and cybersecurity]. *Suchasnyj zakhyst informatsii*, 1(61), 44–59. DOI: 10.31673/2409-7292.2025.016955 [in Ukrainian].

5. Hajduk, O. V. (2025). Kiberdyplomatiia: novi horyzonty dyplomatychnoi diial'nosti u tsyfrovomu sviti [Cyber diplomacy: new horizons of diplomatic activity in the digital world]. In *Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) (pp. 6–8). Kyiv: Dypl. akad. im. H. Udovenka; DUIKT [in Ukrainian].

6. Hajduk, O. V. (2025). Kiberdyplomatiia: novi napriamy rozvytku v tsyfrovu epokhu [Cyber diplomacy: new directions of development in the digital age]. In *Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) (pp. 23–25). Kyiv: Dypl. Akad. im. H. Udovenka; DUIKT [in Ukrainian].

7. Hajduk, O. V. (2024). Kiberdyplomatiia iak paradyhma novoho pidkходу do mizhnarodnykh vidnosyn: dosvid krain svitu, naukovo-akademichni praktyky ta kiberbezpeka mizhnarodnykh komunikatsij [Cyberdiplomacy as a paradigm of a new approach to international relations: experience of countries, scientific and academic practices and cybersecurity of international communications]. In *Stratehichni komunikatsii v umovakh vijny: pohliad vid volontera do naukovtsia: monohrafiia* (pp. 421–431). Kyiv: 7BTs [in Ukrainian].

8. Hrebenuk, V. M. (2025). Normatyvno-pravove zabezpechennia kiberdyplomatii: struktura ta osnovni funktsii [Regulatory and legal support of cyber diplomacy: structure and main functions]. In *Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) (pp. 86–90). Kyiv: Dypl. akad. im. H. Udovenka; DUIKT [in Ukrainian].

9. Matviienko, V., Petushkova, H. (2024). Kiberdyplomatiia v Yevropejs'komu Soiuzi: model' estons'koi kiberdyplomatii ta dosvid Ukrainy [Cyber diplomacy in the European Union: the Estonian model of cyber diplomacy and Ukraine's experience]. *Ukraina dyplomatychna*, 24, 696–708 [in Ukrainian].

10. MZS rozrobiaie Stratehiu kiberdyplomatii Ukrainy, — zastupnyk ministra [MFA is developing Ukraine's cyber diplomacy strategy, — Deputy Minister]. 15.05.2024. URL: <https://www.ukrinform.ua/rubric-politics/3863944-mzs-rozroblaie-strategiu-kiberdyplomatii-ukraini-zastupnik-ministra.html> [in Ukrainian].

11. Miroshnychenko, T., Fedorova, H. (2022). Tsyfrova dyplomatiia iak suchasnyj komunikatsijnyj instrument mizhnarodnykh [Digital diplomacy as a modern communication tool for international relations]. *Naukovo-teoretychnyj al'manakh Hrani*, 24(12), 58–65 [in Ukrainian].

12. Poliakov, O. M. (2024). Kiberdyplomatiia iak vazhlyvyj napriamok mizhnarodno-pravovoho spivrobotnytstva v umovakh rezhymu voiennoho stanu [Cyberdiplomacy as an important area of international legal cooperation under martial law]. *Nove ukrains'ke pravo*, 6, 70–76 [in Ukrainian].

13. Sehed, O. (2020). Tsyfrova dyplomatiia Ukrainy iak element novoi publichnoi dyplomatii [Ukraine's digital diplomacy as an element of a new public diplomacy]. *Naukovyj zhurnal "Politikus"*, 3, 139–147 [in Ukrainian].

14. Khimich, O. M., Korchenko, O. H., & Verkhovtseva, I. G. (2025). Kiberdyplomatiia u protydiv antyukrains'kij propahandi: stratehii, instrumenty [Cyber diplomacy in countering anti-Ukrainian propaganda: strategies, tools]. In *Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) (pp. 96–102). Kyiv: Dypl. akad. im. H. Udovenka; DUIKT [in Ukrainian].

15. Tsivatyj, V. (2023). Tsyfrova dyplomatiia Ukrainy: innovatsijnyj, bezpekovyj ta mizhnarodno-politychnyj dyskursy (synerhiia real'noho i virtual'noho) [Ukraine's digital diplomacy: innovation, security and international political discourses (synergy of real and virtual)]. In *Tsyfrova dyplomatiia Ukrainy: synerhiia real'noho i virtual'noho: mater. Mizhnar. nauk. konfer. L'viv, 24 lystopada 2023 r.* (pp. 108–112). L'viv: LNU imeni Ivana Franka [in Ukrainian].

16. Shestakov V. I., Danyk Yu. H. (2025). Osoblyvosti otsiniuvannia ryzykiv vplyvu sztuchnoho intelektu na dyplomatychnu sferu [Peculiarities of Assessing the Risks of Artificial Intelligence Impact on the Diplomatic Sphere]. In *Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) (pp. 64–66). Kyiv: Dypl. akad. im. H. Udovenka; DUIKT [in Ukrainian].

17. Shulha, V. P., Korchenko, O. H., Ivanchenko, Ye. V., & Haiduk, O. V. (2025). Kiberdyplomatiia yak instrument zabezpechennia mizhnarodnoi kiberbezpekovoї stabilnosti v tsyfrovomu sviti [Cyber diplomacy as a tool for ensuring international cybersecurity stability in the digital world]. In *Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) (pp. 48–56). Kyiv: Dypl. akad. im. H. Udovenka; DUIKT [in Ukrainian].

18. Attatfaa, A., Renauda, K., Paolib, & De S. (2020). Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*, 176, 60–69. DOI: 10.1016/j.procs.2020.08.007.

19. Barrinha, A., Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs*, 3(4–5), 353–364. doi: 10.1080/23340460.2017.1414924.

-
20. Bjola, C., Holmes, M. (2015). Digital Diplomacy Theory and Practice. URL: <https://www.taylorfrancis.com/books/edit/10.4324/9781315730844/digital-diplomacy-corneliu-bjola-marcus-holmes>; <https://doi.org/10.4324/9781315730844>.
21. Christou, G. (2024). Cyber Diplomacy: From Concept to Practice. *Tallinn Paper*. Vol. 14. URL: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf.
22. Rusova, O. (2020). Cyber diplomacy: an intangible reality or a fait accompli? *UA: Ukraine Analytica*, 2(20), 26–33.
23. Robinson, R. Cyber Diplomacy: A New Frontier in International Relations and Professional Practice. *EDRM*. URL: <https://edrm.net/2024/06/cyber-diplomacy-a-new-frontier-in-international-relations-and-professional-practice/> (дата звернення 5.05.2025).
24. Verkhovtseva, I. G. (2024). Ukraine's Cyber Diplomacy In Countering Russian Informational Aggression. *Library Science. Record Studies. Informology*, 20(3), 21–31. <https://doi.org/10.63009/lrsi/3.2024.21>.

Стаття надійшла до редакції 23.05.2025

УДК 327.7:351

Кондратюк Сергій Володимирович

*кандидат політичних наук,
професор кафедри публічного управління та адміністрування
Державний університет інформаційно-комунікаційних технологій*

Kondratiuk Serhii

*Candidate of Political Sciences,
Professor of the Department of Public Management and Administration
State University of Information and Communication Technologies
ORCID: 0009-0000-2354-8763*

Верховцева Ірина Геннадіївна

*доктор історичних наук, професор,
професор кафедри публічного управління та адміністрування,
Державний університет інформаційно-комунікаційних технологій*

Verkhovtseva Iryna

*Doctor of Historical Sciences, Professor,
Professor of the Department of Public Management and Administration
State University of Information and Communication Technologies
ORCID: 0000-0002-5682-993X*

Закіров Марат Борисович

*доктор політичних наук, доцент,
завідувач відділу політологічного аналізу
Національна бібліотека України імені В.І. Вернадського*

Zakirov Marat

*Doctor of Political Science, Associate Professor,
Head of the Department of Political Analysis
V.I. Vernadsky National Library of Ukraine
ORCID: 0000-0003-4897-4325*

Кондратенко Олег Юрійович

*доктор політичних наук, доцент,
професор кафедри філософії, соціології та політології
Державний торговельно-економічний університет*

Kondratenko Oleh

*Doctor of Political Sciences, Associate Professor,
Professor of the Department of Philosophy, Sociology and Political Science
State University of Trade and Economics
ORCID: 0000-0002-1905-934X*

Любченко Андрій Володимирович

*кандидат наук з державного управління,
докторант кафедри публічного управління та адміністрування
Державний університет інформаційно-комунікаційних технологій*

Lyubchenko Andrii

*PhD in Public Administration,
Doctoral student of the Department of Public Management and Administration
Державний університет інформаційно-комунікаційних технологій
ORCID: 0009-0004-0246-7795*

Хорватова Оксана Олегівна

*кандидат юридичних наук, доцент
доцент кафедри публічного управління та адміністрування
Державний університет інформаційно-комунікаційних технологій*

Horvatova Oksana

PhD in Law, Associate Professor,

Associate Professor of the Department of Public Management and Administration

State University of Information and Communication Technologies

ORCID: 0000-0002-1467-3797

DOI: 10.25313/2617-572X-2025-5-10976

ЗМІЦНЕННЯ ІНСТИТУЦІЙНИХ І ЗАКОНОДАВЧИХ ОСНОВ ЄВРОПЕЙСЬКОЇ КІБЕРДИПЛОМАТІЇ В УМОВАХ ЕСКАЛАЦІЇ РОСІЙСЬКИХ ГІБРИДНИХ ЗАГРОЗ

STRENGTHENING THE INSTITUTIONAL AND LEGISLATIVE FOUNDATIONS OF EUROPEAN CYBER DIPLOMACY IN THE FACE OF ESCALATING RUSSIAN HYBRID THREATS

Анотація. Вступ. Після початку повномасштабного російського вторгнення в Україну значно зросли та постійно модифікуються гібридні загрози з боку Кремля, спрямовані на дестабілізацію Європейського Союзу та його країн-членів. Ці загрози проявляються у безпрецедентній кількості кібератак на критичну інфраструктуру, активізації діяльності російських розвідслужб, спробах втручання у виборчі процеси, поширенні дезінформації та підриві довіри до демократичних інститутів тощо.

Таким чином, європейські еліти постали перед необхідністю термінового нарощування власних інституційних та законодавчих спроможностей у сфері кібердипломатії та оборони для забезпечення своєї безпеки, стабільності та цифрового суверенітету. Пошук адекватної протидії деструктивній діяльності Москви є досить актуальною проблемою не тільки для країн Європейського Союзу, а й для його найближчого оточення, зокрема України. Спільні виклики виступають додатковим чинником зближення позицій Києва та Брюсселя, тим самим поглиблюючи європейську інтеграцію України.

Мета статті. Проаналізувати останні зміни у європейській кібердипломатії як системну відповідь на дедалі більш агресивні російські гібридні атаки на країни ЄС, дослідити ключові чинники та особливості цього процесу, а також визначити політико-інституційні наслідки для забезпечення цифрового суверенітету Європи.

Матеріали і методи. Матеріалами дослідження є: 1) нові нормативно-правові регулювання ЄС у сфері кібербезпеки, зокрема прийняття Закону про кіберстійкість, поправок до Акту про кібербезпеку, Закону про цифрову операційну стійкість (DORA) та Закону про кіберсолідарність; 2) праці вітчизняних та європейських авторів, що провадять свої науково-практичні дослідження у царині протидії російським гібридним загрозам.

У статті були використані дедуктивні підходи на базі формальної і діалектичної логіки із залученням аналітичних методів наукового дослідження.

За допомогою діалектичного підходу в роботі встановлюється причинно-наслідковий зв'язок між російськими гібридними атаками та нарощенням інституційних і законодавчих зусиль на рівні ЄС для забезпечення кіберстійкості та цифрового суверенітету Європи.

Під поняттям аналіз розуміється використання певних рамок у класифікації одержаної інформації, окреслення термінів та усвідомлення їх суті, з'ясування критеріїв певних суджень, організацію інформаційної бази з пристосуванням її до поставлених цілей. Використовуючи аналітичні методи (системний, порівняльний, структурно-функціональний тощо) автори прагнули з'ясувати ключові чинники та особливості трансформації європейської кібердипломатії на сучасному етапі.

Результати. У роботі проаналізовано зміцнення інституційних і законодавчих основ європейської кібердипломатії на тлі ескалації російських гібридних загроз. Детально розкрито гібридні операції Росії, спрямовані на підрив демократичних інститутів в країнах ЄС та суміжних державах, зокрема під час виборів у Молдові та Румунії. Висвітлено зусилля ЄС щодо посилення оборонних спроможностей, зокрема через презентацію Білої книги європейської оборони «Готовність 2030» та Плану «Переозброєння Європи».

Визначено особливості законодавчої активності ЄС у сфері кібербезпеки, зокрема прийняття Закону про кіберстійкість, поправок до Акту про кібербезпеку, Закону про цифрову операційну стійкість (DORA) та Закону про кіберсолідарність. У висновках наголошується на складності міжнародного становища ЄС через агресивну політику Кремля та непрогнозовані гії адміністрації Д. Трампа, а також на стратегічній необхідності подальшої консолідації зусиль ЄС у сфері кібербезпеки.

Перспективи. У подальших наукових дослідженнях пропонується зосередити увагу на посиленні європейської єдності, розширенні санкційних механізмів, інвестуванні у кіберосвіту та технології, а також тіснішій співпраці як всередині ЄС, так і з партнерами з НАТО, ООН та іншими міжнародними організаціями для створення ефективної архітектури протидії гібридним загрозам.

Ключові слова: гібридні загрози, відносини ЄС – Росія, російське втручання у вибори, кіберпростір, кібердипломатія, Біла книга європейської оборони «Готовність 2030», План «Переозброєння Європи», Закон про кіберстійкість.

Summary. Introduction. Since the beginning of Russia's full-scale invasion of Ukraine, the Kremlin's hybrid threats aimed at destabilizing the European Union and its member states have increased significantly and are constantly being modified. These threats are manifested in an unprecedented number of cyberattacks on critical infrastructure, intensified activities of Russian intelligence services, attempts to interfere in electoral processes, spreading disinformation and undermining trust in democratic institutions, etc.

Thus, European elites are faced with the need to urgently build up their own institutional and legislative capabilities in the field of cyber diplomacy and defense to ensure their security, stability, and digital sovereignty. Finding an adequate response to Moscow's destructive activities is a pressing issue not only for the European Union, but also for its immediate neighborhood, including Ukraine. Common challenges are an additional factor in the convergence of positions between Kyiv and Brussels, thereby deepening Ukraine's European integration.

The purpose of the article. To analyze the recent changes in European cyber diplomacy as a systemic response to the increasingly aggressive Russian hybrid attacks on EU countries, to explore the key factors and features of this process, and to determine the political and institutional implications for ensuring Europe's digital sovereignty.

Materials and Methods. The research materials are: 1) innovations in EU cybersecurity regulation, in particular the adoption of the Cybersecurity Act, amendments to the Cybersecurity Act, the Digital Operational Resilience Act (DORA) and the Cyber Solidarity Act; 2) works by domestic and European authors conducting their scientific and practical research in the field of countering Russian hybrid threats.

The article uses deductive approaches based on formal and dialectical logic with the use of analytical methods of scientific research.

Using a dialectical approach, the paper establishes a causal link between Russian hybrid attacks and the increasing institutional and legislative efforts at the EU level to ensure cyber resilience and digital sovereignty of Europe.

The concept of analysis means the use of a certain framework in classifying the information received, defining terms and understanding their essence, clarifying the criteria for certain judgments, and organizing the information base to adapt it to the goals set. Using analytical methods (systemic, comparative, structural and functional, etc.), the authors sought to identify the key factors and features of the transformation of European cyber diplomacy at the present stage.

Results. The paper analyzes the strengthening of the institutional and legislative foundations of European cyber diplomacy against the backdrop of escalating Russian hybrid threats. The author describes in detail Russia's hybrid operations aimed at undermining democratic institutions in the EU and neighboring countries, in particular during the elections in Moldova and Romania. The author highlights the EU's efforts to strengthen its defense capabilities, in particular through the presentation of the European Defense White Paper "Readiness 2030" and the "Rearmament of Europe" Plan.

The author identifies the peculiarities of the EU's legislative activity in the field of cybersecurity, in particular the adoption of the Cybersecurity Act, amendments to the Cybersecurity Act, the Digital Operational Resilience Act (DORA) and the Cyber Solidarity Act. The conclusions emphasize the complexity of the EU's international situation due to the Kremlin's aggressive policy and unpredictable actions of the Trump administration, as well as the strategic need to further consolidate the EU's efforts in the field of cybersecurity.

Prospects. Further research is proposed to focus on strengthening European unity, expanding sanctions mechanisms, investing in cyber education and technology, and closer cooperation both within the EU and with partners from NATO, the UN and other international organizations to create an effective architecture for countering hybrid threats.

Key words: hybrid threats, EU-Russia relations, Russian interference in elections, cyberspace, cyber diplomacy, European Defense White Paper "Readiness 2030", Plan "Rearmament of Europe", Cyber Resilience Act.

Постановка проблеми. Ключове питання, що розглядається в статті, полягає у тому, що останні роки значно зросли та постійно модифікуються гібридні загрози з боку російської федерації, спрямовані на дестабілізацію Європейського Союзу та його країн-членів. Ці загрози проявляються

у безпрецедентній кількості кібератак на критичну інфраструктуру, активізації діяльності російських розвідслужб, спробах втручання у виборчі процеси, поширенні дезінформації та підриві довіри до демократичних інститутів тощо. Особливо гостро ця проблема постала на тлі повномасштабної агресії

РФ проти України, що змусило ЄС переглянути свою роль у сфері безпеки та активізувати зусилля для протидії цим викликам. Додатковим фактором, що ускладнює ситуацію, є потенційне послаблення трансатлантичної єдності та зміни в політиці США, зокрема заяви Дональда Трампа щодо НАТО.

Таким чином, ЄС стоїть перед необхідністю термінового нарощування власних інституційних та законодавчих спроможностей у сфері кібердипломатії та оборони для забезпечення своєї безпеки, стабільності та цифрового суверенітету. Пошук адекватної протидії деструктивній діяльності Кремля є досить актуальною проблемою не тільки для країн Європейського Союзу, а й для його найближчого оточення, зокрема України. Спільні виклики виступають додатковим чинником зближення позицій Києва та Брюсселя, тим самим поглиблюючи європейську інтеграцію України.

Аналіз останніх досліджень і публікацій.

З початку 2024 року російська федерація значно активізувала гібридні атаки проти Європейського Союзу та його східних партнерів. Ці дії є частиною ширшої стратегії Кремля, спрямованої на досягнення своїх геополітичних цілей через підрив демократичних інститутів, поширення впливу та перешкодження євроатлантичній інтеграції. Багатогранний характер цих загроз включає дезінформаційні кампанії, кібератаки, політичне втручання, економічний тиск і використання енергетичних ресурсів як зброї тощо. Відповідне нарощення російських зусиль по дестабілізації регіону не залишилося поза увагою як інституцій і посадовців ЄС, так і дослідницької спільноти.

У березні 2025 року Європейська служба зовнішніх справ опублікувала 3-й звіт про загрози маніпулювання та втручання іноземною інформацією (Foreign Information Manipulation and Interference, або FIMI). Кая Каллас, Верховний представник ЄС із закордонних справ та політики безпеки, віцепрезидент Європейської комісії, зазначала, що його новизною стало «викриття величезних цифрових арсеналів, спеціально створених росією та Китаєм для проведення своїх операцій FIMI» [1, с. 2]. Зокрема у грудні 2024 року ЄС запровадив перші в історії санкції за таку поведінку.

Варто згадати звіти EUvsDisinfo, що є флагманським проектом Оперативної робочої групи зі стратегічних комунікацій Європейської служби зовнішніх справ [2], а також публікації Центру передового досвіду НАТО зі стратегічних комунікацій (NATO StratCom COE) [3].

Експертні публікації також багато уваги присвятили аналізу російського гібридного впливу та відзначили активізацію відповідних зусиль Кремля за останній рік. У цьому зв'язку відзначимо спільне розслідування дезінформаційних кампаній та операцій впливу експертів Центру зовнішньої політики (FPC) — незалежного, позапартійного аналітичного

центру з міжнародних справ, що базується у Великій Британії [4], а також праці Корнеліу Бйола [5], Йозефа Шлерки [6], Данієлі Пісо [7], Василіса Нтусаса та Лауренціу Плешку [8] тощо.

Серед вітчизняних публікацій варто відзначити перше наукове видання з кібердипломатії на основі матеріалів міжнародних наукових заходів з кібердипломатії, які відбулись по лінії МЗС України у 2024 році. Виступи та праці, присвячені проблематиці протидії гібридних загроз — Гайдука О. В., Верховцевої І. Г., Мужанової Т. М., Петькун С. М., Корченка О. Г. та інших учасників «круглого столу» [9] стали вагомим кроком на шляху інституціоналізації кібердипломатії та її системного наукового вивчення в Україні.

Враховуючи, що дослідження кібердипломатії і протидії гібридних загроз є відносно новою проблематикою в Україні та ЄС, слід констатувати, що в цій сфері досліджень залишається чимало питань, що потребують вивчення і концептуального оформлення.

Мета статті. Проаналізувати останні зміни у європейській кібердипломатії як системну відповідь на дедалі більш агресивні російські гібридні атаки на країни ЄС, дослідити ключові чинники та особливості цього процесу, а також визначити політико-інституційні наслідки для забезпечення цифрового суверенітету Європи.

Виклад основного матеріалу. Повномасштабна агресія російської федерації проти України зруйнувала світовий порядок та істотно вплинула на геополітичний вибір Європейського Союзу. В умовах наростаючої зовнішньої загрози, військових і гібридних ризиків він усвідомив себе гравцем і став одним із центрів політичної сили, одним із центрів прийняття рішень [10].

Напруження між Брюсселем і Москвою, яке стало від 2022 року, у 2024-му досягло небезпечного рівня. Зокрема, цього року було зафіксовано безпрецедентну кількість кібератак на інфраструктуру країн-членів ЄС. Водночас посилилася діяльність російських розвідслужб: шпигунські скандали, спроби втручання у вибори, підживлення ультраправих та ультралівих сил у Європі. Пошкодження критичної інфраструктури, маневри поблизу кордонів Польщі та країн Балтії — усе це частина багатошарового гібридного тиску.

Протягом 2024 року росія активно використовувала гібридні операції, спрямовані на підрив демократичних інститутів, поширення дезінформації і недовіри до урядів, соціальний розкол у суспільствах, зокрема у Німеччині [11] та Чехії [12].

У листопаді 2024 року з різницею в кілька днів у Балтійському морі було пошкоджено два телекомунікаційні кабелі — між Німеччиною та Фінляндією та між Швецією та Литвою, що викликали істотні проблеми зі зв'язком та інтернетом [13].

Безпрецедентний рівень гібридних атак, що мали значні політичні наслідки, було продемонстровано

під час виборів у Молдові та Румунії у жовтні-грудні 2024 року. Російське втручання, задокументоване розвідувальними звітами та висновками міжнародних спостерігачів, використовувало широкий спектр гібридних тактик: масова дезінформація, незаконне фінансування (включаючи криптовалюти), кібератаки, експлуатація соціальних мереж (особливо TikTok у Румунії), тренування провокаторів та використання проксі-акторів.

Вибори у Молдові. 20 жовтня 2024 року у Молдові відбувся перший тур президентських виборів та Референдум щодо ЄС. Другий тур було проведено 3 листопада. Ці вибори мали вирішальне значення для геополітичного курсу Молдови. Насамперед йшлося про переобрання проєвропейської президентки Маї Санду та закріплення в конституції стратегічної мети вступу до ЄС, що ускладнило б майбутні спроби змінити цей курс [8].

Попри те, що Референдум щодо ЄС відбувся з мінімальною перевагою (50.35% «за»), його перебіг був позначений істотним зовнішнім втручанням. Так, 21 жовтня 2024 року в Спільній заяві Високого представника Жозепа Борреля та Європейської комісії щодо президентських виборів та конституційного референдуму у Молдові зазначалося, що перший тур президентських виборів і конституційний референдум щодо вступу до ЄС проходили в середовищі, яке характеризується «занепокоєнням учасників щодо незаконного іноземного втручання та активних зусиль з дезінформації», а також що «Росія та її ставленики активно намагалися підірвати демократичний процес і процес голосування в Молдові» [14].

Розвідувально-інформаційна служба Молдови (SIS) та інші джерела задокументували багатогранну кампанію втручання, яка координувалася, зокрема, олігархом-втікачем Іланом Шором з Москви [6,8,15]:

- Дезінформаційні кампанії: Масштабні зусилля з дискредитації європейського курсу та прозахідних політиків.
- Незаконне фінансування: Використання різноманітних методів (гранти, пожертви, готівка через кур'єрів, криптовалюти через платформи Binance, Bybit, російську систему «Мир», P2P-системи для фінансування проросійських партій та підкупу виборців. Повідомлялося про спрямування понад 15 мільйонів доларів на рахунки понад 130 000 громадян.
- Вербування та навчання активістів: Створення мережі з понад 100 «рекрутерів» та майже 2000 первинних осередків, що охопили понад 33 000 активістів, завданням яких було переконати виборців (за гроші) голосувати проти ЄС.
- Навчання тактикам протестів: Організація поїздок молоді до Москви (під прикриттям проєктів «Євразія») для навчання методам провокування поліції, фізичних сутичок, використання піротехніки, нейтралізації силовиків. Тренерами виступали,

зокрема, члени «Молодої гвардії Єдиної Росії». Повідомлялося також про можливе просунуте навчання в таборах у Боснії та Герцеговині (операції з дронами, підготовка запалювальних пристроїв).

- Використання Православної Церкви: Організація «паломництв» священників до Москви, де їх схилили до антиєвропейської позиції через контракти та фінансові стимули (виплати через систему «Мир», обіцянки винагороди).
- Кібератаки: Атаки на виборчу інфраструктуру, зокрема DDoS-атаки на урядові сайти в день референдуму.
- Використання організацій ветеранів: Використання партії «ШОР», блоку «Победа-Victorie», НКО «АНО Євразія» як політичного прикриття та платформ для операцій впливу, поширення пропаганди та незаконного фінансування.
- Маніпуляція діаспорою: Створення центрів у Росії для консолідації діаспори та маніпулювання голосуванням за кордоном.
- Кампанії в соцмережах: Активне використання TikTok, Facebook, VKontakte.
- Фізичне втручання: Повідомлення про мінування виборчих дільниць за кордоном.

Попри те, що референдум і перемога Санду у другому турі (55.35% проти 44.65% у Олександра Стояногло) закріпили проєвропейський вектор зовнішньої політики Молдови, детальний аналіз виявив тривожні тенденції та істотні наслідки російської гібридної атаки.

По-перше, Санду програла голосування серед мешканців Молдови, отримавши на 41 тисячу голосів менше, ніж у 2020 році, тоді як проросійський кандидат наростив підтримку. Її перемога була забезпечена виключно голосами діаспори.

По-друге, Референдум щодо ЄС пройшов з мінімальною перевагою (50.35% «за»), а серед мешканців всередині Молдови підтримка склала лише 38%.

По-третє, російське втручання поглибило внутрішні розбіжності в країні та суттєво підірвало підтримку ЄС серед населення Молдови, яке виявилось вразливим до гібридних операцій і передвиборних маніпуляцій.

Усе це створює виклики для майбутньої політичної стабільності Молдови, зокрема через парламентські вибори, які мають відбутися 28 вересня 2025 року.

Президентські вибори у Румунії. Російське втручання у президентські вибори в Румунії (листопад 2024 року) мали ще більш драматичні та деструктивні наслідки для країни, що по суті опинилася на грані політичної кризи.

Результати першого туру виявилися сенсаційними: незалежний ультраправий і проросійський кандидат Келін Джорджеску, який вважався другорядним кандидатом з невеликими шансами на перемогу, отримав перше місце і пройшов до другого туру. За короткий період, він швидко отримав

значну підтримку завдяки кампанії у нетрадиційних ЗМІ, таких як TikTok, отримавши особливу популярність серед тих, хто був незадоволений поточною румунською політикою, включаючи молодь, фермерів, сільських виборців і представників робітничого класу.

Другий тур мав відбутися 8 грудня 2024 року, оскільки в першому турі жоден кандидат не набрав абсолютної більшості. Натомість 6 грудня 2024 року Конституційний суд Румунії одностайно ухвалив рішення скасувати президентські вибори та заново провести виборчий процес в терміни, які визначить уряд.

Приводом для безпрецедентного рішення Конституційного суду стали документи Вищої ради національної оборони, які оприлюднив президент Румунії Клаус Йоганніс. Згідно з цією інформацією, на користь Джорджеску проводилася агресивна рекламна кампанія в обхід національного виборчого законодавства та з використанням алгоритмів платформ соцмереж. Ця кампанія була розгорнута приблизно за два тижні до дати виборів [16].

У інформаційній записці, яку Служба зовнішньої розвідки надіслала до Вищої ради національної оборони, повідомлялося, що Румунія стала мішенню для агресивних гібридних дій росії, включаючи кібератаки, витік інформації та саботаж. Пріоритетом для ворожих дій Росії став вплив на румунське суспільство через пропаганду та дезінформацію, а також підтримка кандидатів-евроскептиків та підживлення антисистемних рухів, зокрема шляхом «залучення їх до протестів, що формують суспільний порядок денний» [17].

Ключовим чинником російського втручання стала масована кампанія в TikTok. Румунські спецслужби та міжнародні звіти вказують на скоординовану кампанію в TikTok як основний інструмент просування Джорджеску. Було задіяно близько 25 000 акаунтів (деякі неактивні з 2016 року), спостерігалася штучна маніпуляція залученням (боти, скоординоване посилення) [5].

Як зазначали автори спільного розслідування «Мережі впливу: Розшифрування іноземного втручання у вибори Румунії»: «Ця гібридна операція втручання у вибори, методично організована для дестабілізації держави-члена НАТО та Європейського Союзу (ЄС), виходить далеко за межі Румунії. Вона відображає ширший геополітичний порядок денний, спрямований на руйнування євроатлантичної єдності, послаблення регіональної стійкості та підрив підтримки продовження війни в Україні» [4].

Румунський випадок став тривожним сигналом про те, як маніпуляції в соціальних мережах, особливо в TikTok, можуть стрімко вивести на політичну арену маргінальних кандидатів і дестабілізувати демократичні процеси, аж до анулювання виборів та спричинення глибокої політичної кризи всередині країни-члена ЄС і НАТО.

Наразі через відміну виборів Румунія переживає переломний політичний момент, який характеризується масштабними протестами громадськості. Термін повноважень президента Клауса Йоганніса було продовжено до повторних виборів. Однак він зіткнувся з масовим невдоволенням, звинуваченнями в неконституційності продовження терміну та погрозами застосування процедури імпічменту. 10 лютого 2025 року Йоганніс оголосив про свою відставку, щоб уникнути поглиблення кризи. Тимчасовим президентом став спікер Сенату Іліє Боложан.

Повторні президентські вибори в Румунії призначені на травень 2025 року. Таким чином, напередодні президентських виборів у травні 2025 року румунське суспільство є розколотим і країна постала перед проблемою подолання значних політичних турбулентностей.

Варто відзначити, що наразі у Польщі також відбуваються президентські вибори і польська влада витратила 2 мільярди євро на те, щоб не допустити втручання за «румунським сценарієм». Зокрема, виступаючи перед журналістами, міністр цифрових технологій Польщі Кшиштоф Гавковський наполягав на тому, що країна готова відбити той тип цифрового втручання, який переслідує вибори по всьому світу [18].

Станом на квітень 2025 року відносини між ЄС та Росією по суті перебувають на межі відкритого конфлікту. Від самого початку повномасштабного вторгнення РФ в Україну еліти Європейського Союзу чітко зрозуміли, що безпека континенту більше не є гарантованою. Але саме останній рік відкрив новий етап — етап прямої конфронтації, хоча й без відкритого зіткнення. Ескалація триває на багатьох рівнях — інформаційному, економічному, енергетичному, військовому.

Водночас необхідно звернути увагу на ще один важливий геополітичний фактор — вплив політики Дональда Трампа на європейську безпеку. Низка заяв Трампа, зокрема про можливу відмову США захищати союзників, які не витрачають «достатньо» на оборону, суттєво підірвала впевненість у стабільності трансатлантичних гарантій. У Москві ці сигнали розцінюються як послаблення єдності Заходу, що може провокувати нові авантюри.

По всій Європі спостерігаються ознаки того, що континент готується до «найекстремальнішого» сценарію, зокрема ЄС починає серйозно ставитися до війни з Росією за «епохи Трампа — Путіна 2.0» [19].

Європейські уряди і громадяни дедалі більше занепокоєні тим, що підбадьорений Кремль може розгорнути свої армії у їхньому напрямку після України. Також широко поширена нервозність через те, що новий президент США — ізоляціоніст — припустив, що він може не захистити історичних союзників Америки по НАТО, якщо вони зазнають нападу з боку Росії. У підсумку агресивні дії Москви та риторика Трампа щодо НАТО, яку можна коротко

сформулювати як: «Європа повинна сама себе захищати», вилилась у практичну реакцію — посилення ідеї стратегічної автономії ЄС.

У відповідь на загрози з боку Росії, Європейський Союз активізував зусилля з нарощування своїх оборонних спроможностей. 19 березня 2025 року президент Єврокомісії Урсула фон дер Ляєн та Високий представник із закордонних справ та політики безпеки/Віце-президент Європейської Комісії Кая Каллас презентували Білу книгу європейської оборони — Готовність 2030. Комісія також представила, в рамках Плану «Переозброєння Європи»/«Готовність 2030», амбітний оборонний пакет на загальну суму понад 800 млрд. євро до 2030 року, що надає державам-членам ЄС фінансові важелі для стимулювання інвестиційного сплеску в оборонний потенціал. Президент Комісії Урсула фон дер Ляєн зазначила: «Епоха мирних дивідендів давно минула. Архітектуру безпеки, на яку ми покладалися, більше не можна сприймати як належне. Європа готова зробити крок вперед. Ми повинні інвестувати в оборону, зміцнювати наші можливості та застосовувати проактивний підхід до безпеки. Ми вживаємо рішучих заходів, представляючи дорожню карту «Готовність 2030» зі збільшенням витрат на оборону, значними інвестиціями в європейський оборонно-промисловий потенціал» [20].

Загалом Біла книга визначає новий підхід до оборони та інвестиційні потреби, у той час як План «Переозброєння Європи»/«Готовність 2030» зміцнює загальноєвропейський оборонний потенціал новими фінансовими засобами. Витрати обсягом понад 800 мільярдів євро будуть спрямовані за 5 основними напрямками:

- Фіскальна гнучкість: тимчасове скасування бюджетних обмежень ЄС, що дозволить країнам-членам збільшити оборонні витрати до 1,5% ВВП (без порушення фінансових правил) протягом щонайменше 4 років. Очікується, що це залучить до 650 мільярдів євро в державах-членах ЄС.
- Запровадження нового Інструменту з досягнення безпеки в Європі (SAFE, Security Action for Europe), за яким ЄС залучить кошти до 150 мільярдів євро та надасть позики державам-членам для підтримки досягнення швидкого та значного збільшення інвестицій в оборонний потенціал Європи.
- Перерозподіл бюджету: перенаправлення існуючих коштів ЄС, зокрема фондів згуртованості, на оборонні інвестиції.
- Використання групи Європейського інвестиційного банку для підтримки оборонних підприємств через зняття обмежень на кредитування.
- Інвестиційне сприяння: створення механізму для мобілізації приватного капіталу в оборонну промисловість.

Ці заходи спрямовані на підвищення обороноздатності ЄС та зменшення залежності від зовнішніх постачальників зброї та техніки. Посадовці ЄС визнають, що до заходів із посилення оборонно-

промислового комплексу спонукала насамперед загроза з боку РФ, а також потреба у диверсифікації оборонної промисловості, зокрема і зменшення залежності від США. Так, Європейський комісар із питань оборони А. Кубілюс: «Ми маємо дивитися не лише на Росію як на загрозу, але й враховувати глобальні геополітичні зміни і те, куди американці спрямовують свою стратегічну увагу» [21].

Враховуючи безпрецедентний рівень гібридних атак, які Росія спрямувала на ЄС протягом останнього року, важливою складовою Плану «Переозброєння Європи»/«Готовність 2030» є необхідність подальшої консолідації зусиль ЄС у сфері кібербезпеки, подолання імплементаційних розривів, інвестування в людський капітал та технології (включаючи квантові комунікації), зміцнення державно-приватного партнерства та міжнародної співпраці, зокрема з США, для ефективної протидії гібридним загрозам та забезпечення цифрового суверенітету Європи.

Станом на кінець квітня 2025 року, ландшафт кібербезпеки Європейського Союзу характеризується безпрецедентною законодавчою активністю, спрямованою на зміцнення колективної стійкості проти все більш складних загроз.

10 грудня 2024 року набрав чинності Закон про кіберстійкість (Cyber Resilience Act, CRA). Цей документ базується на Стратегії кібербезпеки ЄС 2020 року та Стратегії Безпекового союзу ЄС. Він запроваджує обов'язкові вимоги для виробників і роздрібних торговців щодо проектування, розробки та обслуговування продуктів, що містять цифровий компонент. Ці зобов'язання мають виконуватися на кожному етапі ланцюжка створення вартості. Закон також вимагає від виробників забезпечувати турботу протягом життєвого циклу своєї продукції.

15 січня 2025 року було ухвалено цілову поправку до Акту про кібербезпеку (The Cybersecurity Act), яка розширила повноваження Агентства ЄС з кібербезпеки (ENISA) та сферу застосування Європейської системи сертифікації кібербезпеки (ECCF) на «керовані послуги безпеки» [22]. Це охоплює такі критично важливі та чутливі послуги, як реагування на інциденти, тестування на проникнення, аудити безпеки та консалтинг, з метою забезпечення їх високого рівня якості та надійності.

З 17 січня 2025 року обов'язковим для всіх держав-членів ЄС став Закон ЄС про цифрову операційну стійкість (Digital Operational Resilience Act, широко відомий як DORA), що усуває критичну прогалину у фінансовому регулюванні ЄС. До прийняття цього закону фінансові установи переважно керували операційними ризиками, розподіляючи капітал для покриття потенційних збитків. Цей підхід не охоплював усі аспекти операційної стійкості, особливо стосовно інформаційно-комунікаційних технологій (ІКТ). З впровадженням DORA фінансові установи тепер зобов'язані дотримуватися суворих рекомендацій щодо захисту від інцидентів,

пов'язаних з ІКТ. До них належать заходи щодо захисту, виявлення, стримування, відновлення та ремонту. DORA чітко спрямований на ризики, пов'язані з ІКТ, запроваджуючи чіткі правила управління ризиками, пов'язаними з ІКТ, звітності про інциденти, тестування операційної стійкості та нагляду за ризиками третіх сторін, пов'язаними з ІКТ.

З 4 лютого 2025 року набрав чинності Закон про кіберсолідарність (Cyber Solidarity Act), який має на меті посилити спроможність ЄС виявляти кіберзагрози та інциденти, готуватися до них та реагувати на них. Він запроваджує такі ключові Компоненти:

- Європейську систему оповіщення про кіберзагрози. Ця система передбачає створення загальноєвропейської мережі національних та транскордонних центрів кібербезпеки (SOC) по всьому ЄС, які використовуватимуть передові технології, такі як штучний інтелект (ШІ) та аналітика даних, для виявлення та обміну попередженнями про загрози з органами влади за кордоном. Її мета — побудова скоординованих можливостей виявлення та ситуаційної обізнаності по всьому ЄС, посилення виявлення загроз та обміну інформацією між командами реагування на комп'ютерні надзвичайні ситуації (CERT), групами реагування на інциденти комп'ютерної безпеки (CSIRT), центрами обміну та аналізу інформацією (ISAC) та операторами критичної інфраструктури. Інформація, що обмінюється, може включати дані з мереж та сенсорів, потоки розвідданих про загрози, індикатори компрометації та контекстуалізовану інформацію про інциденти, загрози, вразливості тощо.
- Механізм надзвичайних ситуацій у сфері кібербезпеки. Цей механізм призначений для підтримки держав-членів (на їхній запит) та інших користувачів у підготовці до значних та великомасштабних кіберінцидентів, реагуванні на них, пом'якшенні їхнього впливу та ініціюванні відновлення. Він також підтримує скоординоване тестування готовності та взаємну допомогу між державами-членами.
- Резерв ЄС з кібербезпеки. Як ключова частина Механізму надзвичайних ситуацій, цей резерв складається з послуг довірених постачальників керованих послуг безпеки (MSSP). Він призначений для підтримки заходів реагування та початкового відновлення для постраждалих держав-членів, інституцій ЄС та, за певних умов, третіх країн, асоційованих із програмою «Цифрова Європа».
- Європейський механізм огляду кіберінцидентів. Цей компонент дозволяє проводити огляд та оцінку конкретних значних або масштабних кіберінцидентів для аналізу причин, наслідків, заходів пом'якшення та винесення уроків на майбутнє.

Загалом прийняття Закону про кіберсолідарність є важливим кроком від політичних декларацій до створення конкретних, фінансованих ЄС механізмів для колективного захисту. Якщо попередні зусилля значною мірою поклалися на національну імплементацію директив ЄС про мережеву та інформаційну безпеку (як NIS/NIS2) та добровільний обмін інформацією, то цей документ запроваджує спільні структури (центри, резерв), що фінансуються з бюджету ЄС (відповідно до Регламенту (ЄС, Євратом) 2024/2509 та явно спрямований на «зміцнення солідарності та спроможностей». Це свідчить про перехід до більш операціоналізованої форми солідарності, підкріпленої спільними ресурсами та інфраструктурою.

24 лютого 2025 року було опубліковано проєкт Рекомендації Європейської Ради щодо оновленого Плану реагування ЄС на кібернетичні кризи (Cyber Blueprint). Цей документ має на меті представити рамки управління кіберкризами в ЄС у чіткий, простий та доступний спосіб. Оновлений план визначає відповідних суб'єктів ЄС (ENISA, Мережа CSIRT, Комісія, Рада тощо) та їхні ролі протягом усього життєвого циклу кризи: від підготовки, спільної ситуаційної обізнаності та виявлення до реагування та відновлення. Ця ініціатива тісно пов'язана з оперативними аспектами Акту про кіберсолідарність, зокрема з Механізмом надзвичайних ситуацій.

Таким чином, реагуючи на зростаючу ескалацію з боку росії Європейський Союз активно посилює свої оборонні спроможності та колективну стійкість до гібридних загроз, водночас підтримуючи Україну в її боротьбі за суверенітет та територіальну цілісність.

Ключові законодавчі акти, такі як Акт про кіберсолідарність, Акт про кіберстійкість, зміни до Акту про кібербезпеку, разом із сектор-специфічним Законом про цифрову операційну стійкість та оновленим Планом реагування на кібернетичні кризи формують в Європейському Союзі багатопланову регуляторну систему.

Однак, амбітні законодавчі цілі ЄС стикаються з серйозними викликами в імплементації, особливо тривожною виглядає ситуація з імплементацією Директиви № 2 про мережеву та інформаційну безпеку (Network and Information Security Directive 2 або NIS2), де більшість держав-членів не вклалися у визначений термін (17 жовтня 2024 року), що створює ризик фрагментації та затримок у підвищенні рівня безпеки критичних секторів.

Висновки та перспективи подальших досліджень. Узагальнюючи попередні тези, можна зробити чіткий висновок про те, що агресивна політика Кремля та непрогнозовані дії нинішньої адміністрації Д.Трампа істотно ускладнили міжнародне становище Європейського Союзу в частині забезпечення військової безпеки та політичної стабільності.

Геополітичний контекст залишається напруженим, що яскраво демонструють нещодавні вибори в Молдові та Румунії. Російське втручання, задокументоване розвідувальними звітами та висновками міжнародних спостерігачів, використовувало широкий спектр гібридних тактик: масова дезінформація, незаконне фінансування (включаючи криптовалюту), кібератаки, експлуатація соціаль-

них мереж (особливо TikTok у Румунії), тренування провокаторів та використання проксі-акторів. Хоча в Молдові прозахідна президентка Мая Санду була переобрана, аналіз результатів виявив значну вразливість населення до російського впливу та розкол між голосами діаспори та мешканців країни. У Румунії безпрецедентне втручання призвело до анулювання першого туру виборів та глибокої політичної кризи, що підкреслило потенціал соціальних мереж для швидкої дестабілізації демократичних процесів навіть у країнах-членах ЄС та НАТО. Ці події підтверджують, що метою втручання може бути не лише перемога бажаного кандидата, а й загальна дестабілізація та підриз довіри до інститутів.

Наразі політика ЄС у сфері протидії гібридним загрозам характеризується безпрецедентною політичною та законодавчою активністю, спрямованою на підвищення обороноздатності та зміцнення колективної стійкості проти все більш складних інформаційних і кібератак.

Стратегічні імперативи визначають також необхідність подальшої консолідації зусиль ЄС у сфері кібербезпеки, подолання імплементаційних розривів, інвестування в людський капітал та технології, зміцнення державно-приватного партнерства та міжнародної співпраці, зокрема з США, для ефективної протидії гібридним загрозам та забезпечення цифрового суверенітету Європи.

Література

1. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations. *European External Action Service (EEAS)*. March 2025. URL: <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf> (дата звернення: 15.05.2025).
2. Двійник завдає удару у відповідь: розкриття діяльності FIMI, спрямованої проти виборів до Європейського парламенту. URL: <https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/>; EUvsDisinfo. (2024). Російські експерименти з дезінформацією в Молдові. URL: <https://euvsdisinfo.eu/russian-experiments-with-disinformation-in-moldova/>; EUvsDisinfo. (2025). Ще одні вибори, ще одна спроба втручання Кремля. URL: <https://euvsdisinfo.eu/another-election-another-kremlin-interference-attempt> (дата звернення: 15.05.2025).
3. Morley-Davies J., Thomas J., Baines G. Russian information operations outside of the Western information environment (Revised version). The NATO strategic communications centre of excellence. Riga, January 2025. URL: <https://stratcomcoe.org/pdfjs/?file=/publications/download/Russian-info-operations-REVISED-VERSION-DIGITAL.pdf?zoom=page-fit> (дата звернення: 15.05.2025).
4. Andra-Lucia Martinescu, Sorina Stallard & other. Networks of Influence: Decoding foreign meddling in Romania's elections, A collaborative investigation into disinformation campaigns and influence operations. December 2024. URL: <https://fpc.org.uk/wp-content/uploads/2024/12/Networks-of-Influence-Decoding-foreign-meddling-in-Romanias-elections-2024.pdf> (дата звернення: 15.05.2025).
5. Bjola C. Algorithmic invasions: How information warfare threatens NATO's eastern flank. *NATO REVIEW*. 07 February 2025. URL: <https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html> (дата звернення: 15.05.2025).
6. Šlerka J. Intelligence Report Exposes Russian Meddling in Moldova's EU Vote. *VSquare*. 2025-01-17. URL: <https://vsquare.org/intelligence-report-russian-meddling-in-moldova-eu-referendum-sis-ilian-sor> (дата звернення: 15.05.2025).
7. Pisoiu D. Hybrid Threats and the Role of the Far Right. Trend Report 7 / January 2025. Österreichisches Institut für Internationale Politik / Austrian Institute for International Affairs. URL: <https://www.oii.ac.at/en/publications/hybrid-threats-and-the-role-of-the-far-right/> (дата звернення: 15.05.2025).
8. Ntousas V., Pleșca L. Russian Meddling in Moldova. German Marshall Fund of the United States. October 18, 2024. URL: <https://www.gmfus.org/news/russian-meddling-moldova>
9. Кібердипломатія: матеріали Міжнародної науково-практичної конференції (м. Київ, 15–16 травня 2024 року), Науково-практичного круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року) / за заг. ред. чл.-кор. НАН України, докт. техн. наук, проф. О. Г. Корченка; упорядники: І. Г. Верховцева, О. В. Гайдук. Київ: Дипломатична академія імені Геннадія Удовенка; Державний університет інформаційно-комунікаційних технологій, 2025. 118 с. URL: https://duikt.edu.ua/uploads/p_2850_97611772.pdf (дата звернення: 15.05.2025).
10. Долгов І. Геополітичний вимір Євросоюзу: Як змінюється ЄС і як на це впливає Україна. *Укрінформ*. 22.12.2023. URL: <https://www.ukrinform.ua/rubric-world/3803258-geopolitichnij-vimir-evrosouzu-ak-zminuetsya-es-i-ak-na-ce-vplivaie-ukraina.html> (дата звернення: 15.05.2025).
11. США, ЄС і Британія засудили кібератаки ГРУ проти партії канцлера Шольца, оборонних та ІТ-компаній Німеччини. *Голос Америки*. 03 травень, 2024. URL: <https://www.holosameryky.com/a/gru-kiberataka-nimechchyna/7596822.html> (дата звернення: 15.05.2025).
12. Перун В. МЗС Чехії розповіло про кібератаку угруповання APT28 на деякі свої установи. Зловмисники використали раніше невідому вразливість у Microsoft Outlook. *LB.UA*. 3 травня 2024. URL: https://lb.ua/world/2024/05/03/611525_mzs_chehii_rozpovilo_pro_kiberataku.html (дата звернення: 15.05.2025).

13. Павлюк О. У Балтійському морі пошкодили ще один кабель зв'язку. *Європейська правда*. Понеділок, 18 листопада 2024. URL: <https://www.eurointegration.com.ua/news/2024/11/18/7198677/> (дата звернення: 15.05.2025).
14. Moldova: Joint Statement by High Representative Josep Borrell and the European Commission on the Presidential Election and the Constitutional Referendum. 21.10.2024. URL: https://www.eeas.europa.eu/eeas/moldova-joint-statement-high-representative-josep-borrell-and-european-commission-presidential_en (дата звернення: 15.05.2025).
15. Report by Moldova's Intelligence and Security Service (SIS): Foreign interference in electoral processes in the Republic of Moldova. December 2024. URL: https://sis.md/sites/default/files/comunicate/fisiere/Raport_SIS_Public_Interferenta_in_procesul_electoral.pdf (дата звернення: 15.05.2025).
16. Вуець П. Румунський детектив з російським слідом. Як «благодійник» з TikTok зірвав президентські вибори. *Онлайн-медіа «Інформаційне агентство «Главком»*. 10 грудня, 2024. URL: <https://glavcom.ua/publications/rumunskij-detektiv-z-rosijskim-slidom-jak-blahodijnik-z-tiktok-zirvav-prezidentski-vibori-1035421.html> (дата звернення: 15.05.2025).
17. Document CSAT Serviciul de Informații Externe. 04.12.2024. URL: <https://cutt.ly/JrJFq42> (дата звернення: 15.05.2025).
18. Lasica J. Can Poland's cyber umbrella stop digital election meddling? *Monocle: Affairs*, April 23, 2025. URL: <https://monocle.com/affairs/poland-cyber-umbrella-elections/> (дата звернення: 15.05.2025).
19. Smith A. Europe braces for 'most extreme' military scenario as Trump-Putin 2.0 begins. *NBC News*. Jan. 26, 2025. URL: <https://www.nbcnews.com/news/world/trump-putin-europe-war-ukraine-attack-baltic-germany-finland-sweden-rcna187924> (дата звернення: 15.05.2025).
20. Єврокомісія оприлюднила Білу книгу європейської оборони та План «Переозброєння Європи/Готовність 2030». 19.03.2025. Press and information team of the Delegation to UKRAINE. URL: <https://cutt.ly/7rzaWF4d> (дата звернення: 15.05.2025).
21. ЄС посилює оборонні спроможності. *Служба зовнішньої розвідки України*. 21.03.2025. URL: <https://szru.gov.ua/news-media/news/ies-posylyue-oboronni-spromozhnosti-1742515200000> (дата звернення: 15.05.2025).
22. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services. COM/2023/208 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208> (дата звернення: 15.05.2025).

References

1. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations. European External Action Service (EEAS). March 2025. URL: <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>.
2. EUvsDisinfo. (2024). Doppelganger Strikes Back: Unveiling FIMI Activities Targeting European Parliament Elections. URL: <https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/>; EUvsDisinfo. (2024). Russian experiments with disinformation in Moldova. URL: <https://euvsdisinfo.eu/russian-experiments-with-disinformation-in-moldova/>; EUvsDisinfo. (2025). Another election, another Kremlin interference attempt. URL: <https://euvsdisinfo.eu/another-election-another-kremlin-interference-attempt>.
3. Morley-Davies J., Thomas J., Baines G. Russian information operations outside of the Western information environment (Revised version). THE NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE. Riga, January 2025. URL: <https://stratcomcoe.org/pdfjs/?file=/publications/download/Russian-info-operations-REVISED-VERSION-DIGITAL.pdf?zoom=page-fit>.
4. Andra-Lucia Martinescu, Sorina Stallard & other. Networks of Influence: Decoding foreign meddling in Romania's elections, A collaborative investigation into disinformation campaigns and influence operations. December 2024. URL: <https://fpc.org.uk/wp-content/uploads/2024/12/Networks-of-Influence-Decoding-foreign-meddling-in-Romanias-elections-2024.pdf>.
5. Bjola C. Algorithmic invasions: How information warfare threatens NATO's eastern flank. *NATO REVIEW*. 07 February 2025. URL: <https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html>.
6. Šlerka J. Intelligence Report Exposes Russian Meddling in Moldova's EU Vote. — VSquare. 2025-01-17. URL: <https://vsquare.org/intelligence-report-russian-meddling-in-moldova-eu-referendum-sis-ilian-sor>.
7. Pisoiu D. Hybrid Threats and the Role of the Far Right. *Trend Report 7 / January 2025*. Österreichisches Institut für Internationale Politik / Austrian Institute for International Affairs. URL: <https://www.oii.ac.at/en/publications/hybrid-threats-and-the-role-of-the-far-right/>.
8. Ntousas V., Pleșca L. Russian Meddling in Moldova. German Marshall Fund of the United States. October 18, 2024. URL: <https://www.gmfus.org/news/russian-meddling-moldova>.
9. Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) / za zah. red. chl.-kor. NAN Ukrainy, dokt. tekhn. nauk, prof. O. H. Korchenka; uporiadnyky: I. H. Verkhovtseva, O. V. Haiduk. Kyiv: Dyplomatychna akademiia imeni Hennadiia Udovenka; Derzhavnyi universytet informatsiino-komunikatsiinykh tekhnolohii, 2025. 118 s. URL: https://duikt.edu.ua/uploads/p_2850_97611772.pdf.

10. Ihor Dolhov. Heopolitychnyi vymir Yevrosoiuzu: Yak zminiuietsia YeS i yak na tse vplyvaie Ukraina. Ukrinform. 22.12.2023. URL: <https://www.ukrinform.ua/rubric-world/3803258-geopolitichnij-vimir-evrosouzu-ak-zminuetsa-es-i-ak-na-ce-vplyvae-ukraina.html>.
11. SShA, YeS i Brytaniia zasudyly kiberataky HRU proty partii kantslera Sholtza, oboronnykh ta IT-kompanii Nimechchyny. Holos Ameryky. 03 traven, 2024. URL: <https://www.holosameryky.com/a/gru-kiberataka-nimechchyna/7596822.html>.
12. Perun V. MZS Chekhii rozpovilo pro kiberataku uhrupovannia APT28 na deiaki svoi ustanovy. Zlovmysnyky vykorystaly ranishe nevidomu vrazlyvist u Microsoft Outlook. LB.UA. 3 travnia 2024. URL: https://lb.ua/world/2024/05/03/611525_mzs_chehii_rozpovilo_pro_kiberataku.html.
13. Pavliuk O. U Baltiiskomu mori poshkodyly shche odyin kabel zviazku. Yevropeiska pravda. Ponedilok, 18 lystopada 2024. URL: <https://www.eurointegration.com.ua/news/2024/11/18/7198677/>.
14. Moldova: Joint Statement by High Representative Josep Borrell and the European Commission on the Presidential Election and the Constitutional Referendum. 21.10.2024. URL: https://www.eeas.europa.eu/eeas/moldova-joint-statement-high-representative-josep-borrell-and-european-commission-presidential_en.
15. Report by Moldova's Intelligence and Security Service (SIS): Foreign interference in electoral processes in the Republic of Moldova. December 2024. URL: https://sis.md/sites/default/files/comunicate/fisiere/Raport_SIS_Public_Interferenta_in_procesul_electoral.pdf.
16. Vuiets P. Rumunskyi detektyv z rosiiskym slidom. Yak "blahodiinyk" z TikTok zirvav prezidentski vybory. Onlain-media "Informatsiine ahentstvo "Hlavkom". 10 hrudnia, 2024. URL: <https://glavcom.ua/publications/rumunskij-detektiv-z-rosijskim-slidom-jak-blahodijnik-z-tiktok-zirvav-prezidentski-vibori-1035421.html>.
17. Document CSAT Serviciul de Informații Externe. 04.12.2024. URL: <https://cutt.ly/JrlJFq42>.
18. Lasica J. Can Poland's cyber umbrella stop digital election meddling? Monocle: Affairs, April 23, 2025. URL: <https://monocle.com/affairs/poland-cyber-umbrella-elections/>.
19. Smith A. Europe braces for 'most extreme' military scenario as Trump-Putin 2.0 begins. NBC News. Jan. 26, 2025. URL: <https://www.nbcnews.com/news/world/trump-putin-europe-war-ukraine-attack-baltic-germany-finland-sweden-rcna187924>.
20. Commission unveils the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030. 19.03.2025. Press and information team of the Delegation to UKRAINE. URL: <https://cutt.ly/7rzaWF4d>.
21. YeS posylyuie oboronni spromozhnosti. Sluzhba zovnishnoi rozvidky Ukrainy. 21.03.2025. URL: <https://szru.gov.ua/news-media/news/ies-posylyuie-oboronni-spromozhnosti-1742515200000>.
22. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services. COM/2023/208 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208>.

Стаття надійшла до редакції 20.05.2025

УДК 351.86:351/354:327.56:005.56:341.232.1

Литвиненко Євгенія Віталіївна

PhD зі спеціальності 081 Право,

асистент кафедри кримінально-правових дисциплін та судочинства

Навчально-науковий інститут права

Сумський державний університет

Lytvynenko Yevheniia

PhD in the Specialty 081 Law

Assistant of the Department of Criminal Law Disciplines and Judiciary

Educational and Research Institute of Law

Sumy State University

ORCID: 0000-0002-4735-3722

DOI: 10.25313/2617-572X-2025-5-11024

КОМПАРАТИВНИЙ АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ МІЖВІДОМЧОЇ ВЗАЄМОДІЇ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В КРАЇНАХ, ЩО ПЕРЕБУВАЮТЬ У СТАНІ КОНФЛІКТУ АБО ПОСТКОНФЛІКТНОГО ВІДНОВЛЕННЯ¹

COMPARATIVE ANALYSIS OF EXISTING MODELS OF INTERAGENCY COOPERATION IN THE FIELD OF NATIONAL SECURITY IN COUNTRIES IN CONFLICT OR POST-CONFLICT RECOVERY

Анотація. Вступ. Сучасні безпекові виклики характеризуються складністю та взаємопов'язаністю, що унеможливорює їх вирішення зусиллями однієї агенції. Особливої актуальності набуває проблема ефективної міжвідомчої взаємодії для країн, що перебувають у стані конфлікту або постконфліктного відновлення, де необхідна тісна координація між військовими, цивільними та міжнародними структурами. Відсутність ефективних моделей такої взаємодії призводить до розрізнених зусиль, дублювання функцій, низької ефективності та загрози національній безпеці.

Мета. Компаративний аналіз моделей міжвідомчої взаємодії у сфері національної безпеки в США, Ізраїлі, Нігерії та Україні, виявлення їх сильних і слабких сторін, а також формулювання рекомендацій для підвищення ефективності координації в умовах конфлікту або постконфліктного відновлення.

Матеріали і методи. У дослідженні використано нормативно-правові документи, що регулюють міжвідомчу взаємодію у сфері національної безпеки обраних країн, аналітичні звіти міжнародних організацій та праці вітчизняних і зарубіжних науковців. Застосовано компаративний метод для порівняння досвіду різних країн, системний аналіз для виявлення структурних взаємозв'язків між елементами систем національної безпеки, синтез для формулювання універсальних принципів ефективної міжвідомчої взаємодії та метод кейс-стаді для дослідження конкретних прикладів успішної та неуспішної координації.

Результати. Визначено п'ять основних моделей міжвідомчої координації: централізована стратегічна, оперативна через інтеграцію персоналу, координація через формалізовані механізми, модель обміну інформацією та неформальна координація. Виявлено спільні виклики міжвідомчої взаємодії: відсутність чітких стратегій, організаційні відмінності між агенціями, нестача кваліфікованого персоналу, проблеми з обміном інформацією та відсутність формалізованих механізмів співпраці. Проаналізовано успішні практики координації у сфері національної безпеки в досліджуваних країнах та систематизовано фактори, що впливають на ефективність міжвідомчої взаємодії на організаційному, командному та індивідуальному рівнях.

¹ Робота виконана в рамках проекту «Інституційна консолідація через правову синергію: забезпечення національної безпеки в кризових умовах» (номер державної реєстрації 0125U001542)

Перспективи. Подальші дослідження доцільно спрямувати на розробку універсальної методології оцінки ефективності міжвідомчої взаємодії у сфері національної безпеки, вивчення правових механізмів формалізації міжвідомчої співпраці та дослідження впливу цифрових технологій на модернізацію систем координації безпекових структур в умовах гібридних загроз. Особливої уваги заслуговує вивчення мультимодальних моделей взаємодії, що поєднують традиційні ієрархічні структури з мережевими формами координації в умовах дефіциту часу та ресурсів.

Ключові слова: міжвідомча взаємодія, національна безпека, конфлікт, постконфліктне відновлення, координація.

Summary. Introduction. Modern security challenges are characterized by complexity and interconnectedness, making it impossible to address them through the efforts of a single agency. The problem of effective interagency coordination becomes particularly relevant for countries in conflict or post-conflict recovery, where close coordination between military, civilian, and international structures is necessary. The absence of effective models for such interaction leads to fragmented efforts, duplication of functions, low efficiency, and threats to national security.

Purpose. Comparative analysis of interagency coordination models in the national security sphere in the USA, Israel, Nigeria, and Ukraine, identifying their strengths and weaknesses, and formulating recommendations to enhance coordination effectiveness in conflict or post-conflict recovery conditions.

Materials and Methods. The study utilizes regulatory documents governing interagency coordination in the national security sphere of the selected countries, analytical reports from international organizations, and works by domestic and foreign scholars. A comparative method is applied to compare the experiences of different countries, systems analysis to identify structural relationships between elements of national security systems, synthesis to formulate universal principles of effective interagency coordination, and the case study method to examine specific examples of successful and unsuccessful coordination.

Results. Five main models of interagency coordination have been identified: centralized strategic, operational through personnel integration, coordination through formalized mechanisms, information exchange model, and informal coordination. Common challenges of interagency interaction were revealed: lack of clear strategies, organizational differences between agencies, shortage of qualified personnel, problems with information exchange, and absence of formalized cooperation mechanisms. Successful coordination practices in the national security sphere in the studied countries were analyzed, and factors affecting the effectiveness of interagency interaction at organizational, team, and individual levels were systematized.

Future Directions. Further research should focus on developing a universal methodology for evaluating the effectiveness of interagency coordination in national security, studying legal mechanisms for formalizing interagency cooperation, and researching the impact of digital technologies on modernizing coordination systems of security structures in the context of hybrid threats. Special attention should be given to studying multimodal interaction models that combine traditional hierarchical structures with network forms of coordination under time and resource constraints.

Key words: interagency cooperation, national security, conflict, post-conflict recovery, coordination.

Постановка проблеми. Сучасні безпекові виклики, такі як тероризм, кіберзагрози, транснаціональна злочинність та війни, характеризуються складністю та взаємопов'язаністю, що унеможливує їх вирішення зусиллями однієї агенції. Відсутність ефективних моделей міжвідомчої взаємодії призводить до розрізнених зусиль, дублювання функцій, низької ефективності та загрози національній безпеці. Особливо актуальною ця проблема є для країн, що перебувають у стані конфлікту або постконфліктного відновлення, де необхідна тісна координація між військовими, цивільними та міжнародними структурами.

Аналіз останніх досліджень і публікацій. Проблематика міжвідомчої взаємодії та управління безпекою вивчалась Терент'євою А. [6], яка досліджувала досвід Ізраїлю щодо безпеки цивільного населення в кризових ситуаціях. Питання міжнародної співпраці у сфері розвідки розглядали Petrova E. [7] та Chen M. [8], а Lopez M. [10] вивчав державно-приватне партнерство в обміні розвідданими. Nwagu J. та Mathias Z. [12] досліджували міжвідомчу взаємодію в Нігерії.

В українському контексті вагомими дослідження здійснили Поляков О. [17] щодо міжнародної співпраці у кібербезпеці, Жгут А. [18] про реформування безпекового сектору та Дука А., Старченко Г., Шапошникова І. [19], які проаналізували трансформацію візій національної безпеки в умовах війни.

Pendleton J. [5] досліджував рішення для зміцнення міжвідомчої співпраці в контексті безпеки.

Метою статті є компаративний аналіз моделей міжвідомчої взаємодії у сфері національної безпеки в США, Ізраїлі, Нігерії та Україні, виявлення їх сильних і слабких сторін, а також формулювання рекомендацій для підвищення ефективності координації в умовах конфлікту або постконфліктного відновлення.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення щодо регулювання міжвідомчої взаємодії у сфері національної безпеки (Закон про цивільну оборону Ізраїлю 1951 р., Закон України «Про Раду національної безпеки і оборони України», Указ Президента України «Про утворення Ставки Верховного Головнокомандувача»); 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження у царині національної безпеки та міжвідомчої координації, зокрема щодо моделей взаємодії в країнах,

що перебувають у стані конфлікту або постконфліктного відновлення; 3) офіційні звіти та аналітичні документи урядових структур (звіти GAO США, аналітичні матеріали безпекових відомств досліджуваних країн).

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для характеристики основних моделей міжвідомчої координації та їх функціональних особливостей, а також визначення спільних викликів міжвідомчої взаємодії у сфері національної безпеки); порівняльного аналізу (для зіставлення досвіду США, Ізраїлю, Нігерії та України щодо організації міжвідомчої взаємодії); формалізації, аналізу та синтезу (для виявлення структурних взаємозв'язків між елементами систем національної безпеки та формулювання універсальних принципів ефективної міжвідомчої взаємодії); кейс-стаді (для дослідження конкретних прикладів успішної та неуспішної координації в досліджуваних країнах); логічного узагальнення результатів (формулювання висновків та рекомендацій щодо підвищення ефективності міжвідомчої взаємодії в умовах конфлікту або постконфліктного відновлення).

Виклад основного матеріалу. Сучасні безпекові виклики характеризуються значною складністю та потребують комплексного підходу до їх вирішення. США, стикаючись з еволюціонуючими загрозами національній безпеці, розробили низку моделей міжвідомчої взаємодії, які застосовувалися в кризових регіонах. Особливо показовим є досвід американської міжвідомчої координації в контексті операцій в Іраку та Афганістані, де загрози мали дифузний, неоднозначний та взаємопов'язаний характер, що унеможливлювало їх вирішення зусиллями однієї агенції.

Для забезпечення комплексного підходу до стабілізаційних та реконструкційних операцій США залучали широкий спектр державних агентств, серед яких ключову роль відігравали Департамент оборони (DOD), відповідальний за військові операції та стабілізаційні зусилля; Державний департамент, що керував дипломатичними ініціативами та програмами розвитку урядових спроможностей; та Агентство США з міжнародного розвитку (USAID), зосереджене на гуманітарній допомозі та реконструкції. Допоміжні функції виконували також Департамент національної безпеки, Департамент юстиції, Департамент фінансів та інші відомства.

На основі американського досвіду виділяють п'ять ключових моделей міжвідомчої координації: модель стратегічної координації, що передбачає розробку всеохоплюючих стратегій з чітким розподілом ролей і механізмів взаємодії — її відсутність у 2007 році призвела до розрізнених зусиль щодо розвитку іракських міністерств [1]; оперативна координація через інтеграцію персоналу різних агенцій у спільні структури, успішно реалізована в Командуванні

США в Африці для розвитку партнерських спроможностей [2]; координація через формалізовані механізми для інституціоналізації співпраці, відсутність яких негативно позначилася на плануванні місій Північного командування США; модель обміну інформацією між агенціями, важливість якої підтвердив негативний досвід після урагану Катріна, коли втрачалася інформація про реконструкційні проекти; та неформальна координація, що залежить від особистих зв'язків і створює ризики для сталої взаємодії при ротації персоналу [3].

Досвід США в Іраку та Афганістані виявив п'ять системних викликів міжвідомчої взаємодії: відсутність чітких стратегій та розподілу ролей, що призвела до розрізнених зусиль у розвитку спроможностей іракського уряду [1]; організаційні відмінності між агенціями, включаючи різні структури регіональних підрозділів Державного департаменту та DOD, а також фінансування за відомствами, а не за функціями; нестача кваліфікованого персоналу, зокрема 31% дефіцит фахівців з іноземними мовами у Державному департаменті у 2009 році та брак кадрів у USAID для закордонних програм [4]; проблеми з обміном інформацією через відсутність процедур та обмеження безпеки, що створювало перешкоди для доступу неналежного до DOD персоналу до планувальних документів та ускладнювало використання несумісних біометричних даних [2]; відсутність формалізованих механізмів співпраці, що робила взаємодію залежною від особистих зв'язків та ускладнювала залучення інших агенцій до військового планування [5].

Незважаючи на численні виклики, досвід США демонструє і низку успішних практик міжвідомчої координації. Зокрема, інтеграція персоналу в Командуванні США в Африці значно покращила планування та координацію зусиль зі зміцнення партнерських спроможностей [2]. Цей підхід може бути адаптований і для операцій в конфліктних зонах, де необхідна тісна взаємодія між військовими та цивільними агенціями.

Іншим позитивним прикладом є створення центрів обміну інформацією (Fusion Centers), які після 2007 року були запроваджені у більшості штатів США для боротьби з тероризмом і значно покращили співпрацю між федеральними, штатними та місцевими органами [3]. Цей досвід може бути корисним для організації координації в конфліктних зонах.

Досвід США в Іраку та Афганістані демонструє, що ефективна міжвідомча взаємодія є складним процесом, який вимагає системного підходу, чіткого стратегічного бачення, адекватних ресурсів та відповідної організаційної культури. Аналіз цього досвіду може бути корисним для інших країн, що стикаються з подібними викликами у сфері національної безпеки в умовах конфлікту або постконфліктного відновлення [5].

У контексті дослідження моделей міжвідомчої взаємодії у сфері національної безпеки особливий інтерес становить досвід держав, які тривалий час функціонують в умовах безпосередніх загроз національній безпеці. Держава Ізраїль, що впродовж усього свого існування перебуває в стані конфлікту з сусідніми країнами та протистоїть терористичним загрозам, розробила унікальну систему забезпечення безпеки цивільного населення, яка базується на ефективній міжвідомчій координації.

Аналіз ізраїльського досвіду управління безпекою цивільного населення демонструє, що в умовах постійних екзистенційних загроз важливим є створення гнучких механізмів співпраці між військовими та цивільними структурами, поєднання централізованого управління з децентралізованою відповідальністю, а також залучення широких верств суспільства до процесів забезпечення національної безпеки.

Ізраїль стикається з постійними екзистенційними загрозами через географічне розташування, агресивне сусідство та обмежені ресурси. Основні загрози включають терористичні акти (заміновані автомобілі, вибухові пристрої в громадських місцях, захоплення літаків, автобусів, будівель), ракетні та бомбові атаки, зокрема балістичні ракети, потенційні атаки з використанням біологічної, хімічної чи радіоактивної зброї, а також природні та техногенні катастрофи [6, с. 312].

Ці загрози зумовили необхідність створення ефективної системи цивільної оборони, яка є невід'ємною частиною національної безпеки Ізраїлю. Система орієнтована на захист цивільного населення та критичної інфраструктури в умовах кризових ситуацій, що охоплюють як воєнні, так і невоєнні загрози. Управління безпекою в Ізраїлі базується на концепції «внутрішнього фронту» (тилу), яка інтегрує цивільний захист із військовими операціями, враховуючи незначний розподіл між фронтом і тилом через компактність території [6, с. 313].

Ізраїльська система управління безпекою цивільного населення включає п'ять основних моделей: 1) централізовану через Командування внутрішнього фронту, що координує цивільну оборону в складі ЦАХАЛ, розробляє нормативні документи, плани цивільної оборони, управляє службами екстреної допомоги та забезпечує інформування населення; 2) децентралізовану через місцеві органи влади, які відповідають за створення бомбосховищ, розробку планів реагування та захист критичної інфраструктури, співпрацюючи з Командуванням тилу, але маючи автономію в реалізації місцевих заходів; 3) економіку надзвичайних ситуацій, що забезпечує безперервне функціонування критичної інфраструктури в кризових ситуаціях через оперативні запаси ресурсів та координацію державних і приватних ресурсів; 4) спеціальний режим «Особлива ситуація в тилу», який надає Міністерству оборони право вводити обов'язкові розпорядження

для населення на 48 годин із можливістю подальшої ратифікації урядом у разі загрози безпеці; 5) волонтерську координацію, що передбачає залучення організацій ZAKA (1500 волонтерів) та Magen David Adom (26 тис. волонтерів) для реагування на кризові ситуації, включаючи ідентифікацію жертв, надання першої допомоги та пошуково-рятувальні операції.

На основі аналізу ізраїльського досвіду можна виділити ключові фактори ефективності управління безпекою цивільного населення на трьох рівнях: організаційному — чітка мета і стратегічний консенсус у захисті населення, підтримані концепцією «Iron Wall», значні інвестиції в оборонну інфраструктуру та механізм «Економіка надзвичайних ситуацій» [6], міцна нормативна база з Законом про цивільну оборону 1951 р.; командному — поєднання централізованої координації через Командування тилу з децентралізованими діями місцевих органів, висока культура співпраці та суспільна відповідальність, регулярні тренування персоналу служб реагування та волонтерів; та індивідуальному — ефективне поєднання професійних кадрів і волонтерів, психологічні винагороди для волонтерів і громадянська освіта населення, розподілене лідерство на місцевому рівні та стратегічне на національному [6].

Розглянувши досвід Ізраїлю у побудові ефективної системи безпеки доцільно звернути увагу на ситуацію в Нігерії. Ця західноафриканська держава, хоч і перебуває в іншому географічному та соціокультурному контексті, також зіткнулася з серйозними безпековими викликами. Дослідження нігерійського підходу до координації безпекових структур дозволить розширити розуміння різноманітності моделей міжвідомчої взаємодії в кризових умовах та виявити як універсальні принципи, так і унікальні регіональні особливості забезпечення безпеки населення.

Нігерія, як країна, що стикається з численними безпековими викликами, такими як тероризм, транснаціональна злочинність, кіберзагрози та піратство, представляє особливий інтерес для компаративного аналізу, оскільки перебуває в умовах тривалого конфлікту та часткового постконфліктного відновлення, особливо в північно-східних регіонах [7].

Нігерія стикається зі складними безпековими загрозами, які вимагають ефективної координації між численними внутрішніми та міжнародними агентствами. Транскордонний характер таких загроз, як тероризм, транснаціональна злочинність, кіберзагрози та піратство, робить міжвідомчу та міжнародну співпрацю критично важливою [8]. Основними внутрішніми агентствами, залученими до безпекової співпраці в Нігерії, є Департамент державної безпеки (DSS), який відповідає за внутрішню розвідку, контррозвідку та захист урядових осіб і критичної інфраструктури; Національне агентство розвідки (NIA), що зосереджене на зовнішніх загрозах; Агентство військової розвідки (DIA), яке

забезпечує військову розвідку; Нігерійська поліція (NPF), відповідальна за правоохоронну діяльність та підтримання громадського порядку; Комісія з економічних та фінансових злочинів (EFCC), що бореться з економічними злочинами; Нігерійська служба безпеки та цивільної оборони (NSCDC), зосереджена на національній безпеці та управлінні катастрофами; та Нігерійська митна служба (NCS), відповідальна за безпеку кордонів та митне регулювання.

Різноманітність мандатів цих агентств ускладнює координацію, особливо в умовах історичних проблем, таких як конкуренція між агентствами («*turf wars*»), брак довіри та ізольовані операції, що негативно впливає на загальну ефективність безпекової системи країни [9].

У Нігерії виділяють п'ять основних моделей міжвідомчої координації: централізована координація через Національну раду безпеки та Офіс радника з національної безпеки, що забезпечує стратегічне бачення, але має обмежену ефективність на оперативному рівні; оперативна координація через спільні групи, як-от Спільна оперативна група з боротьби з тероризмом, яка поєднує ресурси різних агентств, але може страждати від міжвідомчої конкуренції [7]; міжвідомча співпраця з міжнародними партнерами (ФБР, Інтерпол, МІ6), що забезпечує доступ до передових технологій, але стикається з проблемами довіри; публічно-приватне партнерство з охоронними фірмами, особливо ефективне проти кіберзлочинності та викрадень; і традиційна силосна модель, коли агентства працюють ізольовано, що призводить до дублювання зусиль і низької ефективності, як у випадку з викраденням школярів у Чібоку [10].

Попри виклики, Нігерія демонструє успішні приклади міжвідомчої координації: спільна операція нігерійських та американських розвідувальних агентств у 2018 році, що допомогла зірвати діяльність «Боко Харам» завдяки обміну супутниковими даними; затримання ключового підозрюваного «Боко Харам» у 2014 році завдяки співпраці SSS та Держдепартаменту США; ліквідація наркоторгівельної мережі у 2021 році через співпрацю з Інтерполом; успішна взаємодія з приватним сектором для затримання банди викрадачів у 2021 році; запобігання теракту в Абуджі у 2014 році завдяки інформації від МІ6. Водночас, міжвідомча взаємодія стикається з серйозними викликами: брак довіри та конкуренція між агентствами, що призводить до ізольованих операцій; бюрократичні перешкоди через відсутність стандартизованих протоколів комунікації; технологічні обмеження та нерівність можливостей між агентствами [10]; відсутність чітких правових рамок для обміну розвідданими [11]; проблеми міжнародної співпраці через побоювання витоків інформації та різні правові системи [12].

Проаналізувавши нігерійський досвід забезпечення безпеки цивільного населення з його спе-

цифічними викликами, пов'язаними з діяльністю терористичних угруповань, етнорелігійними конфліктами та обмеженими ресурсами, доцільно розглянути особливий український приклад. Україна, перебуваючи в умовах повномасштабної війни з Російською Федерацією, розробила багаторівневу систему міжвідомчої координації, яка демонструє ефективні механізми адаптації та реагування на безпрецедентні загрози національній безпеці в європейському контексті. Україна демонструє унікальний кейс моделей міжвідомчої взаємодії в умовах збройного конфлікту з РФ, що включає п'ять ключових типів координації: 1) централізована через РНБО як стратегічний координаційний орган, що посилала свою роль з 2014 року [13;14]; 2) оперативно-стратегічна через Ставку Верховного Головнокомандувача, відновлену в 2022 році для військової координації [15]; 3) тактична через міжвідомчі оперативні штаби для вирішення конкретних завдань, як-от розмінування чи евакуація; 4) міжнародна координація з партнерами через такі механізми як 2Рамштайн та JMCC [16]; 5) публічно-приватне партнерство із залученням бізнесу та волонтерів, зокрема з IT-компаніями у сфері кібербезпеки та Army SOS у розробці дронів [17].

Успішними прикладами такої взаємодії є деокупація територій у 2022 році, евакуація цивільних, протидія кібератакам, інтеграція розвідувальних даних України та відновлення енергетичної інфраструктури [18].

Основними викликами залишаються пострадянська бюрократія, правові перешкоди, технологічні обмеження, реформування в умовах війни та кадрові проблеми. Рекомендовано створення єдиної інформаційної платформи, впровадження спільних стандартів, проведення міжвідомчих навчань, спільну підготовку кадрів, посилення громадського контролю, інституціоналізацію державно-приватного партнерства та адаптацію структур до нових викликів [19].

Висновки і перспективи подальших досліджень. Аналіз досвіду США, Ізраїлю, Нігерії та України показав, що ефективна міжвідомча взаємодія залежить від чіткого стратегічного бачення, стандартизованих протоколів, достатнього кадрового забезпечення та залучення суспільства. Кожна країна демонструє унікальні підходи, але спільними викликами є міжвідомча конкуренція, бюрократія та обмежені ресурси. Для підвищення ефективності рекомендуються створення єдиних інформаційних платформ, регулярні міжвідомчі навчання та інституціоналізація державно-приватного партнерства.

На основі компаративного аналізу досвіду США, Ізраїлю, Нігерії та України доцільно запропонувати рекомендації щодо підвищення ефективності міжвідомчої взаємодії у сфері національної безпеки: розробка єдиної міжвідомчої стратегії; формалізація розподілу відповідальності між відомствами;

забезпечення політичного керівництва процесами координації; створення єдиної інформаційної платформи; впровадження стандартизованих протоколів взаємодії; розробка механізмів координації для кризових ситуацій; проведення міжвідомчих навчань; інтеграція персоналу в спільні групи; підготовка фахівців з навичками міжвідомчої взаємодії; забез-

печення технічної сумісності інформаційних систем; впровадження захищених систем обміну даними; інституціоналізація державно-приватного партнерства; адаптація міжнародних стандартів взаємодії. Імплементація має враховувати специфіку кожної країни, її політичну систему, ресурси та культурні особливості.

Література

1. Stabilizing and Rebuilding Iraq: U.S. Ministry Capacity Development Efforts Need an Overall Integrated Strategy to Guide Efforts and Manage Risk. GAO. 2008. URL: <https://www.gao.gov/assets/gao-08-568t.pdf> (дата звернення: 01.05.2025).
2. Defense Management: Actions Needed to Address Stakeholder Concerns, Improve Interagency Collaboration, and Determine Full Costs Associated with the U.S. Africa Command. GAO. 2009. URL: <https://www.gao.gov/assets/gao-09-181.pdf> (дата звернення: 01.05.2025).
3. Homeland Defense: U.S. Northern Command Has Made Progress but Needs to Address Force Allocation, Readiness Tracking Gaps, and Other Issues. GAO. 2008. URL: <https://www.gao.gov/assets/gao-08-251.pdf> (дата звернення: 01.05.2025).
4. Department of State: Comprehensive Plan Needed to Address Persistent Foreign Language Shortfalls GAO. 2009. URL: <https://www.gao.gov/assets/gao-09-955.pdf> (дата звернення: 01.05.2025).
5. Pendleton J. H. National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration, United States Government Accountability Office, Washington. 2010. 22 p.
6. Терент'єва А. Досвід Держави Ізраїль щодо управління безпекою цивільного населення в умовах кризових ситуацій. *Науковий вісник: Державне управління*. 2023. № 2 (14). С. 310–333.
7. Petrova E. Cooperation and Sharing of Intelligence: A Study of Interagency Collaboration in Nigeria. *Cambridge University Press*, UK. 2023.
8. Chen M. The Expanding Role of Intelligence in the Digital Age. *National University Press*, Singapore. 2023.
9. Vanguardngr.ng Siloed Operations Hinder Effective Intelligence Sharing in Nigeria. 2024.
10. Lopez M. Public-Private Partnerships for Intelligence Sharing: Benefits and Challenges. *Universidad Nacional Autónoma de México Press*, Mexico. 2023.
11. Adams L. International Law Enforcement Cooperation in Nigeria. *Taylor & Francis*, UK. 2016.
12. Nwagu J. A., Mathias Z., The Cooperation and Sharing of Intelligence: A Study of Interagency Collaboration in Nigeria. *Global scientific journal*. March 2024. Vol. 12, Issue 3. P. 883–898.
13. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР. *Відомості Верховної Ради України*. 1998. № 35, ст. 237.
14. *Офіційний сайт РНБО України*. URL: <https://www.rnbo.gov.ua/> (дата звернення: 01.05.2025).
15. Про утворення Ставки Верховного Головнокомандувача : Указ Президента України від 24.02.2022 № 72/2022.
16. War Speeches. Дипломатичні й політичні підсумки війни Росії проти України в листопаді. *Українська правда*. 2023. URL: <https://www.pravda.com.ua/columns/2023/12/6/7431886/> (дата звернення: 01.05.2025).
17. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.
18. Жгут А. В. Міжнародне співробітництво в реформуванні безпекового сектору. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2021.
19. Дука, А. П., Старченко, Г. В., Шапошникова І. В. Трансформація візій національної безпеки в умовах військової агресії. *Проблеми сучасних трансформацій*. 2023. № 8. <https://doi.org/10.54929/2786-5746-2023-8-02-06>.

References

1. Stabilizing and Rebuilding Iraq (2008): U.S. Ministry Capacity Development Efforts Need an Overall Integrated Strategy to Guide Efforts and Manage Risk. GAO. URL: <https://www.gao.gov/assets/gao-08-568t.pdf>.
2. Defense Management (2009): Actions Needed to Address Stakeholder Concerns, Improve Interagency Collaboration, and Determine Full Costs Associated with the U.S. Africa Command. GAO. URL: <https://www.gao.gov/assets/gao-09-181.pdf>.
3. Homeland Defense (2008): U.S. Northern Command Has Made Progress but Needs to Address Force Allocation, Readiness Tracking Gaps, and Other Issues. GAO. URL: <https://www.gao.gov/assets/gao-08-251.pdf>.
4. Department of State (2009): Comprehensive Plan Needed to Address Persistent Foreign Language Shortfalls GAO. URL: <https://www.gao.gov/assets/gao-09-955.pdf>.

5. Pendleton J. H. (2010) National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration, United States Government Accountability Office, Washington. 22 p.
6. Terent'yeva A. (2023) The Experience of the State of Israel in Managing Civilian Security in Crisis Situations. *Scientific Bulletin: Public Administration*. № 2 (14). P. 310–333 [in Ukrainian].
7. Petrova E. (2023). Cooperation and Sharing of Intelligence: A Study of Interagency Collaboration in Nigeria. *Cambridge University Press*.
8. Chen M. (2023). The Expanding Role of Intelligence in the Digital Age. *National University Press*.
9. Vanguardngr.ng (2024). Siloed Operations Hinder Effective Intelligence Sharing in Nigeria.
10. Lopez M. (2023). Public-Private Partnerships for Intelligence Sharing: Benefits and Challenges. *Universidad Nacional Autónoma de México Press*.
11. Adams L. (2016). International Law Enforcement Cooperation in Nigeria. *Taylor & Francis*.
12. Nwagu J. A., Mathias Z., (2024). The Cooperation and Sharing of Intelligence: A Study of Interagency Collaboration in Nigeria. *Global scientific journal*. Volume 12, Issue 3. P. 883–898.
13. On the National Security and Defense Council of Ukraine: Law of Ukraine of 05.03.1998 № 183/98-VR. *Bulletin of the Verkhovna Rada of Ukraine*. 1998. № 35, Cr. 237 [in Ukrainian].
14. Official website of the National Security and Defense Council of Ukraine. URL: <https://www.rnbo.gov.ua/> [in Ukrainian].
15. On the establishment of the Supreme Commander-in-Chief's Staff: Decree of the President of Ukraine of 24.02.2022 № 72/2022 [in Ukrainian].
16. War Speeches (2023). Diplomatic and political results of Russia's war against Ukraine in November. *Ukrainska Pravda*. URL: <https://www.pravda.com.ua/columns/2023/12/6/7431886/> [in Ukrainian].
17. Polyakov O. M. (2021). Activation of international cooperation in the field of cybersecurity: ways to improve in today's realities. *Information and Law*. № 2 (37). P. 129–138 [in Ukrainian].
18. Zhgut A. V. (2021). International cooperation in reforming the security sector. *Bulletin of the Student Scientific Society of Vasyli' Stus Donetsk National University* [in Ukrainian].
19. Duka A. P., Starchenko, G. V., Shaposhnikova, I. V. (2023). Transformation of visions of national security in the conditions of military aggression. *Problems of modern transformations*. № 8. <https://doi.org/10.54929/2786-5746-2023-8-02-06> [in Ukrainian].

Стаття надійшла до редакції 02.05.2025

УДК 327:007

Шемаєв Володимир Миколайович

*доктор військових наук, професор,
доцент кафедри інформаційної безпеки держави
Навчально-науковий інститут інформаційної безпеки
та стратегічних комунікацій НА СБ України*

Shemayev Volodymyr

*Doctor of Military Sciences, Professor,
Associate Professor of the Department of Information Security of the State;
Educational and Scientific Institute of Information Security and Strategic
Communications of the National Academy of Security Service of Ukraine
ORCID: 0009-0003-2568-5587*

Єрємінна Людмила Валеріївна

*старший виклад кафедри інформаційної безпеки держави
Навчально-науковий інститут інформаційної безпеки
та стратегічних комунікацій НА СБ України*

Yeromina Lyudmila

*Senior Lecture of the Department of Information Security of the State
Educational and Scientific Institute of Information Security
and Strategic Communications of the Security Service of Ukraine
ORCID: 0009-0009-1656-2546*

DOI: 10.25313/2617-572X-2025-5-11029

«PORCUPINE STRATEGY» ДЛЯ УКРАЇНИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

“PORCUPINE STRATEGY” FOR UKRAINE IN THE CONTEXT OF ENSURING NATIONAL SECURITY

Анотація. Вступ. Одним із пріоритетів формування ефективної європейської оборони в сучасних умовах є нарощування оборонної підтримки України у її боротьбі проти російської агресії, оскільки сильна Україна буде здатною стримати таку агресію у майбутньому та допомогти Європі у зміцненні власної безпеки. В контексті питання гарантій безпеки Україні після закінчення війни найпопулярнішою є концепція «Porcupine Strategy» (стратегія дикобразу). Ця стратегія передбачає створення потужної оборонної спроможності країни, яка робить її максимально складною та витратною для агресора в разі вторгнення. Водночас, ця стратегія орієнтована на те, аби мати гнучкі мобільні сили, які шляхом швидкості й маневровості можуть стримувати просування противника. Головна мета цієї стратегії – створити такі умови, щоб агресія стала невігідною, а вартість нападу перевищувала будь-які можливі вигоди. Тому актуальності набуває аналіз потенційного впливу різних аспектів створюваної Україною спільно з міжнародними партнерами «Стратегії дикобразу» на складові національної безпеки з огляду на необхідність використання можливостей для її забезпечення та попередження розгортання загроз національній безпеці.

Мета. Метою статті є визначення змісту та особливостей реалізації «Стратегії дикобразу» в Україні через призму її впливу на різні складові національної безпеки та обґрунтування пріоритетів державної політики щодо превентивного захисту від зазначених загроз.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення національної безпеки України; 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження у царині можливостей та ризиків використання «Стратегії дикобразу» щодо його застосування в Тайвані та Україні.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для характеристики змісту та ризиків використання «Стратегії дикобразу»; аналізу та синтезу (для характеристики поточного ландшафту особливостей «Стратегії дикобразу» в Україні з точки зору можливостей та загроз для національної безпеки); логічного узагальнення (визначення контрзаходів, які поєднують технологічну, нормативну та освітню сфери для ефективної реалізації «Стратегії дикобразу» в Україні).

Результати. У науковій статті визначено та проаналізовано досвід використання Тайваню щодо «Стратегії дикобразу» та особливості його застосування для України як в умовах війни, так і післявоєнному відновленні.

Визначено, як реалізація «Стратегії дикобразу» впливає/впливатиме на різні складові національної безпеки України, зокрема на: воєнну, економічну, науково-технологічну, енергетичну, інформаційну та державну безпеку.

Обґрунтовано шляхи протидії ризикам зниження ефективності реалізації «Стратегії дикобразу» у воєнній та економічній сферах. Обґрунтовано необхідність корегування видів озброєння (не тільки мобільні засоби, але й засоби стратегічного стримування противника) відповідно до реалій Збройних сил України.

Перспективи. Перспективою подальших досліджень за цим напрямом є дослідження чинників зміцнення та ризиків для національної безпеки за окремими напрямками, пов'язаних із реалізацією «Стратегії дикобразу».

Ключові слова: національна безпека, Porcupine Strategy (Стратегія дикобразу), можливості, загрози, асиметрична тактика.

Summary. Introduction. One of the priorities for the formation of effective European defense in modern conditions is to increase defense support for Ukraine in its fight against Russian aggression, since a strong Ukraine will be able to deter such aggression in the future and help Europe strengthen its own security. In the context of the issue of security guarantees for Ukraine after the end of the war, the most popular concept is the "Porcupine Strategy". This strategy involves the creation of a strong defense capability of the country, which makes it as difficult and costly as possible for the aggressor in the event of an invasion. At the same time, this strategy is focused on having flexible mobile forces that, through speed and maneuverability, can hold back the enemy's advance. The main goal of this strategy is to create such conditions so that aggression becomes unprofitable, and the cost of an attack exceeds any possible benefits. Therefore, the analysis of the potential impact of various aspects of the "Porcupine Strategy" created by Ukraine together with international partners on the components of national security becomes relevant, taking into account the need to use opportunities to ensure it and prevention of the deployment of threats to national security.

Purpose. The article is aimed at determining the content and features of the implementation of the "Porcupine Strategy" in Ukraine through the prism of its impact on various components of national security and substantiating the priorities of state policy on preventive protection against these threats.

Materials and methods. The materials of the study are: 1) regulatory and legal support for ensuring the national security of Ukraine; 2) works of domestic and foreign authors who conduct their scientific and practical research in the field of opportunities and risks of using the "Porcupine Strategy" for its application in Taiwan and Ukraine.

In the process of the study, the following scientific methods were used: theoretical generalization and grouping (to characterize the content and risks of using the "Porcupine Strategy"); analysis and synthesis (to characterize the current landscape of the features of the "Porcupine Strategy" in Ukraine in terms of opportunities and threats to national security); logical generalization (identification of countermeasures that combine technological, regulatory and educational spheres for the effective implementation of the "Porcupine Strategy" in Ukraine).

Results. The scientific article identifies and analyzes the experience of using Taiwan in relation to the "Porcupine Strategy" and the features of its application for Ukraine both in war conditions and post-war recovery.

It is determined how the implementation of the "Porcupine Strategy" affects/will affect various components of Ukraine's national security, in particular: military, economic, scientific and technological, energy, information and state security.

Ways to counteract the risks of reducing the effectiveness of the implementation of the "Porcupine Strategy" in the military and economic spheres are substantiated. The need to adjust the types of weapons (not only mobile means, but also means of strategic deterrence of the enemy) in accordance with the realities of the Armed Forces of Ukraine is substantiated.

Prospects. The prospect of further research in this area is the study of strengthening factors and risks to national security in certain areas related to the implementation of the "Porcupine Strategy".

Key words: national security, Porcupine Strategy, opportunities, threats, asymmetric tactics.

Постановка проблеми. Одним із пріоритетів формування ефективної європейської оборони в сучасних умовах є нарощування оборонної підтримки України у її боротьбі проти російської агресії, оскільки сильна Україна буде здатною стримати таку агресію у майбутньому та допомогти Європі у зміцненні власної безпеки. В контексті питання гарантій безпеки Україні після закінчення війни

найпопулярнішою є концепція «Porcupine Strategy» (стратегія дикобразу).

«Porcupine Strategy» (стратегія дикобразу) узагальнено передбачає створення потужної оборонної спроможності країни, яка робить її максимально складною та витратною для агресора в разі вторгнення. Водночас, ця стратегія орієнтована на те, аби мати гнучкі мобільні сили, які шляхом швидкості й маневровості

можуть стримувати просування противника. Головна мета цієї стратегії — створити такі умови, щоб агресія стала не вигідною, а вартість нападу перевищувала будь-які можливі вигоди. Тому актуальності набуває аналіз потенційного впливу різних аспектів створеної Україною спільно з міжнародними партнерами «Стратегії дикобразу» на складові національної безпеки з огляду на необхідність використання можливостей для її забезпечення та попередження розгортання загроз національній безпеці.

Аналіз останніх досліджень і публікацій. В останні роки у науковій літературі проблема розробки та застосування стратегій дикобразу для Тайваню та України в контексті оборонної стратегії та тактики, розглядається, переважно, зарубіжними дослідниками, зокрема, такими як: Марк Кансіан, Метью Кансіан, Ерік Хегінботам — аналіз сценаріїв ймовірного вторгнення КНР на Тайвань із рекомендаціями доповнення Стратегії дикобразу засобами стримування [1], Вільям С. Мюррей — рекомендації та обґрунтування перегляду оборонної стратегії для Тайваню внаслідок військової модернізації Китаю, що значно зменшила географічну перевагу Тайваню і неможливості його розраховувати на симетричну протидію китайським військовим силам за допомогою перехоплювачів Patriot, дизельних підводних човнів, надводних військових кораблів, винищувачів F-16 та морських патрульних літаків P-3 [2], Кеннет Фанн, Чарльз Бурсі — дослідження сценарію, якщо/коли Китай спробує возз'єднатися з Тайванем та як США виконуватимуть свої зобов'язання щодо його захисту за допомогою Стратегії дикобразу [3], Брент Купер — дослідження змісту «Стратегії дикобразу» та аналіз того, як ця оборонна стратегія Тайваню може стримати Китай [4], Франц Стефан Гаді — аналіз застосування Стратегії дикобразу для озброєння України з метою запобігання повторного нападу з боку РФ [5], Йошіакі Нішімі — аналіз того, як Тайвань може стримати «хижака, більшого за себе» завдяки «Стратегії дикобразу» [6], Лі Сі Мін та Ерік Лі — дослідження оборонної стратегії Тайваню у середовищі з обмеженими ресурсами у часи зростаючої активності у зовнішній політиці Пекіна та зростання ризику військового конфлікту [7], К. Бондар — дослідження шляхів інтеграції України в оборонно-промислову базу Заходу [8] та інші.

Виділення невирішених раніше частин загальної проблеми. Водночас з огляду на специфіку оборонного, економічного, ресурсного потенціалу України, потребу визначення впливу можливостей і ризиків застосування «Стратегії дикобразу» на національну безпеку України.

Метою дослідження є визначення змісту та особливостей реалізації «Стратегії дикобразу» в Україні через призму її впливу на різні складові національної безпеки та обґрунтування пріоритетів державної політики щодо превентивного захисту від зазначених загроз.

Виклад основного матеріалу дослідження.

Вперше про «Стратегію дикобразу» згадувалося на початку 2000-х років у запропонованій військовій доктрині для оборони Тайваню (у разі вторгнення Китайської Народної Республіки). Використання образу дикобразу трактувалося через відомий добродушний характер цієї тваринки, яка, здається, є легкою здобиччю для войовничого хижака. Але коли бачиш голки дикобраза, легко уявити, з якими труднощами стикається хижак у атаці — а тим більше виграші — в бою з дикобразом. Необхідність для Тайваню розробити оборонну стратегію, засновану на асиметричній війні, а також використання термінології «дикобраз» для її позначення, була визначена ще у 2008 році, коли Вільям С. Мюррей, офіцер ВМС США у відставці, опублікував статтю в Naval War College Review, в якій закликав Тайвань «переосмислити та змінити свою оборонну стратегію», відмовившись від прямого знищення сил вторгнення, яке він вважав неможливим через військовий прогрес Китаю, та перейшовши до більш загальної мети протистояння китайській окупації острова [2]. Стратегія загалом передбачала акцент на веденні асиметричної війни проти переважаючих китайських сил. Як наслідок, пропонувалося необхідність інвестування в малодіючі, переносні системи, такі як ракети Stinger та Harpoon, морські міни поблизу берега та ударні гелікоптери; збільшення розгортання ракет малої дальності та великої кількості малих військово-морських суден, здатних ховатися серед рибальських човнів, серед іншої асиметричної зброї [7]. Доктрина набула популярності наприкінці 2010-х років, коли тодішній начальник оборони Тайваню адмірал Лі Сі-мін включив цей принцип до офіційної стратегії, яку він назвав Загальною концепцією оборони, яку до 2019 року схвалила тодішня президентка Цай Інвень [7].

Однак політичне та військове керівництво Тайваню не вважає, що «асиметрична» зброя є синонімом «великої кількості дрібних речей». Під «асиметричною» зброєю вважаються також підводні човни, винищувачі F-16 та танки, незважаючи на їхню високу вартість та вразливість. Зокрема, у Чотирирічному огляді оборони, опублікованому Міністерством оборони Тайваню у березні 2021 року, згадуються також цілі нарощування сил, включаючи можливості ударів на великій дальності, перевагу в повітрі та контроль на морі.

Нова адміністрація ще більше наголосила на високотехнологічних інвестиціях у безпілотники, ракети класу «земля-повітря» та наземні протикорабельні ракети, замість того, щоб вкладати гроші у великі військові кораблі та літаки. Це важливо не лише з огляду на критику програми розвитку підводних човнів Цай та продовження закупівель звичайної зброї під час її перебування на посаді, але й враховуючи історію недостатнього інвестування Тайванем свого оборонного сектору. Таким чином,

стратегія «дикобраза» пропонує більш доступний варіант, зменшуючи тиск на уряд Тайваню щодо подальшого збільшення витрат на оборону.

Важливо зазначити, що Тайвань вже зробив кілька кроків у цьому напрямку. Особливої уваги заслуговує впровадження Тайванем у 2023 році кількох вітчизняних військових безпілотників, оснащених бойовими або спостережливими можливостями, які можна використовувати в різних військових підрозділах. Тайвань також виробляє ракети повітряної та морської оборони, малі ракетні корвети та мінні загороджувальні кораблі.

Отже, спираючись на уроки, отримані під час японського вторгнення наприкінці 1800-х років, у політичному істеблішменті Тайваню знову виникли дискусії щодо асиметричної оборони. Концепція асиметричної війни, яку також називають «Стратегією дикобраза», базується на ідеї досягнення стримування шляхом заперечення, що робить вторгнення дорогим для Китаю. Більше того, навіть якщо стримування не спрацює, вважається, що асиметрична оборона надає Тайваню кращі шанси витримати бій у його прибережних районах, а війна в Україні ще раз підкреслила переваги асиметричної оборони під час взаємодії з військово переважаючою державою.

Цей підхід набув особливої актуальності в Україні ще до повномасштабного вторгнення 2022 року. «Стратегія дикобраза» частково впроваджувалася (реформа армії, закупівля західного озброєння), але не в повному обсязі. А після повномасштабного вторгнення Росії в Україну у 2022 році в Україні «Стратегія дикобраза» діє де-факто за рахунок: масованої підтримки Заходу; масштабної мобілізації суспільства; гнучких тактичних рішень (удари по тилу ворога, використання FPV-дронів тощо); адаптації технологій (старлінки, автоматизоване управління вогнем тощо).

У березні 2025 року Європейська комісія окреслила двоетапну «Porcupine Strategy» (стратегію дикобраза), що передбачає створення потужної оборонної спроможності країни, яка робить її максимально складною та витратною для агресора в разі вторгнення. Головна мета цієї стратегії — створити такі умови, щоб агресія стала не вигідною, а вартість нападу перевищувала будь-які можливі вигоди [8].

У контексті війни в Україні «Стратегія дикобраза» може бути реалізована через: 1) зміцнення оборони за рахунок постачання західної зброї (передача танків, систем ППО та сучасної авіації, таких як F-16, спрямована на посилення оборонного потенціалу країни); 2) асиметричну тактику використання Україною високоточних дронів, мобільних артилерійських установок та протитанкових систем, які дозволяють ефективно протистояти чисельно сильнішому ворогу; 3) підготовку населення до захисту через масштабне розгортання територіальної оборони та мобілізація громадян для підтримки військових операцій. Для реалізації цієї стратегії в ЄС формується

план щодо подвоєння військової допомоги Україні у 2025 році до 40 млрд. євро (44 млрд. дол. США).

Розглянемо далі як «Стратегія дикобраза» впливає/впливатиме на різні складові національної безпеки України — це, перш за все, концепція її оборонної стратегії, яка передбачає створення такого рівня обороноздатності держави, щоб будь-який напад на неї став для агресора занадто болючим, дорогим і не вигідним, незалежно від його військової потуги.

Отже, в контексті впливу «Стратегії дикобраза» на зміцнення воєнної безпеки України доцільно розглядати основні принципи реалізації цієї стратегії, зокрема:

1. Оборонна асиметрія: замість гонки озброєнь з набагато сильнішим ворогом (РФ), акцент робиться на використанні недорогих, мобільних, ефективних засобів стримування (ПТРК, дрони, мобільна артилерія, мінування, тощо). Приклад — активне використання Javelin, NLAW, Bayraktar, FPV-дронів.

2. Масштабування територіальної оборони: війна має стати всенародною: кожен регіон, населений пункт, навіть окремих будинок має бути здатен до оборони; розвиток системи територіальної оборони ЗСУ, партизанських структур, громадянської підготовки.

3. Стратегічна глибина та мобільність: забезпечення глибини оборони, включаючи здатність швидко маневрувати, змінювати позиції, атакувати у відповідь; важливість логістики, мобільного зв'язку, цифрових платформ управління боєм.

4. Насичення технологіями: розвиток дронів, кіберзахисту, штучного інтелекту, спостереження, протиповітряної оборони. Війна майбутнього — це війна дронів, інформації та електронної переваги.

Опосередкований вплив на економічну та науково-технологічну складові національної безпеки здійснює такий аспект реалізації «Стратегії дикобраза», як розвиток внутрішнього військово-промислового комплексу: зменшення залежності від імпорту зброї та розвиток власних технологій. У 2022 році українська оборонна промисловість була спроможна виробляти оборонне обладнання на суму близько 1 млрд. євро на рік, а 2024 рік вона завершила з показником виробництва близько 15 млрд. дол. США, але сектор має потужності для виробництва 35 млрд. дол. США.

При цьому Україна все ще не використовує свої спроможності повною мірою для того, щоб задовольняти навіть потреби самої України, оскільки українським промисловим підприємствам гостро бракує оборонних контрактів. У цьому контексті велику користь може принести продовження «данської моделі», коли європейська допомога спрямовується на українські підприємства для виробництва озброєння для української армії.

Підтримка локалізації оборонного виробництва в Україні з боку ЄС також стане інвестицією в безпеку держав-членів і покращить становище їхньої

промисловості. Однак, існує кілька перешкод для подальшої локалізації та інтеграції, а саме:

- потрібен захист інфраструктури оборонного виробництва, що має першорядне значення. Розсіювання та маскування наразі забезпечують певний захист, але протиповітряна оборона України з великим напруженням перехоплює російські безпілотники та ракети [10];
- існують ризики інвестування в Україну, пов'язані із практикою глобальних корпоративних страховиків, зазвичай, виключати країни, що перебувають у стані війни, зі своїх полісів [11]. Щоб компенсувати ці ризики держави-члени можуть надати «механізми страхування військових ризиків», які, як повідомляється, вже передбачені Францією та Великобританією, для забезпечення покриття витрат західних оборонних компаній. Спільні підприємства, локалізовані в державах-членах, близьких до України, також можуть отримати таку підтримку [8];
- оборонна промисловість України відчуває нестачу кваліфікованих робітників та менеджерів, стикається з відсутністю адекватного нормативного середовища, а також від проявів корупції та ризиків промислового шпигунства.

Отже, Україна має спрямувати свої зусилля на ефективне та прозоре корпоративне управління, нормативно-правове врегулювання в оборонній сфері, яке б виключало можливості хабарництва, порушень прав інтелектуальної власності, а також забезпечувало надійну політику в галузі оборонної промисловості та процесу закупівель. Деякі держави-члени ЄС, такі як Швеція, вже надають підтримку створенню та розвитку сучасної організації оборонних закупівель в Україні.

Важливою складовою національної безпеки, на яку впливає «Стратегія дикобраза» стає енергетична безпека та енергетична незалежність, оскільки стратегія передбачає підвищення стійкості до атак на інфраструктуру, таких як обстріли енергосистеми. Стійкість функціонування енергетичного сектору — це спроможність енергетичного сектору функціонувати у штатному режимі адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після реалізації загроз будь-якого виду.

«Стратегія дикобраза» також відчутно позитивно впливає на інформаційну безпеку держави через підвищення кібербезпеки та інформаційної стійкості держави та суспільства, як вміння адаптуватися до нових викликів і загроз та швидко відновлюватися, вміння вибирати моделі гнучкості та стійкого опору й уміння адекватно реагувати на природні й політичні катаклізми.

Реалізація «Стратегії дикобраза» відчутно вплине на забезпечення державної безпеки, в т.ч. державно-політичного, конституційно легітимізованого політичного ладу держави від змін його неконституційним шляхом; державотворення і конструктивної політики задля стабільності суспільства; політичного суверенітету; територіальної цілісності України і недоторканності її кордонів; інститутів державної влади; національно-державних інтересів у сфері економіки задля ефективної реалізації соціального призначення держави — забезпечення подальшого розвитку особи, суспільства та держави напряму залежить від психологічної мобілізації населення на супротив ворогу: ворог має знати, що навіть окупація території не дасть йому контролю через спротив, якій триватиме, оскільки нація об'єднана, мотивована і не готова здаватися.

Висновок. Отже, реалізація «Стратегії дикобраза» в Україні здатна позитивно вплинути на різні складові національної безпеки: воєнну, зовнішньополітичну, економічну, науково-технологічну, енергетичну, інформаційну та державну. Водночас, «Стратегія дикобраза», про яку йде мова в «Білій книзі»-2025 в ЄС, є недостатньою для реальних оборонних можливостей України. Тому що «Стратегія дикобраза» орієнтована на те, аби мати гнучкі мобільні сили, які шляхом швидкості й маневровості можуть стримувати просування противника. Водночас в українських реаліях ця стратегія має бути стратегія є недостатньою для наших умов, має враховувати ті рішення, які ми сьогодні досягли шляхом розвитку далекобійних дронів, створення власного ударного озброєння.

Перспективою подальших досліджень за цим напрямом має бути дослідження чинників зміцнення та ризиків для національної безпеки за окремими напрямами, пов'язаних із реалізацією «Стратегії дикобраза» в Україні.

Література

1. Cancian M., Cancian M., Heginbotham E. The First Battle of the Next War. Washington, DC: Center for Strategic & International Studies. URL: <https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan> (дата звернення: 10.05.2025).
2. Murray W.S. Revisiting Taiwan's Defense Strategy, Naval War College Review: Vol. 61: No. 3, Article 3. URL: <https://digital-commons.usnwc.edu/nwc-review/vol61/iss3/3> (дата звернення: 10.05.2025).
3. Fann K., Bursi Ch. Protecting the Porcupine: Why Taiwan Matters | Epicenter. URL: <https://epicenter.wcfia.harvard.edu/blog/protecting-porcupine-why-taiwan-matters> (дата звернення: 10.05.2025).

4. Cooper B. What is “porcupine strategy”? How can Taiwan’s crazy porcupine defence strategy deter China? URL: <https://www.quora.com/What-is-porcupine-strategy-How-can-Taiwans-crazy-porcupine-defence-strategy-deter-China> (дата звернення: 10.05.2025).
5. Franz-Stefan Gady. URL: <https://foreignpolicy.com/2023/05/22/ukraine-russia-war-weapons-nato-f16-tanks-deterrence-peace-strategy/> (дата звернення: 10.05.2025).
6. Yoshiaki Nishimi Taiwan Military Expert: ‘Porcupine Strategy’ Could Deter Chinese Invasion. URL: <https://japan-forward.com/taiwan-military-expert-porcupine-strategy-could-deter-chinese-invasion/> (дата звернення: 10.05.2025).
7. Lee Hsi-min, Lee E. (3 November 2020). “Taiwan’s Overall Defense Concept, Explained” The Diplomat. Retrieved 18 August 2024. URL: <https://project2049.net/2020/11/03/taiwans-overall-defense-concept-explained/> (дата звернення: 10.05.2025).
8. Бондар К. Арсенал демократії: інтеграція України в оборонно-промислову базу Заходу. Фонд Карнегі за Міжнародний Мир, 4 грудня 2023 р. URL: <https://carnegieendowment.org/2023/12/04/arsenal-of-democracy-integrating-ukraine-into-west-s-defense-industrial-base-pub-91150>. (дата звернення: 10.05.2025).
9. Оборонна підтримка ЄС: фон дер Ляен розповіла про «стратегію дикобраза» для України. URL: <https://www.radiosvoboda.org/a/news-von-der-leyen-stratehiia-dykobraza-dlia-ukrainy/33407140.html> (дата звернення: 10.05.2025).
10. Вилк А., Зоховски П. Міжнародний форум оборонної промисловості в Києві. OSW. 3 жовтня 2023 р. URL: <https://www.osw.waw.pl/en/publikacje/analysis/2023-10-03/international-defence-industries-forum-kyiv-day-586-war>. (дата звернення: 10.05.2025).
11. Західні оборонні компанії обережно відносяться до пропозиції України про виробництво зброї. *Reuters*. 22 червня 2023 р. URL: <https://www.reuters.com/business/aerospace-defense/western-defence-firms-wary-ukraines-weapons-production-pitch-2023-06-22/> (дата звернення: 10.05.2025).
12. Remžová D., Urhová D. The Porcupine Strategy: Taiwan’s Road to Self-Defense. URL: <https://chinaobservers.eu/the-porcupine-strategy-taiwans-road-to-self-defense/> (дата звернення: 20.05.2025).
13. Sharma S. Taiwan’s Porcupine Strategy. URL: <https://www.impriindia.com/insights/taiwan-porcupine-strategy/> (дата звернення: 20.05.2025).
14. Rickards J. Taiwan may yet become a porcupine. URL: <https://www.aspistrategist.org.au/taiwan-may-yet-become-a-porcupine/> (дата звернення: 20.05.2025).
15. EU Commission’s ‘Readiness 2030’ Plan Envisions Ukraine as a ‘Steel Porcupine’ Integrated Into Europe’s Defense Industry. URL: https://en.defence-ua.com/analysis/eu_commissions_readiness_2030_plan_envisions_ukraine_as_a_steel_porcupine_integrated_into_europes_defense_industry-13885.html (дата звернення: 20.05.2025).

References

1. Cancian M., Cancian M., Heginbotham E. (2023). The First Battle of the Next War. Washington, DC: *Center for Strategic & International Studies*. URL: <https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan>.
2. Murray W.S. Revisiting Taiwan’s Defense Strategy (2008). *Naval War College Review*: Vol. 61: No. 3, Article 3. URL: <https://digital-commons.usnwc.edu/nwc-review/vol61/iss3/3>.
3. Fann K., Bursi Ch. (2023). Protecting the Porcupine: Why Taiwan Matters. *Epicenter. Harvard University*. URL: <https://epicenter.wcfia.harvard.edu/blog/protecting-porcupine-why-taiwan-matters>.
4. Cooper B. What is “porcupine strategy”? How can Taiwan’s crazy porcupine defence strategy deter China? (2022). *Quora*. URL: <https://www.quora.com/What-is-porcupine-strategy-How-can-Taiwans-crazy-porcupine-defence-strategy-deter-China>.
5. Franz-Stefan Gady (2023). Turn Ukraine Into a Bristling Porcupine. *Foreignpolicy*. URL: <https://foreignpolicy.com/2023/05/22/ukraine-russia-war-weapons-nato-f16-tanks-deterrence-peace-strategy/>.
6. Yoshiaki Nishimi (2023). Taiwan Military Expert: “Porcupine Strategy” Could Deter Chinese Invasion. *Japan-forward*. URL: <https://japan-forward.com/taiwan-military-expert-porcupine-strategy-could-deter-chinese-invasion/>.
7. Lee Hsi-min, Lee E. (2020). Taiwan’s Overall Defense Concept, Explained. *Project 2049 Institute*. URL: <https://project2049.net/2020/11/03/taiwans-overall-defense-concept-explained/>.
8. Bondar K. (2020). Arsenal demokratiyi: intehtatsiya Ukrayiny v oboronno-promyslovu bazu Zakhodu [Arsenal of Democracy: Ukraine’s Integration into the Western Defense Industrial Base]. *Fond Karnehy za Mizhnarodnyy Myr*, 4 hrudnya 2023. URL: <https://carnegieendowment.org/2023/12/04/arsenal-of-democracy-integrating-ukraine-into-west-s-defense-industrial-base-pub-91150>. (дата звернення: 10.05.2025).
9. Oboronna pidtrymka YES: fon der Lyayen rozpovila pro “stratehiyu dykobrazu” dlya Ukrayiny [EU defense support: von der Leyen spoke about the “porcupine strategy” for Ukraine]. *Radio Svoboda* 05 travnya 2025. URL: <https://www.radiosvoboda.org/a/news-von-der-leyen-stratehiia-dykobraza-dlia-ukrainy/33407140.html>.
10. Vylk A., Zokhovsky P. (2023). Mizhnarodnyy forum oboronnoyi promyslovosti v Kyievi [International Defense Industry Forum in Kyiv]. *OSW*. 3 zhovtnya 2023. URL: <https://www.osw.waw.pl/en/publikacje/analysis/2023-10-03/international-defence-industries-forum-kyiv-day-586-war>.

11. Zakhidni oboronni kompaniyi oberezhno vidnosyat sya do propozytsiyi Ukrayiny pro vyrobnytstvo zbroyi [Western defense companies cautious about Ukraine's offer to produce weapons]. *Reuters*. 22 chervnya 2023. URL: <https://www.reuters.com/business/aerospace-defense/western-defence-firms-wary-ukraines-weapons-production-pitch-2023-06-22/>.
12. Remzova Dominika, Urhova Dominika (2024). The Porcupine Strategy: Taiwan's Road to Self-Defense. *China observers*. URL: <https://chinaobservers.eu/the-porcupine-strategy-taiwans-road-to-self-defense/>.
13. Samriddhi Sharma (2022). Taiwan's Porcupine Strategy. *Impact And Policy Research Institute*. URL: <https://www.impriindia.com/insights/taiwan-porcupine-strategy/>.
14. Jane Rickards. (2024). Taiwan may yet become a porcupine. *ASPI*. URL: <https://www.aspistrategist.org.au/taiwan-may-yet-become-a-porcupine/>.
15. EU Commission's "Readiness 2030" Plan Envisions Ukraine as a "Steel Porcupine" Integrated Into Europe's Defense Industry. *Defense Express*. URL: https://en.defence-ua.com/analysis/eu_commissions_readiness_2030_plan_envisions_ukraine_as_a_steel_porcupine_integrated_into_europes_defense_industry-13885.html.

Стаття надійшла до редакції 27.05.2025

УДК 346.546.6

ДОСЛІДЖЕННЯ, РОЗРОБКИ, ПРОЕКТИ З ПИТАНЬ
ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

Горбачук Назарій Вікторович

*аспірант спеціальності «Публічне управління та адміністрування»
Національного університету «Львівська політехніка»*

Horbachuk Nazarii

*Postgraduate Student in the specialty “Public management and administration”
Lviv Polytechnic National University*

ORCID: 0000-0003-4072-8592

DOI: 10.25313/2617-572X-2025-5-10990

ПОЛЬСЬКИЙ ДОСВІД РЕГУЛЯЦІЇ РКР ЯК МОДЕЛЬ ДЛЯ ВДОСКОНАЛЕННЯ ПОЛІТИКИ ДЕРЖАВНОГО НАГЛЯДУ

POLISH EXPERIENCE OF PKP REGULATION AS A MODEL FOR IMPROVING STATE SUPERVISION POLICY

Анотація. Вступ. В умовах реформування інфраструктурних галузей України особливої уваги потребує проблема регуляції природних монополій, зокрема в секторі залізничних перевезень. Наразі залізнична галузь функціонує за централізованою моделлю управління, де АТ «Укрзалізниця» поєднує функції власника інфраструктури, оператора перевезень, сервісного обслуговування та адміністратора тарифної політики. Такий підхід формує конфлікт інтересів, знижує прозорість діяльності, ускладнює доступ до ринку нових учасників і стримує розвиток конкуренції.

Мета. Проаналізувати досвід реформування та державного регулювання залізничного сектору в Польщі на прикладі РКР, виявити ключові елементи ефективної моделі нагляду за природними монополіями, а також розробити пропозиції щодо застосування польських підходів для вдосконалення політики державного нагляду в Україні.

Методи. У дослідженні використано порівняльно-аналітичний метод для вивчення підходів до реформування залізничного транспорту в Польщі та Україні. Основними джерелами інформації стали нормативно-правові акти, офіційні звіти РКР Group, аналітичні документи Urząd Transportu Kolejowego (UTK), публікації науковців з економіки транспорту та державного управління. Застосовано також системний підхід до аналізу структури державного нагляду над природними монополіями, що дозволило виявити ключові інституційні особливості та визначити можливості імплементації польської моделі в український контекст.

Результати. У результаті дослідження розроблено конкретні наукові пропозиції для вдосконалення державного нагляду над природними монополіями в Україні.

Запропоновано створення незалежного регулятора залізничного транспорту, аналогічного польському UTK, з чітко визначеними повноваженнями щодо контролю за доступом до інфраструктури, тарифною політикою та забезпеченням конкуренції.

Запропоновано модель розмежування функцій між оператором перевезень та власником інфраструктури, що сприятиме прозорості та ефективності управління.

Розроблено рекомендації щодо впровадження принципів Lean Management у діяльність залізничних підприємств для підвищення операційної ефективності.

Окреслено шляхи лібералізації ринку залізничних перевезень з урахуванням європейських стандартів та досвіду Польщі.

Висновки. Врахування польського досвіду реформування РКР відкриває для України перспективи вдосконалення системи державного нагляду над природними монополіями у сфері залізничного транспорту. Запропоновані заходи сприятимуть створенню конкурентного та прозорого ринку залізничних перевезень, підвищенню якості послуг та ефективності управління галуззю.

Ключові слова: державне регулювання, РКР, природна монополія, залізничні перевезення, Польща, Україна, реформування, незалежний регулятор, Lean Management, конкуренція, інфраструктура.

Summary. Introduction. In the context of the reform of infrastructure sectors in Ukraine, the problem of regulating natural monopolies, in particular in the railway sector, requires special attention. Currently, the railway industry operates under a centralized management model, where JSC "Ukrzaliznytsia" combines the functions of the infrastructure owner, transport operator, service provider and tariff policy administrator. This approach creates a conflict of interest, reduces transparency of activities, complicates access to the market for new participants and inhibits the development of competition.

Purpose. To analyze the experience of reforming and state regulation of the railway sector in Poland using the example of PKP, to identify key elements of an effective model of supervision of natural monopolies, and to develop proposals for the application of Polish approaches to improve state supervision policy in Ukraine.

Methods. The study uses a comparative-analytical method to study approaches to reforming railway transport in Poland and Ukraine. The main sources of information were regulatory and legal acts, official reports of PKP Group, analytical documents of Urząd Transportu Kolejowego (UTK), publications of scientists in the field of transport economics and public administration. A systematic approach was also applied to the analysis of the structure of state supervision over natural monopolies, which allowed to identify key institutional features and determine the possibilities of implementing the Polish model in the Ukrainian context.

Results. As a result of the study, specific scientific proposals were developed to improve state supervision over natural monopolies in Ukraine.

The creation of an independent railway transport regulator, similar to the Polish UTK, with clearly defined powers to control access to infrastructure, tariff policy and ensure competition was proposed.

A model of separation of functions between the transport operator and the infrastructure owner was proposed, which will contribute to transparency and management efficiency.

Recommendations were developed for the implementation of Lean Management principles in the activities of railway enterprises to increase operational efficiency.

Ways of liberalizing the railway transportation market are outlined, taking into account European standards and the experience of Poland.

Conclusions. Taking into account the Polish experience of reforming PKP opens up prospects for Ukraine to improve the system of state supervision over natural monopolies in the railway transport sector. The proposed measures will contribute to the creation of a competitive and transparent railway transportation market, improving the quality of services and the efficiency of industry management.

Key words: state regulation, PKP, natural monopoly, railway transportation, Poland, Ukraine, reform, independent regulator, Lean Management, competition, infrastructure.

Постановка проблеми. У процесі реформування інфраструктурних галузей України особливої уваги потребує проблема регуляції природних монополій, зокрема в секторі залізничних перевезень. Наразі залізнична галузь функціонує за централізованою моделлю управління, де АТ «Укрзалізниця» поєднує функції власника інфраструктури, оператора перевезень, сервісного обслуговування та адміністратора тарифної політики. Такий підхід формує конфлікт інтересів, знижує прозорість діяльності, ускладнює доступ до ринку нових учасників і стримує розвиток конкуренції.

Польща, зі свого боку, успішно реалізувала реформу залізничного транспорту, яка може служити моделлю для України. З початку 2000-х років Польські державні залізниці (РКР) пройшли через етапи структурного реформування, функціонального розмежування, створення незалежного регулятора (Urząd Transportu Kolejowego, UTK) та лібералізації ринку. Зокрема, було створено РКР Polskie Linie Kolejowe S.A. як незалежного оператора інфраструктури, що сприяло відкриттю ринку для нових перевізників та підвищенню ефективності управління.

Цей досвід є надзвичайно цінним для України, зважаючи на схожість стартових умов, європейський вектор інтеграції та необхідність підвищення ефективності державного нагляду за діяльністю природ-

них монополій. Вивчення польської моделі дозволяє Україні не лише уникнути типових помилок при реформуванні залізничної галузі, але й скористатися апробованими інструментами — такими як створення спеціалізованих суб'єктів, розвиток конкурентних умов, прозоре ціноутворення, впровадження інновацій та технологій Lean Management. У поєднанні з політикою відкритості ринку це може забезпечити стабільний розвиток залізничного сектору України та його адаптацію до європейських стандартів.

Таким чином, актуальність дослідження польського досвіду регуляції РКР полягає в можливості адаптації ефективних механізмів державного нагляду та управління природними монополіями до українських реалій з метою підвищення прозорості, ефективності та конкурентоспроможності залізничного транспорту.

Аналіз останніх досліджень і публікацій. У контексті реформування залізничного транспорту Польщі та можливості адаптації цього досвіду в Україні, було проведено низку досліджень, які висвітлюють ключові аспекти трансформації РКР та державного нагляду за природними монополіями.

Дослідження автора Marta Postuła. «Change in Management System in the Public Sector Illustrated with the Example of the Railway Infrastructure in Poland» аналізує реформу РКР, яка включала

комерціалізацію, реструктуризацію та впровадження контрактів на публічні послуги (PSC) [1]. У звіті «The Integrity Pact: A Civil Society Monitoring of Public Projects» розглядається впровадження «Пакту доброчесності» у проектах PKP PLK, що сприяло підвищенню прозорості та ефективності тендерних процедур. Зокрема, описано участь громадських організацій у моніторингу закупівель та впровадження етичних стандартів [2]. Стаття «Polish Railways — Towards Privatization» — EJRCF описує правову базу діяльності PKP, включаючи вимоги до розділення обліку інфраструктури та транспортних операцій [3]. Одним із фундаментальних досліджень є монографія В. Базилевича «Природні монополії», де проаналізовано причини виникнення та особливості функціонування природних монополій в економічному просторі, зокрема в Україні [4]. Автор розкриває специфіку їх діяльності в період трансформації економічного устрою та охарактеризовує основні завдання, методи та інструменти державного впливу на природні монополії. Також можна виділити PKP Polskie Linie Kolejowe S.A. «Network Statement 2024/2025» що містить правила розподілу маршрутів поїздів та внутрішні регламенти, що регулюють діяльність залізничних операторів на інфраструктурі PKP [5]. Case Study: Polish Railways. Дослідження, що аналізує реформу польських залізниць, включаючи розділення обліку для вантажних, пасажирських та інфраструктурних послуг з метою забезпечення прозорості [6]. «Ukrainian Regional Policy: The Path to European Integration». У дослідженні розглядається державна стратегія регіонального розвитку України на 2021–2027 роки, її цілі, пріоритети та механізми реалізації [7]. «Different Choices, Divergent Paths: Poland and Ukraine». Порівняльне дослідження трансформаційних процесів у Польщі та Україні, зокрема в контексті реформування державних підприємств та інфраструктури [8]. У дослідженні, опублікованому на порталі «Українська правда», розглядається досвід реформування PKP у 2012–2015 роках [9].

Також варто відзначити дослідження, проведене Українським державним університетом залізничного транспорту, де аналізується досвід компанії PKP SA у розвитку залізничних компаній та їх структурному управлінні [10 с. 49]. Крім того, у статті, опублікованій на порталі «RailInsider», розглядається процес відкриття доступу до інфраструктури залізниць в Польщі [11].

Загалом, аналіз останніх досліджень свідчить про те, що польський досвід реформування залізничного транспорту та регуляції природних монополій може бути корисним для України. Адаптація ефективних механізмів державного нагляду та управління природними монополіями до українських реалій сприятиме підвищенню прозорості, ефективності та конкурентоспроможності залізничного транспорту.

Метою статті є дослідження польської моделі регулювання залізничної галузі на прикладі тран-

сформації PKP (Polskie Koleje Państwowe) та оцінка можливостей її адаптації до українських реалій з метою вдосконалення політики державного нагляду за природними монополіями у сфері залізничного транспорту.

Матеріали і методи. У даній статті застосовано порівняльно-аналітичний метод для вивчення процесів реформування та регулювання залізничного транспорту в Польщі та Україні. Основними джерелами інформації стали нормативно-правові акти, офіційні звіти PKP Group, аналітичні документи Urząd Transportu Kolejowego (UTK), а також публікації науковців з економіки транспорту та державного управління.

Виклад основного матеріалу. Проблема ефективного державного регулювання природних монополій у сфері залізничних перевезень залишається однією з ключових у структурній трансформації української економіки. Залізниця в Україні, представлена компанією АТ «Укрзалізниця», виконує як функції власника інфраструктури, так і оператора перевезень, що суперечить сучасним європейським підходам до управління транспортними монополіями. Така ситуація призводить до конфлікту інтересів, неефективного використання ресурсів, обмеження конкуренції та недостатньої прозорості у прийнятті рішень.

На цьому тлі досвід Польщі щодо реформування своєї залізничної системи, зокрема реструктуризації PKP (Polskie Koleje Państwowe), є надзвичайно цінним. Польська модель демонструє можливість успішного функціонального поділу діяльності, створення незалежного регулятора та впровадження конкурентних механізмів без втрати контролю над стратегічною інфраструктурою.

Враховуючи плани України щодо інтеграції до європейського транспортного простору та зобов'язання, які випливають з Угоди про асоціацію з ЄС, актуальність адаптації польського досвіду до українських реалій є беззаперечною. Вивчення цієї моделі може надати дієві інструменти для підвищення ефективності управління, залучення інвестицій, а також розвитку конкурентного ринку перевезень у межах державного нагляду.

Вибір Польщі як прикладної моделі для вдосконалення державного регулювання природних монополій у сфері залізничних перевезень в Україні зумовлений рядом факторів. Насамперед, Польща є країною з подібним постсоціалістичним минулим, що дозволяє порівнювати стартові умови реформування залізничної галузі. Обидві країни мали централізовану систему управління транспортом, відсутність ринкових механізмів та високу зношеність інфраструктури на момент початку реформ.

Польська реформа PKP, що стартувала у 2000 році, є однією з найпоспідовніших у Центрально-Східній Європі. Вона передбачала функціональний поділ на інфраструктурні, вантажні та пасажир-

ські підрозділи, створення незалежного регулятора (УТК), поступову лібералізацію ринку та відкриття його для приватних учасників. Це забезпечило зростання конкуренції, підвищення якості послуг, ефективніше використання державних коштів та прозорість тарифоутворення.

Важливо й те, що Польща, як держава-член Європейського Союзу, впроваджувала реформи відповідно до директив ЄС щодо залізничного транспорту. Це робить її досвід особливо цінним для України, яка прагне адаптувати своє законодавство та управлінські практики до європейських стандартів. Крім того, активна участь Польщі в міжнародних логістичних проєктах та транспортних коридорах робить її транспортну модель актуальною в контексті регіональної інтеграції.

Таким чином, польська модель реформ РКР є прикладом поступової, збалансованої та інституційно зваженої трансформації природної монополії, що може бути адаптована в Україні з урахуванням національної специфіки.

Для глибшого розуміння можливостей такої адаптації важливо розглянути теоретичні основи державного регулювання природних монополій, які лежать в основі подібних реформ.

Слово «монополія» походить від грецьких слів «monos» — один і «poleo» — продаю. В економічній науці цей термін використовується для опису ситуації, коли окрема фірма або підприємство є єдиним виробником унікального продукту, що дозволяє їй контролювати значну частину або навіть всю галузь.

З огляду на власні економічні інтереси, продавці (а також і покупці) природно прагнуть уникнути конкуренції, захопити монополійні позиції та закріпитися на них. Кожен з них намагається стати монополістом, оскільки це дає йому певну владу над ринком або перевагу у визначенні прийнятної для

нього ціни. Прагнення до захоплення економічної влади з об'єктивних причин глибоко вкоренилося. Воно було і є повсюди й у всі часи [12, с. 37].

Дослідження й узагальнення різних умов, які визначають функціонування природних монополій, дозволили автору у систематизованому вигляді представити основні причини наявності таких структур (табл. 1).

Дані особливості обумовлюють необхідність державного регулювання діяльності природних монополій у транспортній галузі з метою забезпечення ефективності, доступності та якості послуг для споживачів. У цьому контексті важливо враховувати європейський досвід, де роль державного нагляду не лише зводиться до контролю, а й виступає інструментом стимулювання реформ, підвищення прозорості та ефективності діяльності підприємств.

Функції державного нагляду в європейському контексті набувають особливої ваги при реформуванні стратегічно важливих інфраструктурних секторів, таких як залізничний транспорт. Прикладом служить польська модель трансформації залізничної монополії, яка стала можливою завдяки чітко визначеним законодавчим механізмам.

Ключовим етапом реформ стало ухвалення Закону від 8 вересня 2000 року «Про комерціалізацію та реструктуризацію державного підприємства 'Polskie Koleje Państwowe'». Згідно з цим законом, РКР було перетворено на акціонерне товариство РКР S.A., де єдиним акціонером став Державний скарб Польщі. Це дозволило створити гнучку корпоративну структуру, здатну до адаптації в умовах ринкової економіки. Реструктуризація передбачала функціональний поділ діяльності РКР на окремі компанії, що спеціалізуються на різних аспектах залізничного транспорту.

РКР Group (пол. Grupa PKP) — польський конгломерат, заснований у 2001 році від колишнього

Таблиця 1

Причини існування природних монополій в економіці

Причина	Суть явища	Приклад
Економія на масштабі (ефект масштабу)	Зі збільшенням обсягів виробництва знижується собівартість одиниці продукції. Це робить великого виробника ефективнішим за декількох дрібних.	Електроенергетика, водопостачання
Високі бар'єри для входу на ринок	Необхідність великих капіталовкладень у створення інфраструктури стримує появу конкурентів.	Залізничний транспорт, газопостачання
Переважають постійних витрат над змінними	Постійні витрати (наприклад, на обслуговування мережі) становлять значну частину загальних витрат, що вигідно для одного великого виробника.	Телекомунікації, залізниця
Низька еластичність попиту	Споживачі не можуть легко відмовитись від послуг або замінити їх альтернативою.	Послуги ЖКГ, енергетика
Технічна недоцільність дублювання мереж	Будівництво кількох паралельних інфраструктур є надмірно дорогим або фізично складним.	Мережа газопроводів, електромереж
Контроль над критичною інфраструктурою	Один суб'єкт володіє або керує інфраструктурою, до якої мають бути допущені інші учасники ринку, але це можливо лише за регуляторного втручання.	Диспетчерські центри енергосистем

Джерело: розроблено автором

єдиного національного залізничного оператора Польські Державні Залізниці. Такий поділ дозволив чітко розмежувати функції управління інфраструктурою та надання транспортних послуг, що сприяло підвищенню ефективності та прозорості в галузі. Водночас ефективність реформи значною мірою залежала від створення незалежного органу, здатного забезпечити дотримання принципів конкуренції, рівного доступу до інфраструктури та контролю за якістю послуг.

Роль УТК (Urząd Transportu Kolejowego) як незалежного регулятора стала ключовою в реалізації цих завдань. УТК — центральний орган державної адміністрації Польщі, створений 1 червня 2003 року шляхом трансформації Головної інспекції залізничного транспорту. Його діяльність регулюється Законом про залізничний транспорт та європейськими директивами, зокрема Директивою 2012/34/ЄС, яка вимагає незалежності національних регуляторів залізничного ринку від інших органів влади.

Хоча УТК є частиною державної адміністрації, його президент призначається Прем'єр-міністром Польщі, що забезпечує певну автономію від Міністерства інфраструктури. Однак, згідно з дослідженнями, існують виклики щодо повної незалежності УТК, зокрема вплив політичних та бізнес-інтересів на призначення керівництва та прийняття рішень [13].

Попри це, Польща продовжила інтеграцію до європейського правового поля: з метою реалізації положень Директив 2012/34/ЄС, 2016/797/ЄС та 2016/798/ЄС було ухвалено низку законодавчих змін, зокрема до Закону від 28 березня 2003 року про залізничний транспорт [14].

Одним із ключових результатів реформ стало впровадження сучасних рішень у сфері управління персоналом. PKP Polskie Linie Kolejowe S.A. (PKP PLK) активно впроваджують новітні HR-інструменти для ефективного управління людськими ресурсами, що сприяє оптимізації процесів та підвищенню продуктивності праці [15, с. 56].

Зростання прозорості управління. У рамках реформ РКР було проведено інвентаризацію нерухомості, необхідної для функціонування залізничного транспорту, що дозволило впорядкувати управління майном та забезпечити прозорість у використанні активів [16].

Крім того, впровадження системи електронного обміну даними та автоматизація процесів сприяли підвищенню прозорості та контролю за діяльністю компанії.

У свою чергу, це дозволило знизити витрати та збільшити пропускну здатність залізничних ліній.

Також варто звернути увагу на звіти OECD, РКР, УТК, що містять аналіз даних з річних звітів та кейс-стаді. Вони дають чітке уявлення про результати трансформацій, втілених у польському залізничному секторі.

Комерціалізація РКР та функціональне розмежування діяльності між дочірніми компаніями спри-

яли зміцненню фінансової стійкості та поліпшенню корпоративного управління без потреби істотних додаткових бюджетних впливів [17, с. 73].

Згідно з «Raport finansowy Grupy PKP 2023», виручка холдингу зросла на 12,2% порівняно з 2022 роком, а відношення операційних витрат до доходів знизилася на 12,2%, що підтверджує підвищення операційної ефективності після реструктуризації [18, с. 9].

У дослідженні PPIAF із реструктуризації РКР вказано, доходи відновилися після фінансової кризи 2009 року та вантажного бізнесу знаходиться на стабільній фінансовій основі. Продажі активів значно зменшили борг. Конкуренція на ринку вантажних і пасажирських залізничних перевезень зросла: у 2014 році приватні оператори перевезли 43 відсотки вантажів і 54 відсотки пасажирів. Швидкість руху була збільшена на основних ділянках мережі, якщо це дозволило вищий рівень використання обладнання для вантажних перевезень і вищий рівень обслуговування пасажирів. Ринок залізничних послуг — вантажних і пасажирських, державних чи приватних — продовжує знижуватися. У міру того як сектор приватних залізничних вантажних перевезень зростає, частка РКР на ринку, який сам по собі скорочується, стає все меншою. Таким чином, постійні виклики для РКР, особливо для вантажних перевезень, полягатимуть у ефективній конкуренції як з іншими залізничними операторами, так і з дорожнім сектором. Це передбачає збереження РКР персонал, рухомий склад РКР і фіксовані залізничні активи, які спільно використовуються РКР і приватними операторами відповідно до обсягу бізнесу РКР і залізничного сектору в цілому [19, с. 506].

На фоні польського досвіду, де конкуренція та інновації стимулюють розвиток залізничного сектору, Україна стикається з серйозними організаційними труднощами. Залізничний транспорт в Україні все ще функціонує в межах централізованої структури, де одне підприємство — Укрзалізниця — займається як наданням послуг перевезення, так і управлінням інфраструктурою. Така організаційна модель ускладнює ефективне виконання кожної з функцій, створюючи потенційні конфлікти інтересів, оскільки одне підприємство несе відповідальність за кілька різних і взаємопов'язаних процесів. Зокрема, відсутність чіткого розмежування між операційною та регуляторною діяльністю сприяє погіршенню якості обслуговування та створює умови для маніпуляцій з тарифами [20].

Враховуючи ефективність польської моделі реструктуризації РКР, Україна може адаптувати її основні принципи до власних умов. Насамперед ідеться про відокремлення функцій оператора інфраструктури та перевізника. Застосування європейської моделі передбачає створення окремої державної структури, відповідальної за управління залізничною інфраструктурою, тоді як функції пере-

везення повинні виконувати незалежні оператори — як державні, так і приватні. Такий підхід сприятиме демонополізації ринку, підвищенню прозорості та залученню інвестицій, а також дасть змогу впровадити конкурентні механізми надання транспортних послуг. Таке рішення забезпечує рівний доступ до колії, зменшує конфлікт інтересів і стимулює конкуренцію на ринку перевезень. Забезпечення роздільного обліку витрат і доходів. Відповідно до Директиви ЄС 91/440 про поділ функцій інфраструктури та перевезень, необхідно впровадити чіткий роздільний облік фінансових потоків двох суб'єктів: інфраструктурного оператора та залізничного перевізника. Це дозволить прозоро формувати тарифи за доступ до колії та контролювати ефективність кожної ланки ланцюга надання послуг [21, с. 7].

Укладення контракт-програми між державою та оператором інфраструктури. Для чіткого визначення обсягу державного фінансування інфраструктури та умов доступу перевізників до неї необхідно впровадити механізм контрактпрограми (service contract) із Міністерством інфраструктури та Міністерством фінансів. За наявності чітких KPI та фіксованої суми держдотацій це сприятиме ефективному управлінню інвестиціями та гарантуватиме планове оновлення залізничної мережі [21, с. 7].

Створення конкурентного середовища для перевізників. Після виділення інфраструктурного оператора слід забезпечити вільний вхід приватних перевізників через прозорі та недискримінаційні умови ліцензування й тарифоутворення. Це стимулює зниження цін та підвищення якості послуг, а також залучить інвестиції в рухомий склад і сервіс.

Посилення ролі незалежного регулятора, який би здійснював моніторинг доступу до інфраструктури, контролював ліцензування, перевіряв дотримання норм безпеки та захищав права пасажирів. Такий регулятор має мати чітко закріплені в законі повноваження та автономний бюджет.

З огляду на це, постає необхідність формування нової моделі державного управління залізничною галуззю, яка відповідала б сучасним європейським стандартам та забезпечувала ефективне розмежування функцій регулювання, управління інфраструктурою та надання послуг. У межах цієї моделі функції з державного управління залізничним транспортом пропонується покласти на: Міністерство інфраструктури України, яке формуватиме державну політику та забезпечуватиме розроблення законодавчих та нормативних актів, частково управлятиме корпоративними правами публічного акціонерного товариства «Українська залізниця», здійснюватиме координацію замовлень соціальних перевезень пасажирів та ін.;

Державне агентство залізничного транспорту, яке реалізуватиме державну політику, регулюватиме ринок послуг та контролюватиме рівноправний доступ до інфраструктури, вестиме реєстр операторів інфраструктури, перевізників та операторів рухо-

мого складу, а також здійснюватиме ліцензування залізничних підприємств;

Національну комісію регулювання транспорту, яка як незалежний регулятор виконуватиме функції з державного регулювання цін на монопольні послуги залізничного транспорту, погоджуватиме інвестиційні програми;

Державний орган з безпеки на транспорті, який забезпечить державний нагляд за безпекою руху (видача сертифікатів, ліцензування машиністів, авторизація операторів інфраструктури тощо).

Для розслідування інцидентів на залізничному транспорті, відповідно до Директиви ЄС 2004/49/ЄС, передбачено утворити Комісію з розслідування аварій [22, с. 6–7].

Разом із забезпеченням інституційної незалежності регулятора та створенням механізмів контролю й прозорості, важливим напрямом реформування є фінансова стабільність та захищеність діяльності регулюючого органу. У цьому контексті пропонуємо законодавчо закріпити механізм формування та захисту бюджету регулятора, зокрема заборонити одностороннє зменшення чи замороження його фінансування без погодження з керівництвом агентства.

Призначення президента та членів колегії агентства здійснювати на конкурсній основі за участю профільного парламентського комітету з фіксованим терміном повноважень (не менше 5 років) та обмеженнями на дострокове звільнення лише за чітко визначеними у законі підставами (банкрутство, кримінальна відповідальність тощо).

Регулятор повинен відповідати Директиві 2012/34/ЄС щодо незалежності національних регуляторів: відокремлення його від виконавчої влади, заборона на одночасне виконання регуляторних та операційних функцій, прозорість процедур прийняття рішень.

Передбачити щорічне публічне звітування перед Верховною Радою України та доступ до звітних документів через офіційний вебпортал. Запровадити консультативні ради за участю експертів, бізнес-асоціацій і споживачів, які долучатимуться до розробки проектів регуляторних актів.

Це відповідає принципам незалежності фінансування, викладеним у OECD Best Practice Principles for the Governance of Regulators.

«Закон України «Про залізничний транспорт»» необхідно привести у відповідність до Директиви ЄС 2012/34/ЄС про створення єдиного європейського залізничного простору, що передбачає розмежування функцій інфраструктури та перевізників, а також встановлення чітких правил доступу до колії.

Прийняття окремого закону «Про Національне агентство з регулювання залізничного транспорту» з чітко закріпленими повноваженнями із ліцензування, тарифоутворення та нагляду за безпекою, з бюджетною автономією та гарантіями непрямого впливу виконавчої влади.

Реструктуризація за прикладом польського PKP Group із виділенням окремих компаній для управління інфраструктурою, пасажирськими та вантажними перевезеннями, а також технічного обслуговування рухомого складу, із запровадженням роздільного обліку витрат і доходів.

Створення єдиної інформаційної платформи для збору й аналізу даних про тарифи, обсяги перевезень, безпеку та інвестиції, доступної для державних органів і громадськості. Розділ «Моніторинг показників» Річного звіту АТ «Укрзалізниця» може стати базовим каркасом такої системи.

Відокремлення функцій інфраструктури й перевезень та створення незалежного регулятора сприятиме відкриттю ринку для приватних операторів і зростанню конкуренції, що у свою чергу повинно привабити зовнішні та внутрішні інвестиції в рухомий склад і логістику.

Модернізація інфраструктури та стандартизація за європейськими нормами (ERTMS/ETCS) дозволять значно зменшити час простоїв і підвищити середню швидкість руху поїздів. Як показує досвід країн ЄС, інтеграція європейського обладнання та систем управління безпекою підвищує показники пунктуальності. Для України це означатиме кращу привабливість залізниці для пасажирів і бізнесу, а також зменшення навантаження на автомобільні дороги.

Висновки та перспективи подальших досліджень. Оскільки досвід Польщі у реформуванні залізничного транспорту демонструє ефективність моделі, що поєднує функціональне розділення, ство-

рення холдингової структури та незалежне регулювання. Реорганізація PKP Group із виокремленням інфраструктурного оператора (PKP PLK), перевізників (PKP Intercity, PKP Cargo) та інших компаній дозволила зменшити конфлікт інтересів і сприяла розвитку конкуренції в сегментах, де це можливо. Незалежний регулятор Urząd Transportu Kolejowego (UTK) забезпечує ліцензування, контроль доступу до інфраструктури та моніторинг тарифів, що відповідає європейським директивам щодо відкриття ринку та забезпечення конкуренції.

Польська модель також підкреслює важливість прозорості тарифної політики та залучення інвестицій для модернізації інфраструктури. Ці аспекти сприяють підвищенню якості послуг і безпеки перевезень. Водночас, досвід Польщі вказує на необхідність постійного моніторингу та вдосконалення регуляторних практик для запобігання потенційним зловживанням та забезпечення рівних умов для всіх учасників ринку.

В подальших наукових дослідженнях пропонується зосередити увагу на аналізі ефективності незалежного регулювання. Оцінку впливу функціонального розділення. Дослідження тарифної політики. Аналізування механізмів формування тарифів у Польщі та їх вплив на конкуренцію і доступність послуг для споживачів.

Впровадження подібних реформ в Україні, заснованих на польському досвіді, дозволить значно покращити ефективність та стабільність залізничного сектору, підвищити якість послуг і забезпечити сталий розвиток транспортної інфраструктури країни.

Література

1. Postuła M. Change in Management System in the Public Sector Illustrated with the Example of the Railway Infrastructure in Poland. URL: <https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.cejsh-d5c742f3-c4d5-488c-9d10-eb07eb53c545/c/18.pdf> (дата звернення: 02.05.2025).
2. The Integrity Pact: A Civil Society Monitoring of Public Projects. URL: https://www.researchgate.net/publication/368449571_The_Integrity_Pact_A_Civil_Society_Monitoring_of_Public_Projects_Designing_an_Integrity_Pact_and_the_Contractor_Selection (дата звернення: 02.05.2025).
3. Polish Railways — Towards Privatization. EJRCF. https://www.ejrcf.or.jp/jrtr/jrtr21/F20_Lipinski.html (дата звернення: 02.05.2025).
4. Базилевич В. Д., Філюк Г. М. Природні монополії. К. : Знання, 2006. 367 с.
5. PKP Polskie Linie Kolejowe S. A. "Network Statement 2024/2025". URL: https://en.plk-sa.pl/files/public/user_upload/pdf/Reg_przydzielania_tras/Regulamin_sieci_2024_2025/v.23/01.Network_statement_24_25_v23.pdf (дата звернення: 02.05.2025).
6. Case Study: Polish Railways. URL: https://www.ppiaf.org/sites/ppiaf.org/files/documents/toolkits/railways_toolkit/PDFs/RR%20Toolkit%20EN%20New%202017%2012%2027%20CASE11%20POLAND.pdf (дата звернення: 02.05.2025).
7. Ukrainian Regional Policy: The Path to European Integration. URL: <https://bibliotekanauki.pl/articles/2156737.pdf> (дата звернення: 02.05.2025).
8. Different Choices, Divergent Paths: Poland and Ukraine. URL: <https://wiiw.ac.at/different-choices-divergent-paths-poland-and-ukraine-dlp-6419.pdf> (дата звернення: 02.05.2025).
9. Карновські Я. Як реформувати «Укрзалізницю» так, щоб вона служила українцям. URL: <https://epravda.com.ua/columns/2020/08/4/663682/> (дата звернення: 08.04.2025).

10. Ломотко М. Д. Удосконалення технології доставки вантажів залізничним транспортом в умовах конкурентного середовища: дис. на здобуття ступеня доктора філософії. Український державний університет залізничного транспорту, 2024. С. 49.
11. Відкритий доступ до інфраструктури залізниці — досвід Польщі. URL: <https://www.railinsider.com.ua/vidkrytyj-dostup/> (дата звернення: 10.04.2025).
12. Базилевич В., Колчигін О. Конкуренція як економічна категорія та конкурентні відносини. *Вісник КДТЕУ*. 1999. № 1. С. 37.
13. Art. 11. — [Procedura powołania Prezesa UTK] — Transport kolejowy. URL: <https://sip.lex.pl/akty-prawne/dziedzinnik-ustaw/transport-kolejowy-17029070/art-11> (дата звернення: 10.04.2025).
14. 4th Railway Package implementation. URL: <https://www.era.europa.eu/content/4th-railway-package-implementation-one-europe-one-railway-one-process?> (дата звернення: 12.04.2025).
15. Raport roczny 2009. С. 56. URL: https://en.plk-sa.pl/files/public/raport_roczny/Raport_PKP_PLK_2009_pl-en_cd_.pdf (дата звернення: 20.04.2025).
16. PKP uporządkowały sprawę zarządzania kolejowymi nieruchomościami. URL: <https://biznes.wprost.pl/gospodarka/11068144/pkp-uporzadkowaly-sprawę-zarządzania-kolejowymi-nieruchomosciami.html> (дата звернення: 20.04.2025).
17. Railway reform. Regulation of Freight Transport Markets. С. 73 URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2001/01/railway-reform_g1gh1f9d/9789282112731-en.pdf (дата звернення: 20.04.2025).
18. RAPORT ROCZNY 2023. С. 16. URL: <https://www.pkp.pl/images/download/Raport%20roczny%202023.pdf> (дата звернення: 20.04.2025).
19. Railway Reform: Toolkit for Improving Rail Sector Performance. С. 506 URL: https://www.ppiaf.org/sites/ppiaf.org/files/documents/toolkits/railways_toolkit/PDFs/RR%20Toolkit%20EN%20New%202017%2012%2027%20CASE11%20POLAND.pdf (дата звернення: 22.04.2025).
20. Corporate governance crisis continues at Ukraine's state-owned enterprises. URL: <https://www.atlanticcouncil.org/blogs/ukrainealert/corporate-governance-crisis-continues-at-ukraines-state-owned-enterprises/> (дата звернення: 02.05.2025).
21. Лібералізація ринку залізничних перевезень в Україні. Уроки країн Європейського Союзу. С. 7. URL: https://ces.org.ua/wp-content/uploads/2019/11/%D0%9B%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F-%D1%80%D0%B8%D0%BD%D0%BA%D1%83-%D0%B7%D0%B0%D0%BB%D1%96%D0%B7%D0%BD%D0%B8%D1%87%D0%BD%D0%B8%D1%85-%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D0%B5%D0%B7%D0%B5%D0%BD%D1%8C.pdf?utm_ (дата звернення: 02.05.2025).
22. Стратегічний план розвитку залізничного транспорту на період до 2020 року: Наказ Міністерства інфраструктури України від 21 грудня 2015 № 547. С. 6–7.

References

1. Postuła M. Change in Management System in the Public Sector Illustrated with the Example of the Railway Infrastructure in Poland. URL: <https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.cejsh-d5c742f3-c4d5-488c-9d10-eb07eb53c545/c/18.pdf> (access date: 02.05.2025).
2. The Integrity Pact: A Civil Society Monitoring of Public Projects. URL: https://www.researchgate.net/publication/368449571_The_Integrity_Pact_A_Civil_Society_Monitoring_of_Public_Projects_Designing_an_Integrity_Pact_and_the_Contractor_Selection (access date: 02.05.2025).
3. Polish Railways — Towards Privatization. *EJRCF*. https://www.ejrcf.or.jp/jrtr/jrtr21/F20_Lipinski.html (access date: 02.05.2025).
4. Bazylevych V. D., Filiuk G. M. Natural monopolies. K.: Znannya, 2006. 367 p.
5. PKP Polskie Linie Kolejowe S.A. "Network Statement 2024/2025". URL: https://en.plk-sa.pl/files/public/user_upload/pdf/Reg_przydzielania_tras/Regulamin_sieci_2024_2025/v.23/01.Network_statement_24_25_v23.pdf (access date: 02.05.2025).
6. Case Study: Polish Railways. URL: https://www.ppiaf.org/sites/ppiaf.org/files/documents/toolkits/railways_toolkit/PDFs/RR%20Toolkit%20EN%20New%202017%2012%2027%20CASE11%20POLAND.pdf (access date: 02.05.2025).
7. Ukrainian Regional Policy: The Path to European Integration. URL: <https://bibliotekanauki.pl/articles/2156737.pdf> (access date: 02.05.2025).
8. Different Choices, Divergent Paths: Poland and Ukraine. URL: <https://wiiw.ac.at/different-choices-divergent-paths-poland-and-ukraine-dlp-6419.pdf> (access date: 02.05.2025).
9. Karnowski J. How to reform "Ukrzaliznytsia" so that it serves Ukrainians. URL: <https://epravda.com.ua/columns/2020/08/4/663682/> (access date: 02.05.2025).
10. Lomotko M. D. Improving the technology of cargo delivery by rail in a competitive environment. P. 49.
11. Open access to railway infrastructure — the experience of Poland. URL: <https://www.railinsider.com.ua/vidkrytyj-dostup/> (access date: 10.04.2025).
12. Bazylevich V., Kolchygin O. Competition as an economic category and competitive relations. *Bulletin of the KDTEU*. 1999. No. 1. P. 37.

13. Art. 11. — [Procedura powołania Prezesa UTK] — Transport kolejowy. URL: <https://sip.lex.pl/akty-prawne/dzuzdziennik-ustaw/transport-kolejowy-17029070/art-11> (access date: 10.04.2025).
14. 4th Railway Package implementation. URL: <https://www.era.europa.eu/content/4th-railway-package-implementation-one-europe-one-railway-one-process?> (access date: 12.04.2025).
15. Annual Report 2009. P. 56 URL: https://en.plk-sa.pl/files/public/raport_roczny/Raport_PKP_PLK_2009_pl-en_cd_.pdf (access date: 20.04.2025).
16. PKP has sorted out the issue of managing railway real estate. URL: <https://biznes.wprost.pl/gospodarka/11068144/pkp-uporzadkowaly-sprawe-zarzadzania-kolejowymi-nieruchomosciami.html> (access date: 20.04.2025).
17. Railway reform. Regulation of Freight Transport Markets. P. 73 URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2001/01/railway-reform_g1gh1f9d/9789282112731-en.pdf (access date: 20.04.2025).
18. ANNUAL REPORT 2023. URL: <https://www.pkp.pl/images/download/Raport%20roczny%202023.pdf> (access date: 20.04.2025).
19. Railway Reform: Toolkit for Improving Rail Sector Performance. P. 506. URL: https://www.ppiaf.org/sites/ppiaf.org/files/documents/toolkits/railways_toolkit/PDFs/RR%20Toolkit%20EN%20New%202017%2012%2027%20CASE11%20POLAND.pdf (access date: 22.04.2025).
20. Corporate governance crisis continues at Ukraine's state-owned enterprises. URL: <https://www.atlanticcouncil.org/blogs/ukrainealert/corporate-governance-crisis-continues-at-ukraines-state-owned-enterprises/> (access date: 02.05.2025).
21. Liberalization of the railway market in ukraine. Lessons from the european union countries. P. 7 URL: https://ces.org.ua/wp-content/uploads/2019/11/%D0%9B%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F-%D1%80%D0%B8%D0%BD%D0%BA%D1%83-%D0%B7%D0%B0%D0%BB%D1%96%D0%B7%D0%BD%D0%B8%D1%87%D0%BD%D0%B8%D1%85-%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D0%B5%D0%B7%D0%B5%D0%BD%D1%8C.pdf?utm_ (access date: 02.05.2025).
22. Order of the Ministry of Infrastructure of Ukraine dated December 21, 2015 No. 547 Strategic Plan for the Development of Railway Transport for the Period Until 2020. P. 6–7.

Стаття надійшла до редакції 22.05.2025

УДК 614.2

Корсун Андрій Васильович

*аспірант кафедри публічного управління та адміністрування
Вінницької академії безперервної освіти*

Korsun Andrii

*Postgraduate Student of the Department of Public Management and Administration
Vinnytsia Academy of Continuing Education*

ORCID: 0009-0004-2505-4547

Бабій Вадим Юрійович

*кандидат медичних наук,
доцент кафедри публічного управління та адміністрування
Вінницька академія безперервної освіти*

Babii Vadym

*PhD in Medicine,
Associate Professor of the Department of Public Management and Administration
Vinnytsia Academy of Continuing Education*

ORCID: 0000-0001-6597-6045

DOI: 10.25313/2617-572X-2025-5-10955

БЕЗПЕРЕРВНА ОСВІТА МЕДИКІВ В ЕПОХУ ЦИФРОВІЗАЦІЇ: ФОКУС НА УПРАВЛІННІ КЛІНІЧНИМИ РИЗИКАМИ

CONTINUING EDUCATION OF PHYSICIANS IN THE AGE OF DIGITALIZATION: FOCUS ON CLINICAL RISK MANAGEMENT

Анотація. Вступ. Стрімка цифровізація охорони здоров'я в Україні активізує потребу у безперервній медичній освіті, здатній оперативно реагувати на клінічні ризики, зумовлені людським фактором та високим навантаженням персоналу у воєнний час. Перетворення реальних інцидентів на персоналізовані освітні інтервенції розглядається як ефективний шлях до підвищення безпеки пацієнтів.

Мета. Дослідити значення безперервної медичної освіти в умовах цифровізації та розробити інтегровану модель цифрового навчання і контролю клінічних ризиків, адаптовану до практики українських лікарень

Матеріали і методи. Дослідження спиралося на поєднання теоретичних, емпіричних та статистичних методів, зокрема: аналіз, синтез, узагальнення й систематизація наукових публікацій та чинної нормативної бази МОЗ – для формування концептуальних засад моделі; контент-аналіз клінічних інцидентів для виділення типових помилок і побудови первинної «карти ризиків»; метод експертних оцінок для верифікації блок-схеми та матриці «вагомість наслідків / частота помилки»; моделювання – при конструюванні інтегрованої блок-схеми циклу «ризик → аналіз → навчання → вдосконалення».

Результати. Встановлено, що цифрові освітні технології сприяють підвищенню якості безперервної медичної освіти та зниженню ризиків клінічних помилок шляхом розвитку практико орієнтованих навичок. Підкреслено важливість використання симуляційного навчання, гібридних тренінгів, стандартизованих пацієнтів та адаптивних навчальних платформ для формування культури безпеки. На основі аналізу реальних інцидентів виокремлено п'ять критичних етапів, де найчастіше можна запобігти помилкам (ідентифікація ризику, передача даних, симуляційне навчання, аналітика, управлінські рішення). Розроблена блок-схема інтегрує ці етапи у замкнений цикл «ризик → аналіз → навчання → вдосконалення», а матриця «вагомість / частота» дозволяє ранжувати помилки й визначати пріоритетні освітні та організаційні заходи.

Перспективи. Подальші дослідження мають зосередитися на пілотному тестуванні моделі у кількох типах медичних закладів, стандартизації показників ефективності та інтеграції з національною платформою eHealth. Важливими напрямками залишаються економічна оцінка очікуваних вигод, розробка методичних рекомендацій і створення єдиної бази сценаріїв симуляційних тренінгів для поширення найкращих практик між лікарнями.

Ключові слова: безперервна медична освіта, цифровізація охорони здоров'я, управління клінічними ризиками, симуляційне навчання, блок-схема, матриця вагомості / частота, людський фактор, безпека пацієнтів, культура якості.

Summary. Introduction. The rapid digitalization of healthcare in Ukraine intensifies the need for continuing medical education (CME) that can promptly address clinical risks arising from human factors and the heavy workload of personnel during wartime. Converting real-world incidents into personalized educational interventions is viewed as an effective pathway to improving patient safety.

Purpose. To explore the significance of CME under conditions of digitalization and to develop an integrated model of digital learning and clinical risk control adapted to the realities of Ukrainian hospitals.

Materials and methods. The study employed a combination of theoretical, empirical and statistical methods, namely: analysis, synthesis, generalization and systematization of scientific publications and current Ministry of Health regulations to establish the conceptual foundations of the model; content analysis of clinical incident reports to identify typical errors and construct an initial "risk map"; expert evaluation to validate the block diagram and the "severity / frequency" matrix; and modelling to design an integrated block diagram of the "risk → analysis → training → improvement" cycle.

Results. Digital educational technologies enhance the quality of CME and reduce clinical error rates by strengthening practice-oriented skills. The importance of simulation-based learning, hybrid workshops, standardized patients and adaptive learning platforms for fostering a culture of safety is underlined. Analysis of real incidents isolated five critical stages where most errors can be prevented (risk identification, data transfer, simulation training, analytics and managerial decision-making). The proposed block diagram merges these stages into a closed "risk → analysis → training → improvement" loop, while the severity / frequency matrix makes it possible to rank errors and set priorities for educational and organizational actions.

Prospects. Future research should focus on pilot testing the model in various healthcare settings, standardizing performance indicators, and integrating the approach with the national eHealth platform. Key directions also include economic evaluation of anticipated benefits, development of methodological guidelines, and creation of a unified repository of simulation training scenarios to disseminate best practices among hospitals.

Key words: continuing medical education, healthcare digitalization, clinical risk management, simulation training, block diagram, severity / frequency matrix, human factor, patient safety, quality culture.

Постановка проблеми. Сучасна українська медицина одночасно переживає два потужні виклики: наслідки воєнного стану та стрімку цифрову трансформацію системи охорони здоров'я. Зростання навантаження на персонал, кадровий дефіцит і різноманітність локальних протоколів призводять до збільшення кількості клінічних інцидентів, більшість із яких пов'язані з людським фактором [14; 15]. Попри це, у лікарнях уже накопичено значний масив електронних даних — від внутрішніх розслідувань до записів ЕМЗ, — який поки що використовується фрагментарно.

Існуючі цифрові інструменти — симулятори, VR/AR-платформи, мобільні застосунки — довели свою ефективність у формуванні практичних навичок і запобіганні помилкам. Проте відсутність цілісного підходу до їх впровадження, системи оцінки результативності та механізмів швидкої адаптації навчальних програм до нових ризиків обмежує потенціал цих технологій [6; 20].

Найбільшою прогалиною залишається нестача методологічно обґрунтованого зв'язку між аналізом реальних клінічних помилок і персоналізованим навчанням медичного персоналу. Без такого зв'язку цифрові рішення лише частково покривають потреби системи й не забезпечують сталого зниження рівня небезпечних інцидентів.

Отже, проблема полягає у розробці практичного, даних-орієнтованого механізму, який перетворює результати щоденної клінічної практики на ефективні освітні інтервенції. Запропонована в статті

інтегрована модель цифрового навчання й контролю ризиків покликана заповнити цю прогалину, забезпечивши безперервний цикл «ризик → аналіз → навчання → вдосконалення процесу».

Аналіз останніх досліджень і публікацій.

Цифрові технології дедалі більше інтегруються в медицину, змінюючи підходи до надання медичної допомоги та управління клінічними ризиками. Використання телемедицини, носимих пристроїв і мобільних додатків дозволяє покращити доступність медичних послуг, особливо в умовах криз, таких як пандемія COVID-19. Ці технології сприяють ранньому виявленню захворювань, персоналізованому лікуванню та ефективнішому лікуванню хронічних станів [1].

Впровадження цифрових інструментів у медичну освіту сприяє підвищенню кваліфікації фахівців та покращенню управління клінічними ризиками. Використання цифрових технологій для навчання дозволяє медичним працівникам ефективніше засвоювати нові знання та навички, що необхідні для роботи в сучасному цифровому середовищі. Це, в свою чергу, сприяє зниженню ймовірності медичних помилок та покращенню якості надання медичної допомоги [2; 3].

У сучасній клінічній практиці цифрові рішення відіграють ключову роль у підвищенні ефективності та безпеки медичних послуг. Системи підтримки клінічних рішень (CDSS) допомагають лікарям у прийнятті клінічних рішень, надаючи рекомендації на основі аналізу даних пацієнта. Наприклад, система MilleDSS в Італії підтримує лікарів загальної

практики в управлінні клінічними процесами та оцінці ризиків [4]. Електронні медичні записи (ЕМЗ) дозволяють зберігати та обмінюватися детальною інформацією про пацієнтів у цифровому форматі. Вони сприяють покращенню якості медичної допомоги, забезпечуючи швидкий доступ до історії хвороби та результатів обстежень. Наприклад, дані ЕМЗ використовуються для створення сімейних зв'язків, що покращує дослідження в галузі громадського здоров'я [5]. Використання високотехнологічних манекенів, віртуальної реальності та інших симуляційних інструментів дозволяє медичним працівникам відпрацьовувати клінічні навички в безпечному середовищі. Це покращує їхню підготовку та зменшує ризик помилок при роботі з реальними пацієнтами [6]. Впровадження цих цифрових рішень сприяє підвищенню якості медичних послуг та безпеки пацієнтів [7] electronic health records (EHRs). Цифровізація суттєво впливає на якість та безпеку надання медичної допомоги, пропонуючи як значні переваги, так і певні виклики. Впровадження цифрових технологій, таких як електронні медичні записи та системи підтримки клінічних рішень, сприяє зменшенню кількості помилок, покращенню доступу до інформації та підвищенню ефективності лікування. Наприклад, дослідження показують, що інтеграція ЕМЗ може знизити кількість медикаментозних помилок та покращити координацію догляду за пацієнтами [8]. Однак, цифровізація також може призвести до нових типів помилок, пов'язаних з технологіями. Наприклад, недостатня інтероперабельність систем або погано спроектовані інтерфейси можуть спричинити технологічно індуковані помилки, що негативно впливають на безпеку пацієнтів [9]. Хоча цифрові лікарні та інші технологічні рішення мають потенціал покращити досвід пацієнтів та клініцистів, існує потреба в подальших дослідженнях для оцінки їхнього впливу на безпеку та якість медичної допомоги. Деякі дослідження вказують на змішані результати щодо впливу цифрових лікарень на безпеку пацієнтів та здатність клініцистів надавати медичну допомогу [10].

Таким чином, цифровізація має значний потенціал для покращення якості та безпеки медичної допомоги, але її впровадження повинно супроводжуватися ретельним плануванням, навчанням персоналу та постійним моніторингом для мінімізації можливих ризиків.

Мета статті — дослідити значення безперервної медичної освіти в умовах цифровізації та, спираючись на отримані результати, розробити й обґрунтувати інтегровану модель цифрового навчання і контролю клінічних ризиків, адаптовану до українських лікарень. У статті показано, як зібрані дані про реальні помилки перетворюються на персоналізовані симуляційні й навчальні інтервенції, що підвищують якість клінічних рішень і знижують частоту небезпечних інцидентів.

Виклад основного матеріалу. Клінічний ризик-менеджмент — це систематичний підхід до виявлен-

ня, оцінки та зниження ризиків, пов'язаних із наданням медичної допомоги, з метою підвищення безпеки пацієнтів та якості медичних послуг. Він охоплює комплекс клінічних та адміністративних систем, процесів, процедур і структур звітності, спрямованих на виявлення, моніторинг, оцінку, пом'якшення та запобігання ризикам для пацієнтів [11]

Клінічний ризик у цьому контексті визначається як об'єктивна (математична) або суб'єктивна (індуктивна) ймовірність того, що відбудеться негативна подія, пов'язана з наданням медичної допомоги. Це може включати ймовірність існування або виникнення загрози для здоров'я, перетворення цієї загрози на подію, яка призведе до шкоди здоров'ю, та ймовірність того, що ця шкода спричинить медичну катастрофу [12].

Управління клінічними ризиками включає такі ключові етапи:

Ідентифікація ризиків: Виявлення потенційних загроз та небезпек, які можуть негативно вплинути на пацієнтів або персонал.

Оцінка та аналіз ризиків: Визначення ймовірності та серйозності потенційних несприятливих подій для пріоритезації заходів з управління ризиками.

Розробка та впровадження заходів контролю: Розробка стратегій та процедур для зменшення або усунення ідентифікованих ризиків, таких як впровадження стандартних операційних процедур або навчання персоналу.

Моніторинг: Постійний нагляд за ефективністю впроваджених заходів та їх коригування за необхідності для забезпечення безперервного покращення.

Впровадження ефективної системи клінічного ризик-менеджменту сприяє зменшенню кількості несприятливих подій та покращенню безпеки пацієнтів. Наприклад, дослідження показало, що після впровадження комплексної системи управління клінічними ризиками в університетській лікарні спостерігалось середнє щорічне зниження шкоди для пацієнтів на 60,1% [13].

Таким чином, сучасне розуміння клінічного ризик-менеджменту передбачає інтеграцію його в усі аспекти медичної практики з метою створення культури безпеки та безперервного покращення якості медичної допомоги.

Людський фактор відіграє значну роль у виникненні клінічних помилок, які можуть призвести до серйозних наслідків для пацієнтів. До таких факторів належать втому, стрес, недостатня підготовка та когнітивні упередження медичних працівників. Наприклад, дослідження показують, що втому лікарів може збільшити кількість медичних помилок, включаючи ті, що призводять до ушкоджень або смерті пацієнтів [14]. Системні помилки стосуються недоліків в організації та процесах надання медичної допомоги. Вони можуть включати неефективну комунікацію між відділеннями, недостатню стандартизацію процедур та використання застарілих або складних технологій.

Наприклад, відсутність чітких ліній підпорядкування та неефективна комунікація між медичним персоналом можуть сприяти виникненню помилок [15].

Приклад інциденту: у 2013 році в медичному центрі UCSF 16-річному пацієнту Пабло Гарсія було випадково введено дозу антибіотика, що перевищувала необхідну в 39 разів. Це сталося через низку помилок: лікар неправильно ввів дозування в електронну систему, фармацевт не помітив помилки, а медсестра, довіряючи системі, не перевірила дозу перед введенням [16]. Цей випадок підкреслює небезпеку надмірної довіри до технологій та важливість перевірки інформації медичним персоналом [17].

Для зменшення впливу людського фактора та системних помилок необхідно впроваджувати такі заходи, як навчання та підвищення обізнаності, стандартизація процесів, використання чек-листів, застосування контрольних списків, таких як контрольний список безпеки хірургічних втручань BOOZ та поліпшення комунікації між членами медичної команди для забезпечення чіткого розуміння плану лікування та обов'язків кожного учасника [18; 19].

Цифрові технології стали ключовим інструментом у безперервній медичній освіті, дозволяючи медикам отримувати доступ до навчального контенту, сертифікаційних курсів і клінічних оновлень незалежно від місця розташування. Такі сервіси, як BMJ Learning або Coursera, забезпечують масштабованість і зручність у навчанні. Симулятори, включаючи віртуальну та доповнену реальність (VR/AR), надають медичним працівникам можливість практикувати клінічні навички в умовах, наближених до реальних. Таке навчання дозволяє зменшити кількість помилок у клінічній практиці, підвищити рівень впевненості та покращити готовність до надзвичайних ситуацій [6]. Адаптивне навчання базується на персоналізації освітнього процесу: система підлаштовує контент відповідно до індивідуального рівня знань та прогресу користувача [20]. Це дозволяє більш ефективно засвоювати матеріал і підтримувати високу мотивацію у навчанні. Мобільні додатки, як-от Osmosis або Figure 1, дозволяють лікарям швидко переглядати клінічні випадки, відеоінструкції або протоколи лікування безпосередньо зі смартфона. Це робить навчання більш гнучким та доступним у будь-який момент [21]. Мікронавчання — це формат подачі інформації короткими, концентрованими блоками, що дозволяє ефективно повторювати та засвоювати знання в умовах браку часу. Такий підхід показав свою ефективність у медичній підготовці, особливо при частому оновленні знань [22].

Відстеження компетентностей і оцінка результатів реалізуються за допомогою цифрових портфоліо (ePortfolio) або аналітичних платформ, які фіксують прогрес, визначають прогалини у знаннях та дозволяють планувати індивідуальні освітні траєкторії. Це критично важливо для якісного управління професійним розвитком [23].

Виходячи з наведеного вище аналізу цифрових технологій, можна рекомендувати такі конкретні кроки для використання цифрових інструментів у навчанні лікарів з фокусом на ризик-менеджмент:

Використання симуляційного навчання (Simulation-Based Training — SBT) для відпрацювання сценаріїв, пов'язаних з ризик-менеджментом та безпекою пацієнтів. Високоточні пацієнт-симулятори можуть бути застосовані для створення реалістичних клінічних ситуацій, де лікарі повинні приймати рішення з урахуванням потенційних ризиків, використовуючи медичне обладнання та отримуючи миттєвий зворотний зв'язок. Ці симулятори широко використовуються в Північній Америці, Європі та Азії [6].

Віртуальна реальність (VR) створює комп'ютерно-генеровані середовища, в яких лікарі можуть взаємодіяти зі сценаріями, що моделюють ризикові ситуації. VR набуває все більшого поширення, особливо в розвинених регіонах, та забезпечує безпечне середовище для повторного тренування та отримання зворотного зв'язку.

Доповнена реальність (AR) може накладати цифрову інформацію, наприклад, про потенційні ризики або протоколи безпеки, на реальне клінічне середовище, покращуючи ситуаційну обізнаність лікарів. AR все частіше використовується в медичній освіті, підвищуючи реалізм навчання.

Гібридні симуляції, що поєднують різні методи симуляції (наприклад, високоточні манекени з VR або AR), можуть пропонувати комплексний досвід навчання, інтегруючи сильні сторони різних підходів для відпрацювання навичок ризик-менеджменту в різних контекстах.

Стандартизовані пацієнти актори, навчені зображати пацієнтів зі специфічними медичними станами та історіями, можуть використовуватися для відпрацювання комунікації щодо ризиків та прийняття спільних рішень з пацієнтами. Це особливо корисно для навчання емпатії та культурної чутливості в контексті ризик-менеджменту.

Розробка та впровадження адаптивних електронних навчальних середовищ (ЕНС), що персоналізують навчання з питань ризик-менеджменту. ЕНС можуть адаптувати контент, навігацію, мультимедіа та інструменти відповідно до знань та прогресу лікаря в питаннях ризик-менеджменту. Метою є підвищення ефективності навчання (знань, навичок) та ефективності навчання (знання, отримані за одиницю часу). Адаптивність може бути розробленою (коли експерт визначає навчальну траєкторію залежно від відповідей лікаря) або алгоритмічною (коли система автоматично визначає оптимальну послідовність навчання на основі алгоритмів). Приклади адаптивності можуть включати надання додаткової інформації або складніших завдань у галузі ризик-менеджменту тим лікарям, які демонструють глибші знання, або повторення ключових концепцій для тих, хто потребує додаткової підтримки. Такі платформи можуть

використовувати дані для оптимізації ефективності та результативності навчання, хоча наразі ці дані рідко використовуються повною мірою.

Використання цифрових платформ для поширення навчальних матеріалів з ризик-менеджменту. Забезпечення доступу до оновлених протоколів, клінічних настанов та іншої важливої інформації з ризик-менеджменту через онлайн-платформи. Використання QR-кодів на друкованих матеріалах для швидкого доступу до оновлених електронних ресурсів з ризик-менеджменту, що дозволяє оперативно доносити до лікарів та пацієнтів/опікунів оновлену інформацію з безпеки лікарських засобів. Розміщення навчальних матеріалів з ризик-менеджменту на веб-сайтах медичних установ або фармацевтичних компаній, забезпечуючи вільний доступ для цільової аудиторії (лікарів, пацієнтів/опікунів), зберігаючи контроль доступу до інших ресурсів. Надсилання сповіщень лікарям електронною поштою про оновлення навчальних матеріалів з ризик-менеджменту, за умови їхньої згоди на отримання таких повідомлень.

Використання електронних портфоліо (ePortfolios) для документування компетентностей лікарів у сфері ризик-менеджменту, відображення їхнього навчання та збору зворотного зв'язку. Хоча джерела переважно розглядають ePortfolios у контексті клінічних практик студентів, їх можна адаптувати для безперервної медичної освіти лікарів, дозволяючи їм фіксувати свій прогрес у навчанні з ризик-менеджменту, завантажувати виконані завдання (наприклад, результати симуляцій), отримувати оцінку від колег та менторів. Навчання користуванню ePortfolios має бути індивідуальним та постійним, базуючись на відповідній теоретичній основі.

Важливо враховувати, що успішне впровадження цих цифрових інструментів вимагає ретельного планування, обліку потреб лікарів та забезпечення належної підготовки викладачів для їхнього ефективного використання.

На основі вище викладених інструментів пропонуємо модель інтегрованої системи цифрового навчання й контролю клінічних ризиків у лікарні. Сучасна медична система України працює в умовах подвійного виклику — воєнного стану та необхідності швидкої цифрової трансформації. Кількість несприятливих подій, пов'язаних із людським чинником, зростає через понаднормові навантаження, кадровий дефіцит і варіативність локальних протоколів [13]. Водночас лікарні отримують доступ до електронних медичних записів (ЕМЗ), телемедичних сервісів і симуляційних центрів, що відкриває можливість перетворити реальні клінічні інциденти на керовані освітні інтервенції.

Щоб системно використати цей потенціал, ми розробили модель інтегрованої системи цифрового навчання й контролю ризиків, адаптовану до українських реалій. Вона поєднує аналітику клінічних ризиків, персоналізоване навчання та симуляційні технології в єдиний замкнений цикл (рис. 1). Модулі з'єднані циклічним зв'язком: після реалізації

інтервенцій система повертається до етапу 2 для повторної ідентифікації нових або нерозв'язаних ризиків, що забезпечує принцип ПРПД (плануй — роби-перевіряй-дій).

Перший етап — ідентифікація ризиків. У лікарнях щотижневі наради, медичні ради, комісії з якості та внутрішні аудити формують достатній обсяг даних про помилки — від некоректного дозування ліків до порушень маршруту пацієнта.

Другий етап — передача даних в інформаційно-аналітичний та освітній підрозділ лікарні. На цьому кроці створюється єдиний дашборд ризиків у вигляді звичної для конкретної лікарні бази даних, доступної для аналітиків і симуляційного центру, який може бути підрозділом лікарні, або аутсорсинговою організацією. Після аналізу та адаптації симуляційних тренінгів створюються релевантні сценарії.

Третій етап симуляційні тренінги та розбір помилок. Під час занять віртуально відтворюються небезпечні клінічні ситуації, наприклад, випадок введення неправильного дозування антибіотика підлітку. Після вправи керівник групи проводить детальний розбір: учасники разом з ним визначають, де саме сталася помилка, і формують конкретний перелік дій для її усунення та недопущення в майбутньому.

Четвертий етап — аналітика ризиків. Після кожного симуляційного заняття у лікарні проводиться системне узагальнення результатів. Спершу фахівці беруть первинну карту ризиків, складену на основі даних медичних рад і розслідувань, де вже позначені найбільш небезпечні процеси. До цієї карти додають списки виявлених помилок із симуляцій — вони містять конкретні дії чи рішення, що призвели до уявного ускладнення або негативного результату під час тренування. Третім джерелом є результати підсумкового тестування учасників, яке показує рівень засвоєних знань і навичок.

Усі ці матеріали об'єднують у єдину базу, де спеціальне програмне забезпечення групує дані за схожими ознаками. Такий підхід дозволяє швидко побачити, які саме етапи лікувального процесу найчастіше «спотикаються» об одну й ту саму проблему. Якщо, наприклад, виявляється, що помилки найчастіше трапляються під час розрахунку доз ліків, саме ця ділянка позначається як «гаряча точка».

Після виявлення «гарячих точок» комісія з якості разом із навчально-методичним підрозділом вирішує, які дії потрібні: провести цільовий тренінг, внести зміни до внутрішніх інструкцій чи посилити контроль на проблемній ділянці. Завдяки такому колу «виявили — проаналізували — усунули» лікарня безперервно вдосконалює свої процеси й знижує імовірність реальних клінічних інцидентів.

Рішення про повторне навчання, тренінги та організаційні зміни. Після аналітики ризиків робоча група фахівців з якості й освіти узагальнює результати у двовимірній таблиці — «вагомість наслідків / частота помилки». Кожній ситуації присвоюють

оцінку: наскільки серйозними можуть бути наслідки для пацієнта й наскільки часто така помилка трапляється. Поеднання цих двох показників дозволяє швидко визначити пріоритет дій.

Умовно виділяють три зони. Червона зона (високі наслідки й часті помилки) потребує негайного реагування: організовують повторні тренінги, коригують стандартні операційні процедури та посилюють контроль. Жовта зона (помірні наслідки або рідші випадки) передбачає планове навчання — курси й семінари впродовж найближчих місяців. Зелена зона (незначні наслідки і поодинокі випадки) залишається під спостереженням: дані переглядають під час наступного циклу аналізу, щоб переконатися, що ситуація не погіршується.

Після узгодження пропозицій протокол передають керівництву лікарні. Головний лікар затверджує

перелік заходів та матрицю вагомості наслідків та частоти помилки окремим наказом, що надає документу обов'язкової сили й чітко визначає відповідальних та строки виконання заходів. Таким чином матриця стає одним із ключових інструментів системи управління ризиками лікарні: саме на її підставі плануються повторні навчання, зміни у внутрішніх процедурах і подальший контроль ефективності.

Матриця вагомості наслідків та частоти помилки (Таблиця 1) — це інтегрований аналітичний інструмент системи ризикменеджменту лікарні, який поєднує оцінку серйозності можливих клінічних наслідків із частотою виникнення відповідної помилки. Вона слугує для ранжування виявлених ризиків за пріоритетом реагування, визначення обсягу навчальних та організаційних заходів і офіційно затверджується наказом керівника закладу охорони здоров'я.

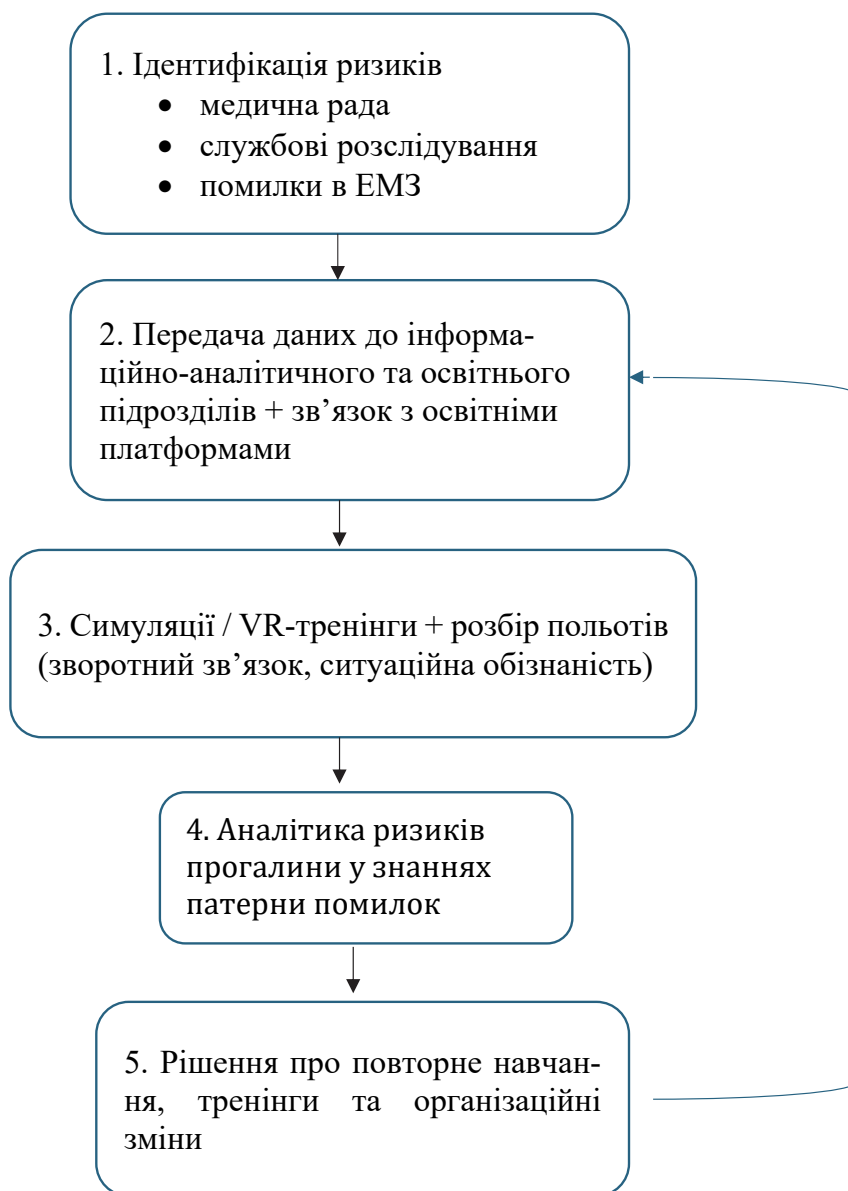


Рис. 1. Інтегрована модель цифрового навчання та управління клінічними ризиками в лікарні

Джерело: розробка автора

Таблиця 1

Приклад заповненої матриці для конкретного відділення (терапія, I півріччя 2025 р.)

№	Виявлена помилка (ризик)	Вагомість наслідків*	Частота за 6 міс**	Зона матриці
1	Неправильне дозування антибіотика ($\geq 30\%$ відхилення від протоколу)	Висока (ризик токсичності, неефективності)	8 разів	Червона
2	Запізнення відправлення зразків крові на коагулограму	Середня (затримка початку терапії)	4 рази	Жовта
3	Пропуск запису про алергію на пеніциліни	Висока (ризик анафілаксії)	1 раз	Помаранчева
4	Заміна периферичного катетера без повної асептики	Середня (ризик флебіту)	7 разів	Червона
5	Невчасне оновлення плану харчування діабетичних пацієнтів	Низька (помірне коливання глікемії)	3 рази	Зелена

* Критерії «Вагомості наслідків»: Висока — можливість тяжкої шкоди або летального наслідку; Середня — тимчасове погіршення стану чи подовження госпіталізації; Низька — мінімальний вплив на здоров'я.

** Критерії «Частоти»: Червона зона — поєднання високої вагомості й частоти ≥ 5 разів за пів року; Жовта зона — середня вагомість або помірна частота; Зелена зона — низька вагомість і рідкісні випадки; Помаранчева — одиничний, але критичний випадок, що потребує негайного розбору.

Джерело: розробка автора

Таким чином, запропонована інтегрована система замикає весь цикл управління клінічними ризиками — від їхньої первинної ідентифікації до впровадження цільових освітніх та організаційних рішень. Модель спирається на наявні в українських лікарнях процеси (медичні ради, службові розслідування, симуляційні центри) і поєднує їх з цифровими інструментами, що забезпечує оперативність, доказовість та економну реалізацію. Блок-схема (рис. 1) і матриця вагомості-частота (табл. 1) утворюють практичний каркас, за яким керівництво може пріоритизувати ризики, планувати навчання та контролювати виконання заходів наказом головного лікаря.

У підсумку модель не лише підвищує безпеку пацієнтів, а й формує в установі культуру постійного вдосконалення: кожен інцидент стає джерелом знань, а кожне навчання — запорукою зменшення помилок у майбутньому. Таким чином модель інтегрованої системи цифрового навчання й контролю клінічних ризиків демонструє, що впровадження системного підходу до ризик-менеджменту є реалістичною та необхідною стратегією для сучасної української лікарні.

Висновки і перспективи подальших досліджень. Впровадження цифрових освітніх технологій довело свою ефективність у зниженні клінічних ризиків. Симуляційні тренінги, VR-сценарії та адаптивні платформи формують практичні навички, підвищують ситуаційну обізнаність персоналу й суттєво зменшують частоту критичних помилок. Це підтверджує доцільність системної цифровізації безперервної медичної освіти в українських лікарнях.

Запропонована інтегрована модель «ризик → аналіз → навчання → вдосконалення» забезпечує замкнений цикл управління безпекою пацієнтів.

Поєднання карти ризиків, симуляційних тренінгів, аналітики й матриці вагомості-частота дозволяє керівництву швидко визначати пріоритети та ухвалювати управлінські рішення.

Закріплення результатів через офіційний наказ робить модель практичним інструментом: визначаються відповідальні особи, строки та критерії оцінки виконання. Це створює передумови для сталої культури безперервного вдосконалення та прозорості відповідальності.

Економічна доцільність моделі полягає у скороченні витрат на лікування ускладнень, зменшенні тривалості госпіталізації та підвищенні ефективності роботи персоналу. Навіть часткове зниження кількості «червоних» інцидентів окупає витрати на симуляційні ресурси протягом двох-трьох років.

Подальші дослідження мають бути спрямовані на: перевірку ефективності моделі у різних типах медичних закладів (обласні, військові, приватні); стандартизацію показників результативності (key performance indicators KPI) для національного моніторингу; інтеграцію даних моделі з платформою eHealth та іншими державними реєстрами; оцінку довгострокових економічних ефектів і впливу на задоволеність пацієнтів; розробку методичних рекомендацій і навчальних пакетів для масштабування моделі на рівні всієї системи охорони здоров'я України.

Отже, авторська модель інтегрованої системи цифрового навчання й контролю клінічних ризиків доводить, що орієнтований на клінічних даних системний підхід є реалістичним шляхом до підвищення безпеки пацієнтів і професійного розвитку медичного персоналу. Її подальша апробація та масштабування становлять перспективний напрям для наукових і практичних досліджень.

Література

1. Ambrosi E., Mezzalana E., Canzan F., Leardini C., Vita G., Marini G., et al. Effectiveness of digital health interventions for chronic conditions management in European primary care settings: Systematic review and meta-analysis. *Int J Med Inform* 2025;196:105820. <https://doi.org/10.1016/j.ijmedinf.2025.105820>.
2. Tian H., Zhang K., Zhang J., Shi J., Qiu H., Hou N., et al. Revolutionizing public health through digital health technology. *Psychol Health Med* 2025;1–16. <https://doi.org/10.1080/13548506.2025.2458254>.
3. Ng A., Celo AN., Fernandes B. Turning the Page on Hardcopy Risk Management Plan Educational Materials: Digitalization Made Possible. *Ther Innov Regul Sci* 2025;59:164-72. <https://doi.org/10.1007/s43441-024-00717-3>.
4. Clinical Decision Support System (CDSS) in primary care: from pragmatic use to the best approach to assess their benefit/risk profile in clinical practice — PubMed n.d. <https://pubmed.ncbi.nlm.nih.gov/35274597/> (accessed April 9, 2025).
5. Using electronic health record data to link families: an illustrative example using intergenerational patterns of obesity — PubMed n.d. <https://pubmed.ncbi.nlm.nih.gov/36857086/> (accessed April 9, 2025).
6. Elendu C., Amaechi DC., Okatta AU., Amaechi EC., Elendu TC., Ezech CP, et al. The impact of simulation-based training in medical education: A review. *Medicine (Baltimore)* 2024;103: e38813. <https://doi.org/10.1097/MD.00000000000038813>.
7. Knevel R., Liao KP. From real-world electronic health record data to real-world results using artificial intelligence. *Ann Rheum Dis* 2023;82:306-11. <https://doi.org/10.1136/ard-2022-222626>.
8. Canfell OJ., Woods L., Meshkat Y., Krivit J., Gunashanhar B., Slade C., et al. The Impact of Digital Hospitals on Patient and Clinician Experience: Systematic Review and Qualitative Evidence Synthesis. *J Med Internet Res* 2024;26: e47715. <https://doi.org/10.2196/47715>.
9. Gomis-Pastor M., Berdún J., Borrás-Santos A., De Dios López A., Fernández-Montells Rama B., García-Esquirol Ó., et al. Clinical Validation of Digital Healthcare Solutions: State of the Art, Challenges and Opportunities. *Healthcare (Basel)* 2024;12:1057. <https://doi.org/10.3390/healthcare12111057>.
10. Canfell OJ., Woods L., Meshkat Y., Krivit J., Gunashanhar B., Slade C., et al. The Impact of Digital Hospitals on Patient and Clinician Experience: Systematic Review and Qualitative Evidence Synthesis. *J Med Internet Res* 2024;26: e47715. <https://doi.org/10.2196/47715>.
11. McGowan J., Wojahn A., Nicolini JR. Risk Management Event Evaluation and Responsibilities. StatPearls, Treasure Island (FL): StatPearls Publishing; 2025.
12. Arnold JL. Risk and risk assessment in health emergency management. *Prehosp Disaster Med* 2005;20:143-54. <https://doi.org/10.1017/s1049023x00002363>.
13. Buchberger W., Schmied M., Schomaker M., Del Rio A., Siebert U. Implementation of a comprehensive clinical risk management system in a university hospital. *Z Evid Fortbild Qual Gesundheitswes* 2024;184:18-25. <https://doi.org/10.1016/j.zefq.2023.11.008>.
14. van Moll C, Egberts T, Wagner C, Zwaan L, Ten Berg M. The Nature, Causes, and Clinical Impact of Errors in the Clinical Laboratory Testing Process Leading to Diagnostic Error: A Voluntary Incident Report Analysis. *J Patient Saf* 2023;19:573-9. <https://doi.org/10.1097/PTS.0000000000001166>.
15. Rodziewicz TL., Houseman B., Vaqar S., Hipskind JE. Medical Error Reduction and Prevention. StatPearls, Treasure Island (FL): StatPearls Publishing; 2025.
16. Wachter B. The Irony of Automation: Why Clinicians Let Computers Make Mistakes. *Wired* n.d.
17. Wachter B. How to Make Hospital Tech Much, Much Safer. *Wired* n.d.
18. Adams JG, Bohan JS. System contributions to error. *Acad Emerg Med* 2000;7:1189–93. <https://doi.org/10.1111/j.1553-2712.2000.tb00463.x>.
19. Sarfati L., Ranchon F., Vantard N., Schwiertz V., Larbre V., Parat S., et al. Human-simulation-based learning to prevent medication error: A systematic review. *J Eval Clin Pract* 2019;25:11-20. <https://doi.org/10.1111/jep.12883>.
20. Mondal H., Mondal S.. Adopting augmented reality and virtual reality in medical education in resource-limited settings: constraints and the way forward. *Adv Physiol Educ* 2025;49:503-7. <https://doi.org/10.1152/advan.00027.2025>.
21. Fontaine G., Cossette S., Maheu-Cadotte M-A., Mailhot T., Deschênes M-F., Mathieu-Dupuis G., et al. Efficacy of adaptive e-learning for health professionals and students: a systematic review and meta-analysis. *BMJ Open* 2019;9: e025252. <https://doi.org/10.1136/bmjopen-2018-025252>.
22. De Gagne JC., Park HK., Hall K., Woodward A., Yamane S., Kim SS. Microlearning in Health Professions Education: Scoping Review. *JMIR Med Educ* 2019;5: e13997. <https://doi.org/10.2196/13997>.
23. Van Ostaeyen S., Embo M., Schellens T., Valcke M. Training to Support ePortfolio Users During Clinical Placements: a Scoping Review. *Med Sci Educ* 2022;32:921-8. <https://doi.org/10.1007/s40670-022-01583-0>.

References

1. Ambrosi E., Mezzalana E., Canzan F., Leardini C., Vita G., Marini G., et al. Effectiveness of digital health interventions for chronic conditions management in European primary care settings: Systematic review and meta-analysis. *Int J Med Inform* 2025;196:105820. <https://doi.org/10.1016/j.ijmedinf.2025.105820>.

2. Tian H., Zhang K., Zhang J., Shi J., Qiu H., Hou N., et al. Revolutionizing public health through digital health technology. *Psychol Health Med* 2025;1-16. <https://doi.org/10.1080/13548506.2025.2458254>.
3. Ng A., Celo AN., Fernandes B. Turning the Page on Hardcopy Risk Management Plan Educational Materials: Digitalization Made Possible. *Ther Innov Regul Sci* 2025;59:164-72. <https://doi.org/10.1007/s43441-024-00717-3>.
4. Clinical Decision Support System (CDSS) in primary care: from pragmatic use to the best approach to assess their benefit/risk profile in clinical practice — PubMed n.d. <https://pubmed.ncbi.nlm.nih.gov/35274597/> (accessed April 9, 2025).
5. Using electronic health record data to link families: an illustrative example using intergenerational patterns of obesity — PubMed n.d. <https://pubmed.ncbi.nlm.nih.gov/36857086/> (accessed April 9, 2025).
6. Elendu C, Amaechi DC, Okatta AU, Amaechi EC, Elendu TC, Ezech CP, et al. The impact of simulation-based training in medical education: A review. *Medicine (Baltimore)* 2024;103: e38813. <https://doi.org/10.1097/MD.00000000000038813>.
7. Knevel R., Liao KP. From real-world electronic health record data to real-world results using artificial intelligence. *Ann Rheum Dis* 2023;82:306–11. <https://doi.org/10.1136/ard-2022-222626>.
8. Canfell OJ., Woods L., Meshkat Y., Krivit J., Gunashanhar B., Slade C., et al. The Impact of Digital Hospitals on Patient and Clinician Experience: Systematic Review and Qualitative Evidence Synthesis. *J Med Internet Res* 2024;26: e47715. <https://doi.org/10.2196/47715>.
9. Gomis-Pastor M, Berdún J, Borrás-Santos A, De Dios López A, Fernández-Montells Rama B, García-Esquirol Ó, et al. Clinical Validation of Digital Healthcare Solutions: State of the Art, Challenges and Opportunities. *Healthcare (Basel)* 2024;12:1057. <https://doi.org/10.3390/healthcare12111057>.
10. Canfell OJ., Woods L., Meshkat Y., Krivit J., Gunashanhar B., Slade C., et al. The Impact of Digital Hospitals on Patient and Clinician Experience: Systematic Review and Qualitative Evidence Synthesis. *J Med Internet Res* 2024;26: e47715. <https://doi.org/10.2196/47715>.
11. McGowan J., Wojahn A., Nicolini JR. Risk Management Event Evaluation and Responsibilities. StatPearls, Treasure Island (FL): StatPearls Publishing; 2025.
12. Arnold JL. Risk and risk assessment in health emergency management. *Prehosp Disaster Med* 2005;20:143-54. <https://doi.org/10.1017/s1049023x00002363>.
13. Buchberger W., Schmied M., Schomaker M., Del Rio A., Siebert U. Implementation of a comprehensive clinical risk management system in a university hospital. *Z Evid Fortbild Qual Gesundheitswes* 2024;184:18-25. <https://doi.org/10.1016/j.zefq.2023.11.008>.
14. van Moll C., Egberts T., Wagner C., Zwaan L., Ten Berg M. The Nature, Causes, and Clinical Impact of Errors in the Clinical Laboratory Testing Process Leading to Diagnostic Error: A Voluntary Incident Report Analysis. *J Patient Saf* 2023;19:573-9. <https://doi.org/10.1097/PTS.0000000000001166>.
15. Rodziewicz TL., Houseman B., Vaqar S., Hipskind JE. Medical Error Reduction and Prevention. StatPearls, Treasure Island (FL): StatPearls Publishing; 2025.
16. Wachter B. The Irony of Automation: Why Clinicians Let Computers Make Mistakes. *Wired* n.d.
17. Wachter B. How to Make Hospital Tech Much, Much Safer. *Wired* n.d.
18. Adams JG, Bohan JS. System contributions to error. *Acad Emerg Med* 2000;7:1189-93. <https://doi.org/10.1111/j.1553-2712.2000.tb00463.x>.
19. Sarfati L., Ranchon F., Vantard N., Schwiertz V., Larbre V., Parat S., et al. Human-simulation-based learning to prevent medication error: A systematic review. *J Eval Clin Pract* 2019;25:11-20. <https://doi.org/10.1111/jep.12883>.
20. Mondal H., Mondal S. Adopting augmented reality and virtual reality in medical education in resource-limited settings: constraints and the way forward. *Adv Physiol Educ* 2025;49:503-7. <https://doi.org/10.1152/advan.00027.2025>.
21. Fontaine G., Cossette S, Maheu-Cadotte M-A., Mailhot T., Deschênes M-F., Mathieu-Dupuis G., et al. Efficacy of adaptive e-learning for health professionals and students: a systematic review and meta-analysis. *BMJ Open* 2019;9: e025252. <https://doi.org/10.1136/bmjopen-2018-025252>.
22. De Gagne JC., Park HK., Hall K., Woodward A., Yamane S., Kim SS. Microlearning in Health Professions Education: Scoping Review. *JMIR Med Educ* 2019;5: e13997. <https://doi.org/10.2196/13997>.
23. Van Ostaeyen S., Embo M., Schellens T., Valcke M. Training to Support ePortfolio Users During Clinical Placements: a Scoping Review. *Med Sci Educ* 2022;32:921-8. <https://doi.org/10.1007/s40670-022-01583-0>.

Стаття надійшла до редакції 05.05.2025

УДК 35.072.6:004.738.5

Михайлов Сергій Юрійович

аспірант кафедри державного управління

Навчально-наукового інституту публічного управління та державної служби

Київського національного університету імені Тараса Шевченка

Mykhailov Serhii

Postgraduate Student of the Department of Public Administration

Educational and Scientific Institute of Public Administration and Civil Service of

Taras Shevchenko National University of Kyiv

ORCID: 0009-0000-1437-2292

DOI: 10.25313/2617-572X-2025-5-10957

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ В ПУБЛІЧНОМУ УПРАВЛІННІ УКРАЇНИ: ЄВРОПЕЙСЬКІ ОРІЄНТИРИ

INSTITUTIONAL SUPPORT FOR DIGITAL SOVEREIGNTY IN PUBLIC ADMINISTRATION OF UKRAINE: EUROPEAN GUIDELINES

Анотація. Вступ. У контексті глобальної цифровізації, зростаючої залежності держав від транснаціональних технологічних корпорацій, а також активізації кіберзагроз і гібридних впливів, проблема забезпечення цифрового суверенітету набуває особливого значення для країн, що перебувають у процесі демократичного та технологічного становлення. Для України, яка веде боротьбу за політичну незалежність і водночас здійснює інтенсивну цифрову трансформацію, формування дієвої системи цифрового суверенітету є критично важливим завданням державного управління. Пошук оптимальної моделі інституційного забезпечення цифрового суверенітету, з урахуванням успішного досвіду Європейського Союзу, постає як ключовий напрям публічної політики.

Мета. Стаття має на меті проаналізувати сутність поняття цифрового суверенітету та його значення в контексті публічного управління, визначити інституційні засади забезпечення цифрового суверенітету в ЄС, оцінити стан інституційного забезпечення цифрового суверенітету в Україні та розробити пропозиції щодо адаптації європейських практик для українських реалій.

Матеріали і методи. Методологічну основу дослідження становлять структурно-функціональний, інституційний, порівняльно-правовий аналіз, контент-аналіз нормативних актів та стратегічних документів, а також елементи емпіричного аналізу, зокрема вивчення міжнародних рейтингів та звітів галузевих інституцій. Джерельну базу склали акти законодавства України та ЄС, аналітичні звіти, державні програми, дані міжнародних індексів (GCI, EGDI, DESI тощо).

Результати. У статті уточнено зміст категорії «цифровий суверенітет» як складової національного суверенітету в умовах цифрової трансформації. Проаналізовано ключові інституційні компоненти європейської моделі цифрового суверенітету, такі як GAIA-X, Chips Act, політика кібербезпеки ЄС, Horizon Europe. Проведено оцінку стану інституційного забезпечення цифрового суверенітету в Україні, виявлено як позитивні зрушення, зокрема розвиток цифрових сервісів, нормативне закріплення кібербезпеки, так і проблемні аспекти – залежність від іноземних хмарних платформ, фрагментарність законодавства, обмежена координація цифрової політики. Запропоновано напрями адаптації європейських підходів з урахуванням українських викликів, серед яких: розширення інституційної спроможності державних органів, імплементація принципів суверенного зберігання даних, розвиток власної технологічної інфраструктури.

Перспективи. Подальші дослідження доцільно зосередити на вивченні механізмів публічно-приватного партнерства у формуванні цифрового суверенітету, а також на оцінці ефективності інтеграції України у європейський цифровий простір у контексті майбутнього членства в ЄС. Також актуальним є моніторинг впровадження законодавства у сфері кібербезпеки та цифрових прав громадян.

Ключові слова: кіберзагроза, гібридний вплив, інформаційний простір, технологічні виклики.

Summary. Introduction. In the context of global digitalization, the growing dependence of states on transnational technology corporations, as well as the intensification of cyber threats and hybrid influences, the problem of ensuring digital sovereignty is of particular importance for countries in the process of democratic and technological formation. For Ukraine, which is fighting for political independence and at the same time carrying out intensive digital transformation, the formation of an effective system of digital sovereignty is a critically important task of public administration. The search for the optimal model of institutional support for digital sovereignty, taking into account the successful experience of the European Union, appears as a key direction of public policy.

Purpose. The article aims to analyze the essence of the concept of digital sovereignty and its significance in the context of public administration, to determine the institutional principles of ensuring digital sovereignty in the EU, to assess the state of institutional support for digital sovereignty in Ukraine and to develop proposals for adapting European practices to Ukrainian realities.

Materials and methods. The methodological basis of the study is structural-functional, institutional, comparative-legal analysis, content analysis of regulatory acts and strategic documents, as well as elements of empirical analysis, in particular, the study of international ratings and reports of industry institutions. The source base was made up of acts of Ukrainian and EU legislation, analytical reports, state programs, data from international indices (GCI, EGDI, DESI, etc.).

Results. The article clarifies the content of the category "digital sovereignty" as a component of national sovereignty in the context of digital transformation. The key institutional components of the European model of digital sovereignty are analyzed, such as GAIA-X, Chips Act, EU cybersecurity policy, Horizon Europe. An assessment of the state of institutional support for digital sovereignty in Ukraine was conducted, revealing both positive developments, in particular the development of digital services, regulatory consolidation of cybersecurity, and problematic aspects – dependence on foreign cloud platforms, fragmentation of legislation, limited coordination of digital policy. Directions for adapting European approaches taking into account Ukrainian challenges are proposed, including: expanding the institutional capacity of state bodies, implementing the principles of sovereign data storage, developing our own technological infrastructure.

Prospects. Further research should be focused on studying the mechanisms of public-private partnership in the formation of digital sovereignty, as well as on assessing the effectiveness of Ukraine's integration into the European digital space in the context of future membership in the EU. Monitoring the implementation of legislation in the field of cybersecurity and digital rights of citizens is also relevant.

Key words: cyber threat, hybrid influence, information space, technological challenges.

Постановка проблеми. У сучасних умовах цифрової трансформації суспільства та державного управління питання цифрового суверенітету набуває особливої актуальності. В умовах зростання кіберзагроз, гібридних впливів та залежності від іноземних цифрових платформ постає необхідність створення ефективної інституційної системи, здатної забезпечити захист інформаційного простору, збереження контролю над цифровими ресурсами та гарантування національного інтересу в цифровій сфері. Україна, яка декларує курс на європейську інтеграцію, зобов'язана враховувати європейські підходи до забезпечення цифрового суверенітету, які поєднують інноваційний розвиток, прозорість, дотримання прав людини та стратегічну автономію. Проте на сьогодні відсутня цілісна модель інституційного забезпечення цифрового суверенітету в публічному управлінні, що ускладнює реалізацію ефективної цифрової політики, знижує стійкість держави до зовнішніх технологічних викликів і гальмує гармонізацію з європейськими стандартами. Це зумовлює потребу у науковому аналізі існуючих викликів, оцінці стану інституційного середовища та формуванні рекомендацій щодо його удосконалення з урахуванням європейського досвіду.

Аналіз останніх досліджень і публікацій. У вітчизняному та зарубіжному науковому дискурсі цифровий суверенітет дедалі частіше розглядається як базовий компонент державної безпеки, самостійності в кіберпросторі та ефективності публічного управління. Водночас аналіз наявної наукової літератури

засвідчує, що питання інституційного забезпечення цифрового суверенітету залишається фрагментарно висвітленим, особливо в українському контексті.

Серед сучасних дослідників важливим є внесок Ю. П. Калайди [1], який здійснив порівняльний аналіз моделей цифрового суверенітету, сформованих у провідних демократичних країнах. Автор підкреслює, що в умовах геополітичного протистояння цифровий суверенітет виходить за межі технічного або правового явища, набуваючи стратегічного значення. У роботі систематизовано закордонний досвід (насамперед ЄС, США, Китаю) щодо захисту даних, розвитку національної хмарної інфраструктури та посилення кібербезпеки, проте потребує подальшої конкретизації питання імплементації подібних моделей в українських умовах.

І. М. Доронін [2] зосереджується на юридичних колізіях, що виникають у процесі «суверенізації Інтернету». Дослідник звертає увагу на конфлікт між прагненням держави до контролю над цифровим простором і необхідністю збереження відкритості глобальної мережі, що обумовлює складність формування єдиної моделі цифрового суверенітету. Його висновки актуалізують проблему балансування між технологічною автономією та дотриманням міжнародних стандартів прав людини.

О. М. Солодка [3] розкриває проблематику інформаційного суверенітету через правовий дискурс, зокрема акцентуючи на законодавчому регулюванні сфер інформаційної безпеки, збереження

персональних даних та інформаційної незалежності. Її підхід дозволяє розглядати цифровий суверенітет як логічне продовження інформаційного, однак не дає повного уявлення про інституційну структуру забезпечення останнього.

Зовнішньополітичний вимір цифрового суверенітету ґрунтовно аналізує С. Гнатюк [4]. У фокусі його дослідження — цифрове візіонерство ЄС і США, їхні підходи до регуляції інтернет-простору, побудови цифрової інфраструктури та стратегій кіберзахисту. Автор окреслює концепцію «цифрової солідарності» як інструмент інтеграції цифрових політик демократичних країн, що становить інтерес у контексті прагнення України до євроінтеграції.

І. М. Милосердна [5] аналізує сучасні інтерпретації поняття цифрового суверенітету та ступінь їх відображення у практичних кроках державної політики. Авторка наголошує на розриві між науковою риторикою та реальним станом речей у сфері цифрової незалежності України, вказуючи на нестачу системного підходу та узгодженої нормативно-правової бази.

У більш ранній роботі Д. В. Дубова [6] цифровий суверенітет розглядається як новий тип національного суверенітету, що формується під впливом цифрових технологій і глобальних інформаційних потоків. Він визначає низку викликів для України, серед яких — технічна залежність, слабка інституційна спроможність та потреба в адаптації найкращих практик. Водночас його дослідження є радше концептуальним, без глибокого аналізу конкретних управлінських інструментів.

К. В. Єфремова [7] підкреслює роль цифрового суверенітету як ключового чинника конкурентоспроможності держави в умовах Індустрії 4.0. Вона наголошує на необхідності побудови власної цифрової екосистеми, здатної забезпечити автономне функціонування критичної інфраструктури. Її напрацювання є цінними для формування інституційної платформи цифрового суверенітету, однак потребують розширення в напрямі публічно-управлінських аспектів.

У зарубіжному науковому полі вартим уваги є дослідження А. Баррінья, Г. Крістоу (A. Barrinha, G. Christou) [8], які аналізують європейську політику цифрового суверенітету як форму стратегічного самоствердження в кіберпросторі. Автори вказують на формування окремої «мови суверенітету», що дозволяє ЄС артикулювати свої інтереси в діджитал-сфері через створення нормативної бази, інституційних структур і технічних стандартів. Їхні висновки підкреслюють складність поєднання політичної волі та технічної реалізації цифрової автономії.

Отже, незважаючи на наявність низки цінних досліджень, залишається недостатньо розкритим комплекс питань, пов'язаних із практичною інституціоналізацією цифрового суверенітету в системі публічного управління України. Зокрема, вкрай обмежено представлені дослідження щодо порівняння

інституційної моделі ЄС з українською дійсністю, а також відсутні узагальнення щодо адаптації європейських управлінських практик до українських умов. Саме заповнення цих прогалин і визначено як мету цього дослідження.

Метою статті є дослідження інституційних засад формування та реалізації цифрового суверенітету в системі публічного управління України з урахуванням європейських підходів, а також розроблення науково обґрунтованих рекомендацій щодо імплементації ефективної моделі цифрового суверенітету в національну управлінську практику.

Завдання статті:

- проаналізувати сутність поняття цифрового суверенітету та його значення в контексті публічного управління;
- визначити основні інституційні складові цифрового суверенітету в європейському управлінському просторі;
- оцінити стан інституційного забезпечення цифрового суверенітету в Україні;
- розробити пропозиції щодо адаптації та впровадження європейських практик забезпечення цифрового суверенітету в Україні.

Матеріали і методи. У процесі дослідження використано комплекс загальнонаукових і спеціальних методів, що дозволили здійснити ґрунтовний аналіз цифрового суверенітету як складної категорії публічного управління. Основу джерельної бази становили чинні нормативно-правові акти України та Європейського Союзу, зокрема Регламент (ЄС) 2016/679 (GDPR), Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки України (2021–2025), законопроекти, програмні документи ЄС (наприклад, Digital Decade 2030, GAIA-X, Chips Act, Data Governance Act) та відповідні урядові постанови.

Метод структурно-функціонального аналізу застосовано для виявлення інституційних елементів цифрового суверенітету та аналізу їх взаємозв'язків у європейській та українській практиках. Порівняльно-правовий метод дозволив зіставити підходи до інституційного забезпечення цифрового суверенітету в ЄС та Україні, визначити загальні риси та відмінності. У ході дослідження також застосовано системний підхід для комплексного розуміння сутності цифрового суверенітету та можливостей його інституційного забезпечення в умовах трансформацій сучасного глобального цифрового простору.

Виклад основного матеріалу. У сучасних умовах стрімкої цифровізації усіх сфер суспільного життя проблема цифрового суверенітету набуває особливої актуальності як з точки зору національної безпеки, так і в контексті ефективного функціонування системи публічного управління. Традиційно поняття суверенітету трактується як верховенство держави, народу або нації у внутрішній та зовнішній політиці, що забезпечує самостійність прийняття

рішень та реалізацію стратегічних цілей [9]. У науковій літературі виділяють три основні типи суверенітету — державний, народний і національний, кожен з яких має свого суб'єкта: відповідно, державу, народ та націю. У межах мононаціональних держав ці види суверенітету можуть збігатися, що спрощує питання управління, тоді як у багатонаціональних державах відбувається постійна взаємодія, узгодження та, подекуди, конфлікт між ними. У цьому контексті державний суверенітет відіграє ключову роль як юридично та політично оформлений механізм реалізації народного волевиявлення, що охоплює як внутрішню автономію державної влади, так і її незалежність у зовнішньополітичних стосунках.

З утвердженням інформаційного суспільства традиційне розуміння державного суверенітету, що спирається на територіальні межі юрисдикції, зазнає суттєвих трансформацій. Глобальні інформаційні потоки, кіберзалежність, розвиток транснаціональних цифрових платформ та систем штучного інтелекту розмивають межі між внутрішнім і зовнішнім простором функціонування держави. У зв'язку з цим у науковий обіг активно входять поняття «інформа-

ційний суверенітет» і «цифровий суверенітет». Інформаційний суверенітет розглядається як здатність держави контролювати, регулювати та захищати національні інформаційні ресурси та інформаційні потоки на своїй території [10]. Він передбачає наявність інституційних механізмів з протидії інформаційно-психологічним впливам, забезпечення автономії національної інформаційної політики та створення умов для безпечного функціонування вітчизняного інформаційного простору.

Цифровий суверенітет є логічним розвитком концепції інформаційного суверенітету, зосередженим переважно на аспектах незалежності у сфері інформаційно-комунікаційних технологій (ІКТ), інфраструктури цифрового управління, кібербезпеки, збереження та обробки персональних даних, а також на цифровій інфраструктурі, через яку здійснюється реалізація управлінських функцій. Він полягає у здатності держави самостійно визначати цифрову політику, керувати розвитком та захистом цифрових систем, гарантувати недопущення зовнішнього втручання у критичні елементи цифрового середовища, включно з державними реєстрами, каналами

Таблиця 1

Функції цифрового суверенітету у публічному секторі

Зміст функції	Значення для публічного управління
<i>Нормативно-регуляторна</i>	
Формування та впровадження законодавчої та регуляторної бази, що визначає правила цифрової діяльності.	Забезпечує контроль над цифровими процесами, легітимізує втручання держави у сферу ІКТ і платформ.
<i>Юрисдикційна</i>	
Встановлення меж державної юрисдикції у цифровому просторі.	Гарантує право держави визначати, хто і як може здійснювати цифрову діяльність у її інформаційно-комунікаційному полі.
<i>Кібербезпекова</i>	
Створення умов для захисту інформаційної інфраструктури від зовнішніх і внутрішніх загроз.	Сприяє безпеці критичних об'єктів, запобігає втраті контролю над цифровими платформами, даними, системами управління.
<i>Технологічно-інфраструктурна</i>	
Розвиток власної цифрової інфраструктури, включно з дата-центрами, хмарними сервісами, національними мережами.	Знижує залежність від іноземних технологій, підтримує цифрову автономію та стійкість у кризових ситуаціях.
<i>Координаційна</i>	
Узгодження дій державних інституцій, бізнесу та громадянського суспільства в цифровій сфері.	Створює єдину цифрову політику, забезпечує узгоджене управління цифровою трансформацією.
<i>Інформаційно-комунікаційна</i>	
Регулювання інформаційних потоків, протидія дезінформації, контроль над інформаційним простором.	Забезпечує національну інформаційну безпеку, зменшує вплив зовнішніх інформаційно-психологічних операцій.
<i>Економічна</i>	
Створення умов для розвитку національного цифрового ринку та зменшення цифрової залежності від іноземних акторів.	Підвищує інноваційність публічного сектору, зберігає цифрову ренту у межах держави.
<i>Освітньо-культурна</i>	
Сприяння формуванню цифрової культури, медіаграмотності та цифрової свідомості населення.	Забезпечує стійкість суспільства до маніпуляцій, сприяє інклюзивності та ефективному управлінню цифровими змінами.

Джерело: власна розробка автора

комунікації, платформами публічного управління та системами електронного урядування.

Значення цифрового суверенітету в контексті публічного управління полягає передусім у створенні передумов для формування незалежної, стабільної та безпечної цифрової держави, спроможної забезпечити захист громадян в інформаційному середовищі, збереження цілісності цифрових процесів управління та мінімізацію ризиків цифрової колонізації через надмірну залежність від іноземних технологій або нормативних режимів. У публічному секторі цифровий суверенітет дозволяє підвищити прозорість та підзвітність управлінських процесів, забезпечити безперебійну роботу електронних послуг, захист персональних даних громадян, унеможливити втручання в інфраструктуру державного управління та забезпечити стратегічний контроль над критичною цифровою інфраструктурою.

У цьому контексті доцільно виокремити ключові функції цифрового суверенітету у публічному секторі, які визначають його системну роль у забезпеченні ефективного, безпечного та незалежного державного управління в цифрову епоху. Таблиця 1 узагальнює основні напрями реалізації цифрового суверенітету на рівні державних інституцій.

У контексті загострення геополітичного протистояння та швидкого розвитку цифрових технологій, формування концепції цифрового суверенітету набуває ключового значення в управлінських практиках сучасного Європейського Союзу. ЄС дедалі активніше позиціонує себе як незалежний глобальний суб'єкт, здатний забезпечити контроль над власною цифровою інфраструктурою, інформаційними потоками та технологічною політикою. Це прагнення до суверенізації цифрового простору не є ізольованим випадком, а частиною ширшої європейської стратегії автономізації в умовах нової реальності — постамериканського, багатопольярного цифрового світу. Відтак, цифровий суверенітет розглядається не лише як технічна або правова категорія, а як стратегічна управлінська мета, що вимагає створення відповідної інституційної архітектури на рівні ЄС та його держав-членів.

Основними інституційними складовими цифрового суверенітету в європейському управлінському просторі виступають: Європейська комісія, відповідальні агентства з питань цифрових технологій та кібербезпеки (зокрема, Європейське агентство з кібербезпеки — ENISA), Європейська рада з питань цифрового десятиліття, а також національні органи регулювання в державах-членах. Ключову роль відіграє Європейська комісія, яка не лише ініціює відповідні законодавчі акти, але й забезпечує стратегічне планування, моніторинг реалізації цифрової політики, а також координацію міждержавних дій у сфері цифрової трансформації. Зокрема, такі ініціативи, як Digital Services Act (DSA), Digital Markets Act (DMA), Data Governance Act (DGA) та Європейська

декларація про цифрові права і принципи, мають не лише нормативну, а й інституційну функцію — вони закладають підґрунтя для формування єдиної європейської цифрової юрисдикції.

ENISA, зі свого боку, виконує функції експертного, консультативного й координаційного центру у сфері забезпечення кіберстійкості та управління ризиками цифрового середовища. Вона активно взаємодіє з національними органами кібербезпеки та бере участь у формуванні спільних стандартів та методик для країн-членів ЄС. Іншим важливим елементом є платформи багаторівневої координації, які формуються на основі Стратегії цифрового десятиліття ЄС — 2030 [гнідий]. У рамках цієї стратегії створено механізм співпраці між інституціями ЄС і державами-членами з метою досягнення чотирьох ключових цілей: розвиток цифрових навичок, цифрової інфраструктури, цифровізації бізнесу та електронного урядування. Таким чином, формується комплексна інституційна модель, що передбачає як вертикальну (інституції ЄС — держави-члени), так і горизонтальну (між-агентську та міждержавну) інтеграцію.

Особливу увагу в європейській моделі цифрового суверенітету приділено питанням локалізації даних та розвитку стратегічно важливих технологій. Для цього ЄС просуває такі ініціативи, як GAIA-X — федеративна європейська хмарна інфраструктура, спрямована на зменшення залежності від американських і китайських технологічних гігантів. У свою чергу, Інвестиційна програма Horizon Europe та нова Ініціатива Chips Act мають на меті підтримку інновацій, R&D, розвиток власного напівпровідникового виробництва та цифрових індустрій, що також прямо пов'язано з забезпеченням суверенітету у високотехнологічному вимірі. Крім того, не менш важливим інструментом є політика кібербезпеки, що охоплює як нормативно-правові документи, так і інфраструктурні проекти, зокрема спільні платформи для виявлення, реагування та протидії кіберзагрозам.

Таким чином, формування цифрового суверенітету Європейського Союзу базується на багаторівневому та комплексному підході, що охоплює технологічний розвиток, захист персональних даних, інноваційне виробництво та кібербезпеку. Реалізація відповідних стратегій потребує ефективної координації між низкою інституцій ЄС, кожна з яких виконує специфічні функції у цій сфері. З метою систематизації основних організаційних компонентів цифрового суверенітету ЄС доцільно виділити їх у структурованому вигляді (табл. 2).

Таким чином, інституційна модель цифрового суверенітету в ЄС є багатокомпонентною системою, яка поєднує політичні, технічні, правові та управлінські інструменти. На відміну від американської моделі цифрової солідарності, заснованої на глобальному партнерстві, європейський підхід ґрунтується на прагненні до стратегічної автономії та контролю

Таблиця 2

Основні інституційні складові цифрового суверенітету Європейського Союзу

Інституція/Орган	Ключові функції у сфері цифрового суверенітету	Ключові ініціативи / документи
Європейська комісія	Розробка цифрової політики; законодавчі ініціативи; реалізація програм цифровізації	Цифровий компас 2030, DSA, DMA, GAIA-X
Європейський парламент	Законодавча підтримка ініціатив; контроль над виконанням цифрових стратегій	Підтримка DSA/DMA; обговорення питань кібербезпеки
Рада Європейського Союзу	Співзаконодавець; визначення стратегічних напрямів цифрового розвитку	Схвалення Цифрового компаса; позиції щодо кібербезпеки
ENISA (Агентство ЄС з кібербезпеки)	Координація кібербезпеки; створення стандартів; допомога державам-членам	Європейський акт про кіберстійкість; національні стратегії
EDPB (Європейська рада із захисту даних)	Контроль за дотриманням GDPR; захист цифрових прав громадян	Тлумачення та рекомендації щодо застосування GDPR
Національні регулятори (держави-члени)	Виконання цифрових стратегій ЄС на національному рівні; адаптація регулювання	Національні стратегії цифрової трансформації
Європейська рада з інновацій (EIC)	Фінансування інновацій, стартапів у цифровій сфері	Horizon Europe, Digital Europe Programme
Data Governance Board (DGB)	Координація використання даних у ЄС; забезпечення суверенітету даних	Data Governance Act; European Data Spaces

Джерело: власна розробка автора

над ключовими елементами цифрової екосистеми. Це зумовлено не лише прагненням до захисту економічних інтересів, а й необхідністю гарантувати інформаційну безпеку, технологічну незалежність та захист основоположних прав громадян у цифровому середовищі. У майбутньому посилення інституційного виміру цифрового суверенітету в Європі, імовірно, відіграватиме дедалі важливішу роль у формуванні нових глобальних правил цифрової гри.

Україна, перебуваючи в умовах війни та активної цифрової трансформації, стикається з низкою викликів у сфері цифрового суверенітету. Ці виклики охоплюють як внутрішні проблеми, пов'язані з нормативно-правовим забезпеченням та інституційною спроможністю, так і зовнішні загрози, зокрема кібератаки з боку держав-агресорів.

Одним із ключових викликів є відсутність цілісної та узгодженої нормативно-правової бази у сфері цифрового суверенітету. Хоча в Україні існують окремі законодавчі акти, спрямовані на регулювання інформаційної безпеки та кібербезпеки, вони часто не узгоджені між собою та не враховують сучасних викликів. Одним із ключових нормативних актів у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року, який визначає правові та організаційні основи захисту національних інтересів у кіберпросторі, а також повноваження державних органів у цій сфері [11]. У 2025 році було затверджено План заходів з реалізації Стратегії кібербезпеки України, який передбачає конкретні кроки щодо посилення кіберзахисту, включаючи створення єдиної системи реагування на кіберінциденти та впровадження посад відповідальних за кібербезпеку в органах влади та критичній інфраструктурі [12].

Крім того, в березні 2025 року Верховна Рада ухвалила Закон № 11290, який вносить зміни до законодавства щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури. Цей закон передбачає створення єдиної системи реагування на кібератаки та запровадження посад відповідальних за кібербезпеку в органах влади та критичній інфраструктурі. У сфері цифрової трансформації важливу роль відіграє Міністерство цифрової трансформації України, яке координує впровадження електронних послуг та розвиток цифрової інфраструктури. Зокрема, реалізується проект «Дія», який об'єднує низку електронних сервісів для громадян та бізнесу.

Україна постійно зазнає кібератак з боку держав-агресорів, що спрямовані на дестабілізацію інформаційного простору, порушення роботи критичної інфраструктури та викрадення конфіденційної інформації. За даними Національного координаційного центру кібербезпеки при РНБО України, у 2024 році було зафіксовано понад 3 000 кібератак на державні органи та об'єкти критичної інфраструктури [13]. Ці атаки включали як DDoS-атаки, так і складніші методи, такі як фішинг, використання шкідливого програмного забезпечення та експлуатація вразливостей у програмному забезпеченні. Особливо небезпечними є атаки на енергетичну, фінансову та транспортну інфраструктуру, які можуть мати серйозні наслідки для національної безпеки та економіки країни.

Ще одним викликом є висока залежність України від іноземних технологій, зокрема програмного забезпечення, хмарних сервісів та телекомунікаційного обладнання. Це створює ризики для цифрового суверенітету, оскільки іноземні постачальники можуть

обмежити доступ до своїх продуктів або зловживати своїм становищем. Крім того, використання іноземних технологій може призвести до витоку конфіденційної інформації та порушення національної безпеки.

Україна має значний потенціал у сфері ІТ та інновацій, проте розвиток національних технологій стримується низкою факторів, зокрема недостатнім фінансуванням, відсутністю державної підтримки та нестачею кваліфікованих кадрів. Це ускладнює створення власних технологічних рішень, які могли б замінити іноземні аналоги та забезпечити цифровий суверенітет країни.

Для подолання зазначених викликів Україна може вжити низку заходів. Зокрема, розробити та впровадити комплексну стратегію цифрового суверенітету, яка включатиме оновлення нормативно-правової бази, створення інституційної структури та визначення пріоритетних напрямів розвитку. Також важливо забезпечити зменшення залежності від іноземних технологій через підтримку національних виробників, розвиток власних технологічних рішень та створення сприятливих умов для інноваційної діяльності. Успішна реалізація цих заходів вимагатиме консолідації зусиль держави, бізнесу, наукової спільноти та громадянського суспільства. Тільки за умови спільної роботи та стратегічного підходу Україна зможе забезпечити свій цифровий суверенітет та стати повноцінним учасником глобального цифрового простору.

Висновки і перспективи подальших досліджень. У результаті проведеного дослідження було з'ясовано, що цифровий суверенітет являє собою багатогранне поняття, що поєднує технологічну незалежність держави, здатність захищати критичну цифрову інфраструктуру та здійснювати ефективне публічне управління в умовах цифрової трансформації. У контексті публічного управління цифровий суверенітет відіграє ключову роль у забезпеченні національної безпеки, збереженні інформаційного простору, а також у гарантуванні цифрових прав громадян. Аналіз інституційного наповнення цього поняття в європейському управлінському просторі дозволив виокремити низку ключових елемен-

тів, серед яких: наявність стратегічних документів цифрової трансформації, інституцій з кібербезпеки, нормативно-правова база щодо захисту даних (зокрема GDPR), а також стимулювання розвитку національних технологічних екосистем.

Оцінка стану інституційного забезпечення цифрового суверенітету в Україні показала наявність низки суттєвих викликів, серед яких: фрагментарність нормативно-правового поля, слабка координація між інституціями, висока залежність від іноземних технологій, а також недостатнє фінансування у сфері цифрової безпеки. Водночас Україна демонструє поступове наближення до європейських стандартів, зокрема шляхом створення цифрових державних сервісів, розвитку системи кіберзахисту, а також інтеграції до європейських ініціатив у сфері цифрової безпеки.

У рамках дослідження запропоновано адаптувати до українських реалій низку ефективних європейських практик. Серед них: розробка комплексної національної стратегії цифрового суверенітету, гармонізація нормативно-правового забезпечення із законодавством ЄС, створення центрів цифрової автономії, підтримка національних виробників критичних технологій та посилення міжвідомчої координації. Реалізація цих заходів сприятиме підвищенню спроможності України у сфері захисту цифрових інтересів, зменшенню зовнішніх залежностей і формуванню сталого цифрового середовища.

Перспективи подальших досліджень полягають у більш глибокому аналізі механізмів реалізації цифрового суверенітету в конкретних секторах (енергетика, транспорт, охорона здоров'я), вивченні впливу міжнародного права на формування національних цифрових політик, а також в оцінюванні ефективності вже впроваджених заходів на основі емпіричних даних. Окрему увагу варто приділити порівняльному аналізу моделей цифрового суверенітету в країнах Центрально-Східної Європи, що мають спільний історичний і політичний досвід із Україною, що дозволить адаптувати успішні інституційні рішення до національного контексту.

Література

1. Калайда Ю.П. Забезпечення цифрового суверенітету в умовах геополітичного протистояння: кращі практики зарубіжного досвіду. *Інформація і право*. 2021. Вип. 2(37). С. 145–154. URL: <http://il.ippi.org.ua/article/view/238363> (дата звернення: 01.05.2025).
2. Доронін І.М. Правові проблеми суверенізації Інтернету. *Інформація і право*. 2019. Вип. 2(29). С. 74–81. [https://doi.org/10.37750/2616-6798.2019.2\(29\).249380](https://doi.org/10.37750/2616-6798.2019.2(29).249380).
3. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. Вип. 1(32). С. 80–87. [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311).
4. Гнатюк С. Геополітичне цифрове візонерство США та ЄС: цифрова солідарність, цифровий суверенітет і нова американська стратегія розвитку міжнародного кіберпростору. 06.01.2025. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/heopolitychne-tsyfrovo-vizionerstvo-ssha-ta-yes-tsyfrova?__cf_chl_tk=SHZuM5lvNOIFrbfWqjZRhumgY7iKRGHLMf0rL_ML04-1746070327-1.0.1.1-wAB0fYGy4s5_MVR5EAZ5C2TH96jPjcGPIs11ZVK2lfQ (дата звернення: 01.05.2025).

5. Милосердна І. М. Цифровий суверенітет держави: наукова риторика та реальні зміни. *Політикус*. 2024. Вип. 6. С. 154–160. <https://doi.org/10.24195/2414-9616.2024-6.23>.
6. Дубов Д. В. «Цифровий суверенітет» у сучасному світі: виклики та можливості для України. *Вісник Національної академії керівних кадрів культури і мистецтв*. 2015. Вип. 1. С. 205–209. URL: <https://journals.uran.ua/visnyknakkkim/article/download/138366/135286> (дата звернення: 01.05.2025).
7. Єфремова К. В. Забезпечення цифрового суверенітету держави в умовах індустрії 4.0. *Конституційні засади розвитку інноваційного суспільства: зб. наук. пр. за матеріалами інтернет-конференції* (м. Харків, 25 червня 2021 року) / за ред. А. В. Стріжкової. Харків : НДІ ПЗІР НАПрН України, 2021. С. 25–30. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/f981db39-23a5-470f-bf25-e1af2f3701dc/content> (дата звернення: 01.05.2025).
8. Barrinha A., Christou G. Speaking sovereignty: The EU in the cyber domain. *European Security*. 2022. Vol. 31(3) P. 356–376. <https://doi.org/10.1080/09662839.2022.2102895>.
9. Bellanova R., Carrapico H., Duez, D. Digital sovereignty and European security integration: An introduction. *European Security*. 2022. Vol. 31(3). P. 337–355. <https://doi.org/10.1080/09662839.2022.2101887>.
10. Crespi F., Caravella S., Menghini M., Salvatori Ch. European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*. 2021. Vol. 56(6). P. 348–354. URL: <https://www.intereconomics.eu/contents/year/2021/number/6/article/europeantechnological-sovereignty-an-emerging-framework-forpolicy-strategy.html> (дата звернення: 01.05.2025).
11. Про основні засади забезпечення кібербезпеки України : Закон України № 2163-VIII від 5 жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 01.05.2025).
12. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 7 березня 2025 р. № 204-р. URL: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80>. (дата звернення: 01.05.2025).
13. Казанцев Д. Кібербезпека під час війни: виклики, тренди, стартапи. *Українська правда*. 20.03.2025. URL: <https://mezha.media/articles/vid-diversiy-do-shpigunstva-vikliki-ta-trendi-kiberviyni-300559/amp/> (дата звернення: 01.05.2025).

References

1. Kalaida, Yu. P. (2021). Zabezpechennia tsyfrovoho suverenitetu v umovakh heopolitychnoho protyborstva: krashchi praktyky zarubizhnogo dosvidu [Ensuring digital sovereignty under geopolitical confrontation: Best foreign practices]. *Informatsiia i pravo — Information and Law*, (2)37, 145–154. <http://il.ippi.org.ua/article/view/238363> [in Ukrainian].
2. Doronin, I. M. (2019). Pravovi problemy suverenizatsii Internetu [Legal problems of Internet sovereignization]. *Informatsiia i pravo — Information and Law*, (2)29, 74–81. [https://doi.org/10.37750/2616-6798.2019.2\(29\).249380](https://doi.org/10.37750/2616-6798.2019.2(29).249380) [in Ukrainian].
3. Solodka, O. M. (2020). Zabezpechennia informatsiinoho suverenitetu derzhavy: pravovyi dyskurs [Ensuring state information sovereignty: Legal discourse]. *Informatsiia i pravo — Information and Law*, (1)32, 80–87. [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311) [in Ukrainian].
4. Hnatiuk, S. (2025, January 6). Heopolitychne tsyfrovoe viziunerstvo SSHA ta YeS: tsyfrova solidarist, tsyfrovyy suverenitet i nova amerykanska stratehiia rozvytku mizhnarodnoho kiberprostoru [Geopolitical digital vision of the USA and EU: Digital solidarity, digital sovereignty, and the new American strategy for international cyberspace development]. <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/heopolitychne-tyfrove-vizionerstvo-ssha-ta-yes-tyfrova> [in Ukrainian].
5. Myloserdna, I. M. (2024). Tsyfrovyy suverenitet derzhavy: naukova rytoryka ta realni zminy [State digital sovereignty: Scientific rhetoric and real changes]. *Politykus — Politykus Academic Journal*, (6), 154–160. <https://doi.org/10.24195/2414-9616.2024-6.23> [in Ukrainian].
6. Dubov, D. V. (2015). «Tsyfrovyy suverenitet» u suchasnomu sviti: vyklyky ta mozhlyvosti dlia Ukrainy [«Digital sovereignty» in the modern world: Challenges and opportunities for Ukraine]. *Visnyk Natsionalnoi akademii kerivnykh kadrov kultury i mystetstv — Bulletin of the National Academy of Culture and Arts Leadership*, (1), 205–209. <https://journals.uran.ua/visnyknakkkim/article/download/138366/135286> [in Ukrainian].
7. Yefremova, K. V. (2021). Zabezpechennia tsyfrovoho suverenitetu derzhavy v umovakh industrii 4.0 [Ensuring digital sovereignty of the state under Industry 4.0]. In A. V. Strizhkova (Ed.), *Konstitutsiini zasady rozvytku innovatsiinoho suspilstva — Constitutional Principles of Innovation Society Development* (pp. 25–30). Kharkiv: NDI PZIR NAPrN Ukrainy. <https://openarchive.nure.ua/server/api/core/bitstreams/f981db39-23a5-470f-bf25-e1af2f3701dc/content> [in Ukrainian].
8. Barrinha, A., & Christou, G. (2022). Speaking sovereignty: The EU in the cyber domain. *European Security*, 31(3), 356–376. <https://doi.org/10.1080/09662839.2022.2102895> [in English].
9. Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital sovereignty and European security integration: An introduction. *European Security*, 31(3), 337–355. <https://doi.org/10.1080/09662839.2022.2101887> [in English].
10. Crespi, F., Caravella, S., Menghini, M., & Salvatori, Ch. (2021). European technological sovereignty: An emerging framework for policy strategy. *Intereconomics*, 56(6), 348–354. <https://www.intereconomics.eu/contents/year/2021/number/6/article/europeantechnological-sovereignty-an-emerging-framework-forpolicy-strategy.html> [in English].

11. Verkhovna Rada Ukrainy. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy № 2163-VIII vid 5 zhovtnia 2017 roku* [On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017]. <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].

12. Kabinet Ministriv Ukrainy. (2025). *Pro zatverdzhennia planu zakhodiv na 2025 rik z realizatsii Stratehii kiberbezpeky Ukrainy: Rozporiadzhennia KМУ vid 7 bereznia 2025 r. № 204-r* [On approval of the 2025 action plan for implementing the Cybersecurity Strategy of Ukraine: Order of the CMU No. 204-r dated March 7, 2025]. <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80> [in Ukrainian].

13. Kazantsev, D. (2025, March 20). Kiberbezpeka pid chas viiny: vyklyky, trendy, startapy [Cybersecurity during war: Challenges, trends, startups]. *Ukrainska Pravda — Ukrainian Truth*. <https://mezha.media/articles/vid-diversiy-doshpigunstva-vikliki-ta-trendi-kiberviyni-300559/amp/> [in Ukrainian].

Стаття надійшла до редакції 06.05.2025

УДК 35.07:004.8:351.746(477)

Прокопчук Ілля Петрович

*аспірант кафедри державного управління і місцевого самоврядування
факультету міжнародних економічних відносин, управління і бізнесу
Херсонського національного технічного університету*

Prokopchuk Illia

*Postgraduate Student of the
Department of State Administration and Local Self-Government
Faculty of International Economic Relations, Management and Business
Kherson National Technical University
ORCID: 0000-0002-9172-4383*

Вознюк Наталія Іванівна

*старший викладач кафедри цивільно-правових дисциплін
юридичний факультет
Волинський національний університет імені Лесі Українки*

Vozniuk Nataliia

*Senior Lecturer of the Department of Civil Law Disciplines
Faculty of Law
Lesya Ukrainka Volyn National University
ORCID: 0000-0002-6705-0497*

Супруненко Світлана Анатоліївна

*кандидат економічних наук, доцент,
проректор з науково-педагогічної та виховної роботи,
доцент кафедри менеджменту, маркетингу та публічного управління
Національна академія статистики, обліку та аудиту*

Suprunenko Svitlana

*PhD in Economics, Associate Professor,
Vice-Rector for Scientific, Pedagogical and Educational Work,
Associate Professor of the Department of Management, Marketing and Public Administration
National Academy of Statistics, Accounting and Auditing
ORCID: 0000-0002-4585-3440*

DOI: 10.25313/2617-572X-2025-5-11016

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОПТИМІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ У ПЕРІОД ПІСЛЯВОЄННОГО ВІДНОВЛЕННЯ

USING ARTIFICIAL INTELLIGENCE TO OPTIMIZE PUBLIC ADMINISTRATION IN UKRAINE DURING THE POST-WAR RECOVERY PERIOD

Анотація. Вступ. Післявоєнне відновлення є важливим етапом для будь-якої країни, яка зазнала значних руйнувань через війну. Для України, яка після початку повномасштабного вторгнення Росії пережила важкі випробування, завдання відновлення національної інфраструктури, економіки та суспільних інститутів набуває стратегічного значення. В умовах обмежених ресурсів, високих ризиків та необхідності швидкої адаптації до нових реалій, важливу роль у досягненні ефективності та стабільності віграє оптимізація публічного управління.

Одним із ефективних інструментів для цього є використання технологій штучного інтелекту (ШІ), що вже набули популярності у багатьох країнах світу. В Україні ШІ здатен сприяти не лише підвищенню ефективності адміністративних процесів, але й забезпеченню прозорості, підвищенню якості державних послуг, а також інтеграції інноваційних рішень у розбудову інфраструктури та системи управління.

Мета. Метою дослідження є обґрунтування теоретичних та прикладних засад використання технологій ШІ у системі публічного управління України в умовах післявоєнного відновлення, з урахуванням потреб оптимізації управлінських процесів, підвищення прозорості та ефективності державного управління.

Матеріали і методи. Матеріалами дослідження є праці вітчизняних та зарубіжних авторів, які досліджують застосування штучного інтелекту в публічному управлінні, цифровізацію державних процесів, з урахуванням особливостей післявоєнного відновлення суспільства.

У процесі дослідження було використано наукові методи: теоретичного узагальнення та групування (для систематизації підходів до використання ШІ у сфері публічного управління та визначення основних напрямів його впровадження у післявоєнний період); формалізації, аналізу та синтезу (для структурування наукових поглядів, визначення зв'язків між цифровими технологіями та інструментами державного управління); логічного узагальнення результатів (для формулювання висновків щодо потенціалу і ризиків використання ШІ у сфері публічного адміністрування в умовах післявоєнного відновлення України).

Результати. У науковій статті окреслено ключові напрями застосування ШІ у системі публічного управління: автоматизація адміністративних процедур, прогнозування і відновлення інфраструктури, покращення публічного управління інформаційною безпекою, системи для боротьби з корупцією. Визначено та проаналізовано основні виклики, зокрема, застарілу інфраструктуру, низький рівень кваліфікації кадрів, недовіру громадян до цифрових послуг та фінансові обмеження. Запропоновано комплексний підхід до впровадження цифрових технологій, що включає модернізацію технічної інфраструктури, підвищення професійної підготовки працівників, розробку стандартів кібербезпеки та створення єдиної стратегії цифровізації.

Перспективи. У подальших дослідженнях пропонується зосередити увагу на комплексному вивченні можливостей застосування ШІ у публічному управлінні, з урахуванням національних особливостей та міжнародного досвіду.

Ключові слова: публічне управління, штучний інтелект, цифрова трансформація, етика, прозорість, великі дані, цифрове врядування, компетентність, кібербезпека.

Summary. Introduction. Post-war recovery is an important stage for any country that has suffered significant destruction as a result of war. For Ukraine, which has endured severe trials since the start of Russia's full-scale invasion, the task of rebuilding its national infrastructure, economy and social institutions is of strategic importance. In a context of limited resources, high risks and the need for rapid adaptation to new realities, optimising public administration plays an important role in achieving efficiency and stability.

One effective tool for this is the use of artificial intelligence (AI) technologies, which have already gained popularity in many countries around the world. In Ukraine, AI can contribute not only to improving the efficiency of administrative processes, but also to ensuring transparency, improving the quality of public services, and integrating innovative solutions into the development of infrastructure and management systems.

Purpose. The purpose of the study is to substantiate the theoretical and applied foundations for the use of AI technologies in the public administration system of Ukraine in the context of post-war recovery, taking into account the needs for optimising management processes and increasing the transparency and efficiency of public administration.

Materials and methods. The research materials include works by domestic and foreign authors who study the application of artificial intelligence in public administration and the digitisation of state processes, taking into account the peculiarities of post-war recovery of society.

The following scientific methods were used in the research: theoretical generalisation and grouping (to systematise approaches to the use of AI in public administration and identify the main directions for its implementation in the post-war period); formalisation, analysis and synthesis (to structure scientific views and identify links between digital technologies and public administration tools); logical generalisation of results (to formulate conclusions on the potential and risks of using AI in public administration in the context of Ukraine's post-war recovery).

Results. The scientific article outlines the key areas of AI application in public administration: automation of administrative procedures, infrastructure forecasting and restoration, improvement of public information security management, and anti-corruption systems. The main challenges have been identified and analysed, in particular outdated infrastructure, low staff qualifications, public mistrust of digital services and financial constraints. A comprehensive approach to the implementation of digital technologies is proposed, including the modernisation of technical infrastructure, improving the professional training of employees, developing cybersecurity standards, and creating a unified digitalisation strategy.

Prospects. Further research should focus on a comprehensive study of the possibilities of applying AI in public administration, taking into account national characteristics and international experience.

Key words: public administration, artificial intelligence, digital transformation, ethics, transparency, big data, digital governance, competence, cybersecurity.

Постановка проблеми. Післявоєнний період для України стане важливим етапом не лише у відновленні інфраструктури, а й у глибокій трансформації публічного управління, яке охоплює як державне, так і муніципальне врядування, а також взаємодію з громадянським суспільством. Одним із ключових інструментів для модернізації та забезпечення ефективного управління є впровадження новітніх технологій, зокрема штучного інтелекту. ШІ спроможний значно підвищити ефективність роботи публічних органів, сприяючи не лише оптимізації адміністративних процесів, але й покращенню якості надання послуг громадянам, підвищенню прозорості та скороченню витрат. Враховуючи актуальність та потенціал таких технологій, Україна стоїть перед необхідністю створення ефективної стратегії використання штучного інтелекту для підтримки сталого розвитку в умовах післявоєнного відновлення. Цей процес є одним із ключових елементів модернізації публічного управління, що допоможе країні не лише відновитися, а й стати більш конкурентоспроможною на світовій арені.

Аналіз останніх досліджень і публікацій. Значний внесок у формування базових положень та теоретичних засад щодо впровадження ШІ у систему публічного управління зробили багато дослідників цього питання. Так, Н. Василенко [2] акцентує увагу на ролі публічного управління в умовах післявоєнного відновлення, де цифровізація, зокрема, впровадження інтелектуальних технологій, розглядається як один із ключових чинників модернізації управлінської системи. С. Домашенко [5] визначає напрями практичного використання технологій ШІ у сфері публічного адміністрування, зокрема, через автоматизацію управлінських функцій. Перспективи впровадження ШІ у системі публічного управління, виокремлюючи ризики та виклики, пов'язані з цифровою трансформацією розглядає й Л. Корнута [9]. Т. Яровой [13] також аналізує як позитивні, так і негативні наслідки використання ШІ у публічному секторі, наголошуючи на важливості балансування між ефективністю та етикою. У роботі Н. Максименцевої та М. Максименцева [10] обґрунтовано як переваги цифрових технологій, так і загрози, що постають перед інформаційним суверенітетом держави в умовах активного впровадження ШІ. О. Дегтяр, С. Безносенко та О. Білий [3] аналізують застосування ШІ у контексті інформаційної безпеки та кіберзахисту, підкреслюючи важливість міжгалузевої взаємодії у системі державного управління. М. Думчиков [6] досліджує потенціал генеративних моделей ШІ у виявленні та протидії корупційним проявам, акцентуючи увагу на їх аналітичній здатності. С. Квітка, Н. Новіченко та О. Бардах [7] розглядають вектори розвитку ШІ на рівні місцевого самоврядування, підкреслюючи роль технологій у підвищенні ефективності муніципального управління.

Водночас враховуючи значну кількість праць, що стосуються загальних питань цифровізації, трансформації публічного управління та впровадження інноваційних технологій, проблематика використання ШІ для оптимізації публічного управління в Україні в період післявоєнного відновлення досі залишається недостатньо дослідженою. Наукові підходи переважно орієнтовані на окремі аспекти цифрового врядування, не враховуючи повною мірою специфіку кризового та посткризового контексту, в якому перебуває українська державність після початку повномасштабної збройної агресії Росії.

Актуальність цього дослідження зумовлена потребою не лише у підвищенні ефективності та прозорості публічного управління, а й у створенні гнучких, адаптивних, технологічно підкріплених механізмів, які б сприяли швидкому та якісному відновленню країни. ШІ може виступати важливим інструментом для прийняття рішень на основі великих масивів даних, автоматизації процесів, прогнозування ризиків і оптимізації розподілу ресурсів, що набуває особливого значення в умовах післявоєнної реконструкції.

Метою статті є обґрунтування теоретичних та прикладних засад використання технологій ШІ у системі публічного управління України в умовах післявоєнного відновлення, з урахуванням потреб оптимізації управлінських процесів, підвищення прозорості та ефективності публічного управління.

Матеріали та методи дослідження. Джерельною базою дослідження слугували наукові праці вітчизняних і зарубіжних учених, присвячені проблемам застосування штучного інтелекту в публічному управлінні та цифровізації державних процесів, з урахуванням специфіки післявоєнного відновлення суспільства. У процесі дослідження було застосовано комплекс загальнонаукових методів: узагальнення — для систематизації концептуальних підходів до використання ШІ у сфері публічного управління та визначення пріоритетних напрямів його імплементації в післявоєнний період; для формулювання висновків щодо потенційних переваг та ризиків використання ШІ у сфері публічного адміністрування в контексті післявоєнного відновлення України; формалізації, аналізу та синтезу — для структурування наукових поглядів, виявлення кореляційних зв'язків між цифровими технологіями та інструментами публічного управління.

Виклад основного матеріалу. Публічне управління зазнає впливу багатьох тенденцій і чинників, що формуються під впливом суспільних змін. Серед ключових — трансформації у зовнішньому середовищі, зокрема, глобалізаційні процеси та перехід до інформаційного етапу розвитку суспільства. Додатковим вагомих викликом є воєнні дії, які суттєво змінюють контекст управлінських рішень. У зв'язку з цим виникає необхідність у впровадженні інноваційних підходів і засобів управління, які б відповідали сучасним вимогам [9, с. 38].

Одним з інструментів оптимізації державного управління є штучний інтелект, який набуває особливої популярності. Це обумовлено його здатністю автоматизувати рутинні процеси, що дозволяє ефективніше використовувати ресурси, знижувати фінансові витрати та покращувати якість прийняття рішень [5, с. 58].

Згідно з Концепцією розвитку штучного інтелекту в Україні, ухваленою у грудні 2020 року, штучний інтелект розглядається як «організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень та алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [8].

Штучний інтелект — це сучасний інструмент цифрових технологій, який моделює когнітивні функції, зокрема здатність аналізувати інформацію, приймати рішення, навчатися на основі досвіду та адаптуватися до нових умов. Він є сукупністю алгоритмів, моделей і технічних рішень, що дозволяють автоматизувати складні процеси, підвищувати ефективність управлінських рішень і забезпечувати інноваційний розвиток у різних сферах, включно з публічним управлінням, що в успішних країнах поєднується з пріоритетом на розвиток людських ресурсів та людського капіталу високих технологій [18].

Технології ШІ, як і інші проривні цифрові інновації — зокрема розподілений реєстр, великі дані тощо — відіграють ключову роль у процесі цифрової трансформації суспільства. Їх головне призначення полягає в підвищенні загального добробуту, що охоплює як покращення соціально-економічних умов, так і полегшення щоденних людських обов'язків, шляхом автоматизації рутинних процесів. Ці технології, які спочатку активно розвивалися у приватному секторі (наприклад, у сферах управління персоналом, аналітики, прийняття рішень, підготовки складної звітності), поступово знаходять своє застосування й у сфері публічного управління, сприяючи її модернізації та підвищенню ефективності [12, с. 127].

Сьогодні питання впровадження ШІ у сферу публічного управління набуває особливої важливості з огляду на стратегічні пріоритети цифрової трансформації в Україні. І держава, і громадськість усвідомлюють потребу в інтенсивному розвитку ШІ та цифрових технологій не лише в бізнес-середовищі, а й у системі публічного управління. Розбудова цифрової економіки має сприяти зростанню ефективності функціонування державних інституцій і підвищенню якості життя населення. У цьому контексті важливо проаналізувати складові ШІ, які можуть бути корисними для реалізації нової державної Програми та Стратегії розвитку ШІ в Україні [9, с. 38].

Війна загострила необхідність формування цілісної системи публічного управління, яка поєднує державне управління, місцеве самоврядування та громадський сектор на всіх рівнях ієрархії. Основним викликом повоєнного періоду є створення ефективного механізму управління, здатного враховувати геополітичні ризики, відповідати європейським стандартам та адаптуватися до національних реалій. Це є важливою передумовою для відновлення, модернізації та сталого розвитку країни за принципом «відбудувати краще, ніж було» [2, с. 34].

Використання ШІ для оптимізації публічного управління в Україні у період післявоєнного відновлення має значний потенціал для підвищення ефективності державних процесів, покращення прозорості та забезпечення більш швидкої адаптації до змінних умов. Серед ключових напрямків, де ШІ може відіграти важливу роль, зазначимо наступні:

1. Автоматизація державних послуг.

Програмні рішення на основі ШІ мають потенціал значно підвищити ефективність та якість надання адміністративних послуг, а також сприяти більш обґрунтованому прийняттю урядових рішень. Це можливо завдяки здатності таких систем моделювати й аналізувати різні сценарії політики, що забезпечує гнучкість і прогнозованість у реалізації функцій публічного управління [10].

Науковці підкреслюють потенціал використання технологій ШІ для вдосконалення політики шляхом надання держслужбовцям додаткової інформації, отриманої з аналізу великих масивів даних [19], автоматизації рутинних завдань і процесів [15], покращення якості інформації для громадян, персоналізації послуг, а також глибшого розуміння потреб і настроїв населення, зокрема, через аналіз даних із соціальних мереж.

Прикладом успішної автоматизації державних послуг є портал Дія. У 2024 році до Положення про Єдиний державний вебпортал електронних послуг [4] було внесено зміни, які передбачають можливість використання технологій ШІ для надання інформаційної підтримки користувачам порталу. Такі новації дозволять покращити якість обслуговування та підвищити ефективність надання державних послуг громадянам, зокрема через персоналізацію.

Також можна відзначити ініціативу Міністерства цифрової трансформації України, яке запустило WINWIN AI Center of Excellence — центр передового досвіду з розробки та інтеграції ШІ, що має на меті створення інноваційних рішень для вдосконалення державних послуг [11].

Деякі IT-директори наголошують, що інтеграція ШІ у діяльність органів державної влади має багато спільного із застосуванням цих технологій у приватному секторі [14], і труднощі в отриманні переваг від інновацій є подібними [17]. Водночас інші дослідники звертають увагу на суттєві відмінності: зокрема, державний сектор має орієнтуватися

не на комерційну, а на суспільну цінність. Також існують специфічні бар'єри — інституційні, ресурсні та організаційні — що уповільнюють впровадження ІІІ на публічній службі.

Окрім того, державний сектор стикається з підвищеними очікуваннями громадян і жорсткішими вимогами до прозорості як у функціонуванні ІІІ-систем, так і щодо відкритості інформації про використання бюджетних коштів. Це зумовлює специфічні підходи до впровадження ІІІ у сфері надання публічних послуг та адміністрування, що відрізняються від корпоративного досвіду.

Отже, хоча деякі труднощі у застосуванні інноваційних технологій є спільними для обох секторів, особливості функціонування державних інституцій вимагають адаптації підходів, які довели ефективність у бізнес-середовищі.

Для ефективного використання ІІІ у публічному управлінні була розроблена концепція «можливостей штучного інтелекту», яка покликана визначити які ресурси слід розвивати в організаціях, аби досягти очікуваного ефекту. Попри високі очікування, багато інституцій стикаються з труднощами в досягненні приросту продуктивності. Ця концепція ґрунтується на ресурсній теорії (RBV — Resource-Based View), теорії інноваційного потенціалу та моделі «Технологія — Організація — Середовище» (TOE — Technology-Organisation-Environment) [10].

З точки зору ресурсного підходу, ефективність інновацій залежить від взаємодії технологічних активів із внутрішніми організаційними можливостями. Така інноваційна спроможність — здатність організації виявляти, тестувати, інтегрувати та впроваджувати новачки — є ключовим чинником створення суспільної цінності у державному секторі. Саме ці організаційні чинники пояснюють нерівномірність прогресу електронного урядування в різних інституціях, навіть попри наявність технологічних засобів.

Отже, ІІІ може автоматизувати багато адміністративних процесів, таких як подання та обробка заяв, ліцензування, реєстрація підприємств, призначення й верифікація соціальних виплат тощо. Це дозволить зменшити бюрократичні бар'єри, скоротити час обробки запитів і зменшити рівень корупції завдяки прозорим і автоматизованим процесам.

2. Прогнозування і відновлення інфраструктури.

ІІІ може бути використаний для прогнозування потреб у відновленні інфраструктури, визначення пріоритетних напрямків відбудови. Використовуючи дані про стан доріг, будівель та інших важливих об'єктів, алгоритми можуть створювати точні карти пошкоджень і допомагати у формуванні стратегій відновлення.

ІІІ дозволяє оптимізувати розподіл ресурсів для їх ефективного використання, а також має здатність аналізувати новини, соціальні мережі та інші джерела інформації для прогнозування кризових ситуацій [13].

Прикладом є розробка інтерактивної карти пошкоджень у рамках ініціативи RebuildUA, яка використовує супутникові знімки, машинне навчання та відкриті дані для оцінки руйнувань у регіонах України [16].

3. Покращення публічного управління інформаційною безпекою.

Механізми публічного управління інформаційною безпекою — це складене поєднання організаційних, правових, технологічних та соціальних заходів, що забезпечують захист інформаційних ресурсів від зовнішніх та внутрішніх загроз. В умовах сучасного світу, де цифрові технології відіграють центральну роль, інформаційна безпека стає однією з ключових складових державної політики у галузі безпеки. Важливою складовою цього процесу є впровадження передових цифрових технологій, що значно покращують ефективність управлінських процесів, зменшують ризики та забезпечують оперативну реакцію на кіберзагрози. Основним елементом механізмів публічного управління інформаційною безпекою є розробка національної політики у сфері кібербезпеки, яка визначає стратегію та пріоритети у захисті інформаційних ресурсів [3, с. 555].

4. Системи для боротьби з корупцією.

Інтеграція штучного інтелекту (ІІІ) у боротьбу з корупцією в Україні є ефективною у виявленні та запобіганні корупційним правопорушенням. ІІІ може аналізувати великі обсяги даних у реальному часі, виявляючи аномалії та потенційні корупційні ризики, зокрема, через алгоритми машинного навчання. Прикладом є система Dozorro, яка моніторить публічні закупівлі через платформу ProZorro, дозволяючи виявляти підозрілі тендери за допомогою аналізу коментарів користувачів і даних про попередні закупівлі.

Автоматизація процесів, таких як перевірка декларацій, дозволяє підвищити прозорість діяльності антикорупційних органів і зменшити вплив людського фактора. Окрім того, інтеграція ІІІ з блокчейн-технологіями забезпечить доступність та незмінність даних, що посилить громадський контроль і сприятиме створенню прозорого механізму боротьби з корупцією [6, с. 140]. Це все дає можливість збільшити прозорість та попередити недоброчесні дії [13].

Узагальнюючи, можна стверджувати, що поступово приходить усвідомлення того, що ми вступаємо у цифрову епоху, важливим елементом якої стає розвиток і активне використання технологій ІІІ у публічному управлінні, зокрема, у стратегічному плануванні та оперативному управлінні економічним розвитком під час реалізації «цифрової економіки» в країні [7, с. 92].

ІІІ має значний потенціал для трансформації публічного управління в Україні у період післявоєнного відновлення, забезпечуючи швидке, прозоре і ефективне управління ресурсами, інфраструктурою та людським потенціалом. Водночас важливо

Таблиця 1

Виклики інтеграції штучного інтелекту в публічне управління

№	Виклик	Опис
1	Застаріла інфраструктура	Більшість державних органів мають технічно застарілі системи, які не підтримують технології ШІ.
2	Низький рівень кваліфікації кадрів	Відсутність у працівників необхідних знань і навичок для роботи з ШІ та розуміння етичних аспектів його використання.
3	Недовіра громадян до цифрових послуг	Скептичне ставлення населення через побоювання щодо захисту даних і приватності.
4	Фінансові обмеження	Брак ресурсів на закупівлю технологій, навчання персоналу та оновлення систем.
5	Відсутність належного правового регулювання	Чинними нормативними актами врегульовано окремі аспекти впровадження та використання ШІ. Імплементація європейських стандартів і розробка спеціального закону перебувають на стадії формування

Джерело: складено автором за [3]

забезпечити етичні стандарти у використанні ШІ та належний рівень захисту даних, щоб уникнути можливих ризиків.

Водночас інтеграція ШІ в публічне управління стикається з низкою викликів (табл. 1).

Впровадження цифрових технологій у систему публічного управління України вимагає комплексного підходу, що включає в себе:

- модернізацію технічної інфраструктури;
- підвищення професійної підготовки працівників;
- розробку стандартів кібербезпеки;
- створення єдиної стратегії цифровізації та належної законодавчої бази [3].

Тільки за дотримання цих умов можливе ефективне впровадження цифрових рішень, що підвищуватимуть якість та доступність публічних послуг.

Висновки і перспективи подальших досліджень. Отже, у сучасних умовах публічне управління переживає масштабну трансформацію під впливом глобалізації, цифровізації та воєнних дій,

що вже не один рік тривають в Україні. Виклики сьогодення зумовлюють потребу в пошуку нових, ефективніших управлінських рішень, які відповідають вимогам часу. Штучний інтелект є одним із дієвих інструментів цифрової трансформації, здатним покращити якість публічного управління шляхом автоматизації процесів, підвищення прозорості та адаптивності до змін.

У повоєнний період особливої актуальності набуває використання ШІ для управління відбудовою, прогнозування потреб громад та забезпечення стійкого розвитку. Доцільно розвинути та поширити подібні ініціативи в усіх рівнях публічного управління, інтегруючи ШІ в аналітику, прийняття рішень і зворотний зв'язок із громадянами.

У подальших наукових дослідженнях пропонується зосередити увагу на комплексному вивченні можливостей застосування ШІ в публічному управлінні, з урахуванням національних особливостей та міжнародного досвіду.

Література

1. Баранівська М. МЗС презентувало цифрову особу Вікторію ШІ, яка офіційно коментуватиме консульську інформацію для преси. *Детектор Медіа*. 01 травня 2024 року. URL: <https://detector.media/infospace/article/226186/2024-05-01-mzs-prezentovalo-tsyfrovu-osobu-viktoriyu-shi-yaka-ofitsiyno-komentuvatyme-konsulsku-informatsiyu-dlya-presy/> (дата звернення: 03.05.2025).

2. Василенко Н. В. Публічне управління в умовах післявоєнного відновлення в Україні. *Наукові інновації та передові технології*. 2025. № 1(41). С. 28–35. [https://doi.org/10.52058/2786-5274-2025-1\(41\)-28-35](https://doi.org/10.52058/2786-5274-2025-1(41)-28-35).

3. Дегтяр О. А., Безносенко С. Ю., Білий О. А. Розвиток штучного інтелекту в системі публічного управління інформаційної безпеки. *Суспільство та національні інтереси*. 2025. № 2. С. 549–560. URL: http://nbuv.gov.ua/UJRN/scntint_2025_2_49 (дата звернення: 28.04.2025).

4. Положення про Єдиний державний вебпортал електронних послуг: затв. постановою Кабінету Міністрів України від 4 грудня 2019 р. № 1137. URL: <https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text> (дата звернення: 04.05.2025).

5. Домашенко С. Штучний інтелект у публічному управлінні. *ЛОГОС*. 2024. С. 58–60. <https://doi.org/10.36074/logos-19.07.2024.010>.

6. Думчиков М. О. Роль та перспективи використання генеративних систем штучного інтелекту у боротьбі з корупцією. *Наукові записки Львівського університету бізнесу та права*. 2024. Вип. 42. С. 138–143. URL: <https://nzlubp.org.ua/index.php/journal/article/download/1385/1230> (дата звернення: 27.04.2025).

7. Квітка С., Новіченко Н., Бардах О. Штучний інтелект у муніципальному управлінні: вектори розвитку. *Аспекти публічного управління*. 2021. № 9(4). С. 85–94. <https://doi.org/10.15421/152140>.
8. Концепція розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 27.04.2025).
9. Корнута Л. М. Штучний інтелект у публічному управлінні: перспективи впровадження. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень: у 2 т.: матеріали Міжнар. наук.-практ. конф.* (м. Одеса, 19 травня 2023 р.) / за заг. ред. С. В. Ківалова. Одеса: Видавництво «Юридика», 2023. Т. 2. С. 37–39. URL: <https://hdl.handle.net/11300/25938> (дата звернення: 27.04.2025).
10. Максименцева Н. О., Максименцев М. Г. Штучний інтелект у публічному управлінні: переваги цифрових технологій та загрози суверенному інформативному простору. *Державне управління: удосконалення та розвиток*. 2024. № 2. <http://doi.org/10.32702/2307-2156.2024.2.7>.
11. Мінцифра запускає WINWIN AI Center of Excellence — центр передового досвіду з розробки та інтеграції ІІІ. URL: <https://thedigital.gov.ua/news/mintsifra-zapuskae-winwin-ai-center-of-excellence-tsentr-peredovogo-dosvidu-z-rozrobki-ta-integratsii-shi> (дата звернення: 04.05.2025).
12. Пархоменко-Кущевіч О. Теоретичні засади застосування штучного інтелекту в системі публічного управління як основа транспарентності. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2025. № 11. С. 126–135. <https://doi.org/10.31470/2786-6246-2025-11-126-135>.
13. Яровой Т. С. Возможности та риски использования штучного интеллекта в публичном управлении. *Economic Synergy*. 2024. № 2. С. 36–47. <https://doi.org/10.53920/es-2023-2-3>.
14. Criado J. I., Ode Zarate-Alcarazo L. Technological frames, CIOs, and artificial intelligence in public administration: A socio-cognitive exploratory study in Spanish local governments. *Government Information Quarterly*. 2022. № 39(3). <https://doi.org/10.1016/j.giq.2022.101688>.
15. Ranerup A., Henriksen H. Z. Digital discretion: Unpacking human and technological Agency in Automated Decision Making in Sweden's social services. *Social Science Computer Review*. 2022. № 40(2). PP. 445–461. URL: https://www.researchgate.net/publication/347674724_Digital_Discretion_Unpacking_Human_and_Technological_Agency_in_Automated_Decision_Making_in_Sweden's_Social_Services (дата звернення: 28.04.2025).
16. RebuildU A. URL: <https://rebuildua.net/> (дата звернення: 04.05.2025).
17. Shollo A., Hopf K., Thiess T., Müller O. Shifting ML value creation mechanisms: A process model of ML value creation. *Journal of Strategic Information Systems*. 2022. № 31(3). <https://doi.org/10.1016/j.jsis.2022.101734>.
18. Sidorova E., Dniprov O., Yunina M., Bobrishova L., Mkrtchian K. Administrative and legal principles of public control over the implementation of state policy in the humanitarian sphere. *Amazonia Investiga*. 2022. № 11(56). PP. 124–131. <https://doi.org/10.34069/AI/2022.56.08.13>.
19. Veale M., Brass I. Administration by algorithm? Public management meets public sector machine learning. *Algorithmic Regulation* (Karen Yeung and Martin Lodge eds., Oxford University Press). 2019. <https://doi.org/10.31235/OSF.IO/MWHNB>.

References

1. Baranivska, M. (2024, May 1). *MZS prezentovalo tsyfrovu osobu Viktoriia SHI, iaka ofitsiino komentuvatyme konsulsku informatsiiu dlia presy* [The MFA presented the digital person Viktoriia AI, who will officially comment on consular information for the press]. *Detector Media*. <https://detector.media/infospace/article/226186/2024-05-01-mzs-prezentovalo-tsifrovu-osobu-viktoriiu-shi-yaka-ofitsiyno-komentuvatyme-konsulsku-informatsiyu-dlya-presy/> [in Ukrainian].
2. Vasylenko, N. V. (2025). Publichne upravlinnia v umovakh pisliavoiennoho vidnovlennia v Ukraini [Public administration in the context of post-war reconstruction in Ukraine]. *Naukovi innovatsii ta peredovi tekhnologii*, (1(41)), 28–35. [https://doi.org/10.52058/2786-5274-2025-1\(41\)-28-35](https://doi.org/10.52058/2786-5274-2025-1(41)-28-35) [in Ukraine].
3. Diehtiar, O. A., Beznozenko, S. Yu., & Bilyi, O. A. (2025). Rozvytok shtuchnoho intelektu v systemi publichnoho upravlinnia informatsiinoi bezpeky [Development of artificial intelligence in the public administration system of information security]. *Suspilstvo ta natsionalni interesy*, (2), 549–560. Retrieved from http://nbuv.gov.ua/UJRN/scntint_2025_2_49 [in Ukraine].
4. Cabinet of Ministers of Ukraine. (2019). Polozhennia pro Yedynyi derzhavnyi vebportal elektronnykh posluh: zatverdzheno Postanovoiu Kabinetu Ministriv Ukrainy vid 4 hrudnia 2019 r. № 1137 [Regulation on the Unified State Web Portal of Electronic Services: approved by Resolution of the Cabinet of Ministers of Ukraine dated 4 December 2019 No. 1137]. URL: <https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text> [in Ukrainian].
5. Domashenko, S. (2024). Shtuchnyi intelekt u publichnomu upravlinni [Artificial intelligence in public administration]. *Collection of Scientific Papers "ΛΟΓΟΣ"*, 58–60. <https://doi.org/10.36074/logos-19.07.2024.010> [in Ukraine].
6. Dumchikov, M. O. (2024). Rol ta perspektyvy vykorystannia henertyvnykh system shtuchnoho intelektu u borotbi z koruptsiieiu [The role and prospects of using generative artificial intelligence systems in the fight against corruption]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava*, (42), 138–143. Retrieved from <https://nzlubp.org.ua/index.php/journal/article/download/1385/1230> [in Ukraine]

7. Kvitka, S., Novichenko, N., & Bardakh, O. (2021). Shtuchnyi intelekt u munitsypalnomu upravlinni: vektory rozvytku [Artificial intelligence in municipal management: development vectors]. *Aspekty publichnoho upravlinnia*, 9(4), 85–94. <https://doi.org/10.15421/152140> [in Ukraine].
8. Kontsepsiia rozvytku shtuchnoho intelektu v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 2 hrudnia 2020 r. № 1556-r [Concept for the development of artificial intelligence in Ukraine: Order of the Cabinet of Ministers of Ukraine dated December 2, 2020 No. 1556-r]. Retrieved from <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#-Text> [in Ukraine].
9. Kornuta, L. M. (2023). Shtuchnyi intelekt u publichnomu upravlinni: perspektyvy vprovadzhennia [Artificial intelligence in public administration: prospects for implementation]. In S. V. Kivalov (Ed.), *Yevropeiski oriientyry rozvytku Ukrainy v umovakh viiny ta hlobalnykh vyklykiv XXI stolittia: synerhiia naukovykh, osvitykh ta tekhnolohichnykh rishen: u 2 t.: materialy Mizhnar. nauk.-prakt. konf.* (Vol. 2, pp. 37–39). Vydavnytstvo “Yurydyka”. Retrieved from <https://hdl.handle.net/11300/25938> [in Ukraine].
10. Maksimetsieva, N. O., & Maksimetsiev, M. H. (2024). Shtuchnyi intelekt u publichnomu upravlinni: perevahy tsyfrovykh tekhnolohii ta zahrozy suverennomu informatyvnomu prostoru [Artificial intelligence in public administration: advantages of digital technologies and threats to the sovereign information space]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, (2). <http://doi.org/10.32702/2307-2156.2024.2.7> (Accessed 27.04.2025) [in Ukraine].
11. Ministry of Digital Transformation of Ukraine. (2024, May 3). *Mintsifra zapuskaie WINWIN AI Center of Excellence — tsentr peredovoho dosvidu z rozrobky ta intehtatsii SHI* [The Ministry of Digital Transformation launches WINWIN AI Center of Excellence — a center of excellence for AI development and integration]. <https://thedigital.gov.ua/news/mintsifra-zapuskaie-winwin-ai-center-of-excellence-tsent-peredovoho-dosvidu-z-rozrobky-ta-integratsii-shi> [in Ukrainian].
12. Parkhomenko-Kutsevil, O. (2025). Teoretychni zasady zastosuvannia shtuchnoho intelektu v systemi publichnoho upravlinnia yak osnova transparentnosti [Theoretical principles of the use of artificial intelligence in the public administration system as a basis for transparency]. *Publichne upravlinnia: kontsepsii, napaduzma, rozvytok, udoskonalennia*, (11), 126–135. <https://doi.org/10.31470/2786-6246-2025-11-126-135> [in Ukraine].
13. Yarovoi, T. S. (2024). Mozhlyvosti ta ryzyky vykorystannia shtuchnoho intelektu v publichnomu upravlinni [Opportunities and risks of using artificial intelligence in public administration]. *Economic Synergy*, (2), 36–47. <https://doi.org/10.53920/es-2023-2-3> [in Ukraine].
14. Criado, J. I., & Ode Zarate-Alcarazo, L. (2022). Technological frames, CIOs, and artificial intelligence in public administration: A socio-cognitive exploratory study in Spanish local governments. *Government Information Quarterly*, 39(3). <https://doi.org/10.1016/j.giq.2022.101688>.
15. Ranerup, A., & Henriksen, H. Z. (2022). Digital discretion: Unpacking human and technological Agency in Automated Decision Making in Sweden’s social services. *Social Science Computer Review*, 40(2), 445–461. Retrieved from https://www.researchgate.net/publication/347674724_Digital_Discretion_Unpacking_Human_and_Technological_Agency_in_Automated_Decision_Making_in_Sweden’s_Social_Services.
16. RebuildU A. *Initiative for assessing war damages using satellite imagery and AI*. <https://rebuildua.net/> [in Ukrainian].
17. Shollo, A., Hopf, K., Thiess, T., & Müller, O. (2022). Shifting ML value creation mechanisms: A process model of ML value creation. *Journal of Strategic Information Systems*, 31(3). <https://doi.org/10.1016/j.jsis.2022.101734>.
18. Sidorova, E., Dniprov, O., Yunina, M., Bobrishova, L., & Mkrtchian, K. (2022). Administrative and legal principles of public control over the implementation of state policy in the humanitarian sphere. *Amazonia Investiga*, 11(56), 124–131. <https://doi.org/10.34069/AI/2022.56.08.13>.
19. Veale, M., & Brass, I. (2019). Administration by algorithm? Public management meets public sector machine learning. In K. Yeung & M. Lodge (Eds.), *Algorithmic Regulation* (pp.). Oxford University Press. <https://doi.org/10.31235/OSF.IO/MWHNB>.

Стаття надійшла до редакції 22.05.2025

УДК 35:004.8

Франчук Володимир Сергійович

*аспірант кафедри публічного управління та адміністрування
Державного університету «Житомирська політехніка»*

Franchuk Volodymyr

PhD Student of the Department of Public Management and Administration

Zhytomyr Polytechnic State University

ORCID: 0009-0005-5439-6105

DOI: 10.25313/2617-572X-2025-5-11028

ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ: ПОТЕНЦІАЛ ТА РИЗИКИ

ARTIFICIAL INTELLIGENCE IN THE PUBLIC ADMINISTRATION SYSTEM: POTENTIAL AND RISKS

Анотація. Вступ. Штучний інтелект (ШІ) набуває дедалі більшого значення у сфері публічного управління, сприяючи вдосконаленню процесів прийняття рішень, раціоналізації використання ресурсів і підвищенню загальної ефективності управлінських механізмів. У цій статті розглядаються потенційні напрями інтеграції ШІ в систему публічного управління, а також аналізуються етичні виклики, що супроводжують його впровадження. Отримані результати акцентують на тому, що застосування ШІ може стати ключовим чинником у підвищенні прозорості, відкритості та інноваційності управлінських практик. З огляду на стрімкий розвиток цифрових технологій, порушена тематика є надзвичайно актуальною та заслуговує на особливу увагу як наукової спільноти, так і практиків у галузі державного управління. У статті досліджено потенціал та ризики інтеграції штучного інтелекту (ШІ) у систему публічного управління, зокрема в контексті сучасних викликів, з якими стикається Україна.

Мета. Метою роботи є аналіз наукових досліджень, законодавчої бази та практики використання ШІ у державному секторі та оцінка суспільних, технологічних і правових ризиків, пов'язаних із впровадженням цих технологій. А також, на основі аналізу міжнародного та вітчизняного досвіду навести рекомендації для подальшої інтеграції ШІ в сферу публічного управління.

Матеріали і методи. Методологія дослідження ґрунтується на системному підході, що поєднує аналіз наукової літератури, нормативно-правових актів і прикладів застосування ШІ. Зокрема, розглянуто ініціативи автоматизації державних послуг, впровадження машинного навчання в медицині, фінансовому секторі та адміністративних процесах. Встановлено, що ШІ значно підвищує ефективність управління через автоматизацію рутинних операцій, оптимізацію аналітики та прогнозування. Наприклад, українські проекти (мобільний додаток «Дія», системи діагностики в охороні здоров'я) демонструють зростання доступності послуг і скорочення часу їх надання.

Проте виявлено низку критичних ризиків. Соціально-економічні загрози включають упередженість алгоритмів через низьку якість даних, фінансові перевантаження бюджету та організаційні складнощі інтеграції з застарілими ІТ-системами. Технологічні ризики пов'язані зі складністю адаптації алгоритмічних рішень у різномірних умовах. Інституційні виклики охоплюють правову невизначеність, відсутність етичних стандартів і недовіру громадян до впровадження державною технологій що базуються на ШІ. Наприклад, використання закритих алгоритмів приватним сектором може підривати прозорість державних рішень.

Результати. На основі проведеного аналізу сформульовано рекомендації для мінімізації ризиків. Серед них: створення централізованого органу з координації ШІ-проектів, розробка чітких правових рамок, що регулюють прозорість алгоритмів і захист даних, та реалізація освітніх програм для держслужбовців і громадян. Зауважується, що успіх цифрової трансформації залежить від балансу між інноваціями та гарантіями безпеки. Зокрема, запропоновано інтегрувати етичні принципи (наприклад, гуманізацію технологій) у державну політику, а також забезпечити участь наукової спільноти та громадськості в аудиті ШІ-систем.

ШІ має потенціал радикально змінити традиційні моделі управління, але його впровадження вимагає комплексного підходу. Ключовою умовою такого підходу є впровадження технологічної модернізації з правовим регулюванням,

розвитком кадрового потенціалу та формуванням довіри суспільства. Така стратегія може дозволить Україні реалізувати переваги ШІ, мінімізувати ризики пов'язані з використанням технології, забезпечуючи стабільність держави в умовах глобальних викликів.

Перспективи. В подальшому дослідження буде спрямоване на оцінку ефективності алгоритмів ШІ в різномірних державних процесах, розробку етичних та правових механізмів контролю, інтеграцію інструментів машинного навчання у прийняття рішень та аналіз потенційних ризиків із метою забезпечення прозорості й безпеки, а також формування практичних рекомендацій для державних установ.

Ключові слова: штучний інтелект, публічне управління, цифрова трансформація, алгоритмічна прозорість, цифровий суверенітет, етичні ризики.

Summary. Introduction. Artificial intelligence (AI) is increasingly recognized as a transformative force in public administration, enhancing decision-making processes, optimizing resource allocation, and elevating the overall efficiency of governance mechanisms. This article explores promising avenues for integrating AI within public administration frameworks, while also addressing the ethical considerations inherent to its deployment. The findings underscore that AI applications can serve as pivotal catalysts for greater transparency, openness, and innovation in administrative practices. Given the rapid pace of digital advancement, this topic remains exceptionally pertinent and merits sustained attention from both the scholarly community and public-sector practitioners. This article explores the potential and associated risks of integrating artificial intelligence (AI) into the system of public administration, particularly in the context of contemporary challenges faced by Ukraine.

Purpose. The purpose of the study is to analyze scholarly research, the legislative framework, and practical applications of AI within the public sector, as well as to assess the social, technological, and legal risks associated with the deployment of these technologies. Furthermore, based on an examination of both international and domestic experiences, the study proposes recommendations for the further integration of AI into public administration.

Materials and methods. The research methodology is grounded in a systems-based approach that combines the analysis of academic literature, legal acts, and practical cases of AI implementation. Particular attention is paid to initiatives related to the automation of public services, the use of machine learning in healthcare, the financial sector, and administrative processes. The findings indicate that AI significantly enhances management efficiency by automating routine tasks, optimizing analytical processes, and improving forecasting capabilities. For instance, Ukrainian projects such as the mobile application «Diia» and diagnostic systems in healthcare demonstrate increased accessibility and reduced service delivery times.

Nonetheless, the study also identifies a range of critical risks. Socioeconomic threats include algorithmic bias due to poor data quality, fiscal burdens on public budgets, and organizational challenges associated with integrating AI into outdated IT infrastructures. Technological risks emerge from the complexity of adapting algorithmic solutions to diverse operational environments. Institutional challenges encompass legal ambiguity, the lack of ethical standards, and public distrust toward the deployment of AI-based technologies in the public domain. For example, the use of proprietary algorithms by private entities may undermine the transparency of state decision-making processes.

Results. Based on the conducted analysis, the article offers a set of recommendations aimed at mitigating these risks. These include the establishment of a centralized body for coordinating AI-related initiatives, the development of clear legal frameworks governing algorithmic transparency and data protection, and the implementation of educational programs for civil servants and the general public. It is emphasized that the success of digital transformation depends on achieving a balance between innovation and security guarantees. Specifically, the integration of ethical principles (e.g., the humanization of technology) into national policy and the involvement of academia and civil society in the auditing of AI systems are recommended.

AI holds the potential to radically reshape traditional models of governance; however, its implementation requires a comprehensive approach. A key condition for this approach is the combination of technological modernization with robust legal regulation, human capacity development, and the cultivation of public trust. Such a strategy may enable Ukraine to fully harness the advantages of AI while minimizing the risks associated with its use, thereby strengthening state resilience in the face of global challenges.

Discussion. Further research will focus on assessing the effectiveness of AI algorithms in multilevel government processes, developing ethical and legal control mechanisms, integrating machine learning into decision-making, and analyzing potential risks to ensure transparency and security, as well as formulating practical recommendations for public institutions.

Key words: artificial intelligence, public administration, digital transformation, algorithmic transparency, digital sovereignty, ethical risks.

Постановка проблеми. У контексті трансформацій що відбуваються в українській державі та на тлі збройної агресії щодо України, зростає потреба в модернізації публічного управління як засобу забезпечення стабільності й стійкості держави. Сучасна система адміністративного управління має не лише відповідати викликам часу, а й сприяти утвердженню

України як демократичної, правової європейської держави. Досягнення цієї мети вимагає інтеграції сучасних наукових підходів у сфері державного управління, законотворчості та практики реалізації управлінських рішень [1]. Оновлення організаційної структури органів влади, посилення технічної бази їх функціонування — усе це є необхідними складовими цього процесу.

Дієвість публічного управління нині значною мірою визначається здатністю держави оперативно реагувати на зовнішні та внутрішні виклики. Водночас відсутність належної координації між рівнями влади й нестача ефективних інструментів прийняття рішень ускладнює розвиток інтеграції ІІІ в державне управління, породжуючи ризики пов'язані з використанням технологій.

Публічна адміністрація зазнає впливу як внутрішніх, так і зовнішніх чинників трансформації, серед яких особливе значення мають глобалізаційні процеси та цифровізація суспільства. У зв'язку з цим актуалізується потреба в пошуку нових управлінських підходів. Зокрема, використання технологій штучного інтелекту (ІІІ) стає інструментом, здатним суттєво підвищити результативність державного управління.

Але, важливо, розвиток інформаційних технологій спрямовувати на забезпечення соціально-економічного зростання без послаблення національної безпеки або компрометації цифрової незалежності держави. Протягом останніх кількох років питання цифрового суверенітету стало критичним елементом безпекової стратегії багатьох урядів, оскільки зростає ризик втрати контролю над державними сервісами через залежність від іноземних провайдерів інфраструктури й каналів передачі та зберігання даних.

ІІІ дедалі активніше проникає у публічний сектор, підвищуючи продуктивність та зменшуючи витрати в державному управлінні. Завдяки можливості опрацьовувати великі обсяги інформації, ІІІ автоматизує рутинні операції, покращує точність аналітики та сприяє оптимальному розподілу ресурсів. Водночас впровадження таких систем вимагає розробки чітких нормативних актів, які гарантуватимуть відкритість алгоритмів, захист персональних даних громадян і визначатимуть відповідальність за наслідки рішень, сформованих машинним навчанням.

Аналіз останніх досліджень і публікацій. У сучасних умовах цифрової трансформації особливої актуальності набувають інноваційні та модернізаційні процеси в національних системах державного управління. З огляду на глобальний характер цифрового переходу, наукова спільнота активно досліджує трансформаційні зміни в адміністративному управлінні, які супроводжуються впровадженням цифрових технологій.

Поглиблений аналіз впливу цифрової епохи на механізми державного управління здійснено у працях Ф. М. Ідзі та Р. К. Гомеса. Вони зосередили увагу на необхідності перегляду соціальних контрактів у межах цифрового врядування, а також виокремили основні виклики, що постають перед державними інституціями при розробці політики в цифровому середовищі [4]. Водночас на прикладі Італійського національного інституту соціального забезпечення В. Бонаволонти та М. Д'Анджело дослідили наслідки

цифрового переходу в системі публічного адміністрування Італії [5].

Зокрема, дослідники К. Лоу, Дж. Ріголіні та Л. Солбес Кастро наголошують, що в багатьох державах цифрові інструменти набувають дедалі більшої ролі у сфері надання соціальних послуг [2]. Така цифровізація охоплює всі етапи ланцюга надання соціального захисту — від нових підходів до обробки даних до впровадження сучасних технологічних платформ і пристроїв. Водночас цифрова трансформація соціальної сфери визначається як один із ключових напрямів державної цифрової стратегії, спрямованої на формування ефективної сервісно-орієнтованої держави.

З іншого боку, В. Хоодаківська та її колеги запропонували підходи до активізації цифровізації в органах влади, аргументуючи свою позицію результатами, що свідчать про позитивний вплив цифрових технологій як на діяльність органів влади, так і на якість обслуговування населення [6].

У свою чергу, А. Хоодаді та А. Аббаспур [7] презентували модель цифрового державного управління на прикладі «віртуальних організацій» державного сектору. Актуальним є і дослідження А. Скуполи та І. Мергеля, які акцентують на потенціалі спільного виробництва у процесі цифрової трансформації надання державних послуг та формування суспільної цінності [8].

Паралельно з цифровою трансформацією державного управління значно зростає інтерес до проблематики штучного інтелекту (ІІІ), що набуває міждисциплінарного характеру та є предметом дослідження науковців, фахівців-практиків і експертів з різних галузей знань — від публічного управління до права, економіки й менеджменту. Застосування ІІІ супроводжується низкою потенційних ризиків і викликів, що, своєю чергою, обумовлює необхідність удосконалення правового регулювання цієї сфери.

На додаток, дослідження Ю. Тюрі, С. Квіткі, Н. Новіченко та О. Бардаха засвідчують, що ІІІ є однією з провідних цифрових технологій, яка відіграє ключову роль у вирішенні складних завдань публічного управління, зокрема у сфері муніципального адміністрування. Відтак, впровадження ІІІ в управлінську практику органів місцевого самоврядування сприяє розробці ефективних стратегій використання муніципальних ресурсів [9].

Формулювання цілей статті (постановка завдання). Метою статті є дослідження наукових статей та законодавства що наразі регулюють галузь ІІІ, аналіз прикладів використання штучного інтелекту в публічному управлінні, оцінка ризиків які виникають під час інтеграції штучного інтелекту у сферу публічного управління, а також сформулювати рекомендації для подальшої інтеграції ІІІ в сферу публічного управління.

Виклад основного матеріалу. Інтерес до ІІІ як засобу цифрової модернізації державного сектору

постійно зростає. Це зумовлено як загальними тенденціями цифрового переходу, так і політичними пріоритетами. У цьому контексті ІІІ розглядається не лише як технічне нововведення, а як ключовий елемент майбутньої цифрової економіки, що має потенціал підвищити ефективність державного управління та поліпшити якість життя населення.

Застосування ІІІ в публічному секторі охоплює різноманітні аспекти: від оптимізації адміністративних процедур до автоматизації рутинних завдань і вдосконалення взаємодії з громадянами. ІІІ здатен оперативно аналізувати великі обсяги інформації, виявляти закономірності та забезпечувати більш точне й обґрунтоване прийняття рішень. У результаті зменшиться обсяг технічної роботи, покладеної на державних службовців, а тому зможуть зосередитися на стратегічних завданнях [10].

Українське законодавство вже визначає поняття штучного інтелекту як систему, що поєднує інформаційні технології, алгоритмічні рішення, бази знань і моделі прийняття рішень для вирішення складних завдань [11]. Це означає, що ІІІ розглядається як міждисциплінарний інструмент, здатний об'єднати наукові підходи з практичними механізмами реалізації державної політики.

У Великій Британії практики застосування інноваційних цифрових рішень у державному управлінні реалізуються за двома напрямками: грантування проектів комерційного сектору та підтримка науково-дослідних ініціатив у навчальних та дослідницьких установах. Ще у 2010 році в більшості розвинених країн було запроваджено електронне надання державних і муніципальних послуг, а в Британії створено єдиний відкритий портал державних даних [10]. Ця платформа слугує базою для розробки аналітичних сервісів, у тому числі на основі ІІІ, що уможливорює оперативний доступ до статистичних даних та прозорість роботи органів державної влади.

У Сполучених Штатах має місце комплексний підхід до розвитку ІІІ на державному рівні, офіційно закріплений у «Національному стратегічному плані досліджень і розробок в області штучного інтелекту» [10]. Починаючи з 2022 року Міністерство фінансів США впроваджує системи машинного навчання для аналізу фінансових транзакцій у реальному часі, що дозволяє виявляти шахрайські операції, прогнозувати ризики та оптимізувати реагування на інциденти, значно знижуючи навантаження на аналітичні служби.

В українському контексті практична реалізація технологій ІІІ відбувається у декількох ключових напрямках. Державна служба статистики України автоматизує збір і обробку даних за допомогою алгоритмів ІІІ, що підвищує точність статистичних звітів. Міністерство охорони здоров'я використовує машинне навчання для діагностики захворювань, аналізу медичної статистики та прогнозування результатів лікування, що сприяє покращенню якості

медичних послуг. Крім того, у мобільному додатку «Дія» інструменти ІІІ автоматизують багатофункціональні процеси надання публічних послуг, скорочують час обслуговування населення та підвищують його доступність.

Банківський сектор України також впроваджує рішення на базі ІІІ. «ПриватБанк» реалізував систему поведінкової автентифікації на платформі NuDetect (MasterCard), що аналізує біометричні й поведінкові характеристики користувачів у реальному часі, виявляє аномальні патерни взаємодії та запобігає кібератакам. Крім того, у торговельних мережах були впроваджені біометричні POS-термінали «Android PAX» з технологією FacePay24, що дозволяють здійснювати оплати за допомогою розпізнавання обличчя.

Впровадження технологій штучного інтелекту в сфері публічного управління забезпечує низку комплексних переваг. По-перше, завдяки високоточному моделюванню та прогнозуванню великих обсягів даних системи ІІІ значно підсилюють аналітичні можливості органів влади, дозволяючи передбачати попит на державні послуги та виявляти приховані закономірності в інформаційних масивах. Це створює міцну основу для планування політики і організації надання послуг, оскільки ухвалення рішень базується на емпіричних висновках, а не на інтуїції чи фрагментарних оцінках [12].

Крім явних переваг — скорочення часу обробки заявок, підвищення якості та доступності державних сервісів, економія бюджетних ресурсів і підтримка зростання продуктивності праці — варто насамперед звернути увагу на менш очевидні ефекти. Зокрема, налаштування комунікаційних інтерфейсів ІІІ на урядових порталах дозволяє досягати глибшої персоналізації взаємодії з громадянами, адаптуючи відповіді до індивідуальних запитів та поведінкових характеристик користувачів, що потребує додаткових досліджень і випробувань у реальних умовах [13].

ІІІ також відіграє важливу роль у внутрішніх процесах державних установ, сприяючи ефективнішому відбору пріоритетних справ і розподілу навантаження між співробітниками. Ілюстрацією цього може слугувати система, яка, аналізуючи фінансові дані громадян, своєчасно прогнозує накопичення проблемних боргів і надає цю інформацію соціальним працівникам для здійснення превентивних заходів; або алгоритми виявлення аномалій, що на основі аналізу різномірних дата-сетів визначають типові ознаки шахрайства під час обробки конфіденційної інформації одержувачів адміністративних послуг [12].

У довгостроковій перспективі ці механізми сприятимуть оптимізації розподілу ресурсів і підвищенню ефективності публічних сервісів, адже вже зараз спостерігається скорочення часу обробки даних і розширення спектру передбачуваних послуг [12]. Отже, поширення ІІІ в державному секторі стає безповоротним трендом, що забезпечує не лише підвищення

оперативності та достовірності рішень, але й зниження рівня помилок і шахрайських дій, а також формування нових підходів до розробки внутрішньої політики, орієнтованої на персоналізацію сервісів [12].

Водночас реалізація цих можливостей залежить від того, хто розробляє та впроваджує ІІІ в публічному управлінні. Виконання проєктів безпосередньо державними структурами сприяє більшій прозорості алгоритмів і легшому зовнішньому аудиту систем [14]. Якщо ж розробку доручати приватним компаніям із налагодженою експертизою, зростає ризик обмеженості доступу до вихідних даних і моделей, що може поставити під загрозу відкритість процесів і захист фундаментальних прав громадян [15].

Отже, політика інтеграції ІІІ в публічне управління має базуватися на всебічному аналізі не лише технічних переваг, а й супутніх ризиків. Це передбачає поширення ефективних практик, оптимізацію нормативного поля, узгодження можливостей ІІІ з цілями державної політики, а також регулярний моніторинг рівня цифровізації суспільства через оцінку попиту й використання ІІІ-орієнтованих послуг громадянами та органами влади [12].

Попередній аналіз переваг ІІІ дозволяє стверджувати про відносну безпечність його подальшого застосування. Водночас, як і будьяка інноваційна технологія, впровадження ІІІ супроводжується занепокоєннями щодо потенційних ризиків та можливих шкідливих наслідків, породжених його алгоритмічними системами.

Аналізуючи особливості застосування ІІІ в публічному управлінні, можна виокремити дві основні групи ризиків:

1. Соціально-економічні ризики, пов'язані із впливом ІІІ на громади та добробут громадян.
2. Технологічні ризики, які стосуються складності роботи інформаційно-комп'ютерних систем та програмного забезпечення.

Для публічного сектору особливо критичними є інституційні ризики — потенційне зниження ефективності та результативності роботи інститутів публічного управління внаслідок невідповідності організаційних процесів сучасним цифровим вимогам. До таких ризиків належать:

1. Якість даних і упередженість алгоритмів. Рішення, що генерує ІІІ, суттєво залежать від якості вхідних даних. Неповні, застарілі або упереджені дані можуть призвести до хибних або дискримінаційних висновків. У разі відсутності механізмів контролю ризик повторного відтворення упереджень у алгоритмах зростає, що підвищує ймовірність прийняття неправомірних рішень.

2. Фінансові та організаційні витрати. Високі початкові інвестиції на розробку й інтеграцію рішень ІІІ, ліцензування технологій, адаптацію існуючої ІТ-інфраструктури, підготовку персоналу та подальшу підтримку систем є вагомим бар'єром для багатьох державних установ з обмеженими бюджетами [8]. Без

ретельного бюджетного планування впровадження ІІІ може спричинити фінансові перевитрати.

3. Складність системної інтеграції. Поєднання нових ІІІ-моделей з різномірними даними та застарілими ІТ-системами ускладнюється технічними, організаційними та юридичними перешкодами. Розбіжність форматів даних, нерозвинена комунікація між департаментами та брак фахівців з відповідними навичками створюють додаткові ризики невдалого впровадження.

4. Правові та етичні аспекти. Незавершеність нормативної бази, відсутність чітких етичних стандартів та механізмів зовнішнього аудиту алгоритмів сприяють правовій невизначеності. Це гальмує розвиток ІІІ у публічному управлінні та підсилює недовіру громадськості.

Варто зазначити, що впровадження штучного інтелекту (ІІІ) у сферу публічного управління, як показують дослідження, вимагає не лише технічних рішень, а й ґрунтового інституційного підґрунтя. Звісно, мова йде про формування механізмів, що поєднують правові норми, управлінські процедури та етичні стандарти для контролю алгоритмічних систем. Важливо розуміти: саме гармонізація цих компонентів, на думку експертів, створює умови для зниження ризиків, пов'язаних із технологіями, та робить їх інтеграцію в державні процеси безпечнішою.

Хорошим рішенням може бути створення центрального органу з питань ІІІ, який міг би функціонувати безпосередньо в межах державного апарату та об'єднувати людські, технологічні й фінансові ресурси для підтримки та реалізації державних ініціатив. Окрім того, до обов'язків такого органу слід віднести координацію співпраці між урядовими структурами, галузевими агентствами та представниками індустрії, сприяння науковим дослідженням і встановлення партнерських зв'язків із академічними інституціями та приватним сектором.

Враховуючи високий рівень ризиків, пов'язаних із масштабним застосуванням ІІІ, публічний сектор має розробити механізм, здатний прогнозувати, локалізувати і нейтралізувати потенційні загрози, а також забезпечити чітке та послідовне дотримання принципів і пріоритетів у сфері штучного інтелекту. З одного боку, важливо забезпечити дотримання етики — скажімо, гарантій конфіденційності даних або прозорості алгоритмів. З іншого боку, як показує практика, без чіткого розподілу відповідальності між учасниками процесів обробки інформації ефективне управління неможливе. До слова, наукова спільнота наполегливо наголошує: моніторинг впливу ІІІ на права людини має бути динамічним, а методи аналізу — гнучкими, щоб вчасно реагувати на нові виклики.

Велике значення має підвищення обізнаності громадськості та державних службовців щодо базових принципів роботи ІІІ. Саме тому публічні установи мають активізувати освітні ініціативи — скажімо, безкоштовні курси чи відкриті лекції. Подібні

кроки, зрештою, не лише «демістифікують» технології, а й допоможуть зменшити упередження, які, часто виникають через нестачу знань.

Отже, як бачимо, успішна інтеграція ІІІ у публічне управління — це баланс між інноваціями та захистом суспільних цінностей. Зрозуміло, що без науково обґрунтованої політики, яка враховує і технічні, і соціальні аспекти, досягти такого балансу неможливо. Адже технології, як би вони не були складними, завжди залишаються інструментом — і саме людина має залишатися їхнім творцем та головним бенефіціаром.

Висновки. Не можна заперечувати: ІІІ має потенціал кардинально змінити традиційні моделі публічного управління, адже здатний аналізувати колосальні масиви даних з неймовірною швидкістю, автоматизувати рутину та генерувати прогнози, які людському розуму важко відтворити. Цікаво, що саме через здатність виявляти приховані зв'язки між даними ІІІ може стати основою для прийняття рішень, адже такі рішення будуть ґрунтуватися повній інформації щодо проблеми, а не тільки частині. Проте, така трансформація державного сектору супроводжується цілою низкою проблем, і мова тут не лише про технічні аспекти, а й про соціально-етичні проблеми.

Для забезпечення гармонійної інтеграції ІІІ в публічний сектор необхідно вивести на передній план формування комплексного підходу, в якому держуправління, наукова спільнота та громадські організації співпрацюватимуть на засадах відкритості та підзвітності. Це передбачає створення чітких норм регулювання, що визначають вимоги до прозорості алгоритмів, стандарти захисту персональних даних і процедури зовнішнього аудиту. Водночас слід активніше розвивати освітні програми для державних службовців та технічних фахівців, щоб зменшити розрив між технологічним потенціалом і наявними компетенціями кадрів.

Отже, майбутнє публічного управління в епоху цифровізації багато в чому залежить від здатності держави не лише впроваджувати інноваційні рішення, а й ефективно управляти ризиками, які з ними пов'язані. Комплексне поєднання модернізації інфраструктури, правового забезпечення, етичного контролю та кадрового розвитку створить передумови для відповідального використання ІІІ. Лише такий збалансований підхід дозволить державі використати всі переваги технологій штучного інтелекту, забезпечивши при цьому належний рівень безпеки, прозорості та довіри з боку громадян.

Література

1. Міністерство та Комітет цифрової трансформації України. (n.d.). *Офіційний сайт*. URL: <https://thedigital.gov.ua> (дата звернення: 06.05.2025).
2. Idzi, F. M., & Gomes, R. C. (2022). Digital governance: government strategies that impact public services. *Global Public Policy and Governance*. <https://doi.org/10.1007/s43508-022-00055-w>.
3. Bonavolontà, V., & D'Angelo, M. (2021). Digital transition and public administration in Italy: the experience of the Italian National Social Security Institution — INPS. *Ubezpieczenia Społeczne. Teoria i praktyka*, 150(3). <https://doi.org/10.5604/01.3001.0015.5236>.
4. Lowe, C., Rigolini, J., Solbes Castro, L., & Bastagli, F. (2023). *Pathways toward digitalization in Social Protection and Labor (SPL) service delivery*. World Bank, Washington, D.C. <https://doi.org/10.1596/40473>.
5. Unynets-Khodakivska, V., Prystupa, L., Ivanyshyna, O., Panura, I., & Tuchak, T. (2023). Implementation of digital technologies in Public Administration. *Revista de la Universidad del Zulia*, 14(39), 295–312. <https://doi.org/10.46925/rdluz.39.16>.
6. Khodadadi, A., Abbasspour, A. (2022). Modeling digital governance in virtual organizations in the public sector: A case study of the Social Security Insurance Organization. *Political Sociology of Iran*, Vol. 5, No. 12, Pp. 3231–3246. <https://doi.org/10.30510/psi.2022.339758.3407>.
7. Scupola, A., & Mergel, I. (2022). Co-production in digital transformation of public administration and public value creation: The case of Denmark. *Government Information Quarterly*, 39(1), 101650. <https://doi.org/10.1016/j.giq.2021.101650>.
8. Квітка, С., Новіченко, Н., & Бардах, О. (2021). Штучний інтелект у муніципальному управлінні: вектори розвитку. *Аспекти публічного управління*, 9(4), 85–94. <https://doi.org/10.15421/152140>.
9. Author, Larsson, A., Teigland R., (2019). *Digital Transformation and Public Services* (Taylor & Francis). doi: 10.4324/9780429319297.
10. Концепція розвитку штучного інтелекту в Україні. (2020). URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80> (дата звернення: 06.05.2025).
11. Sullivan-Paul, M. (2024). Why AI literacy is essential for public administration. *European Institute of Public Administration*. URL: <https://www.eipa.eu/blog/ai-literacy-for-public-administration/> (дата звернення: 06.05.2025).
12. Rzycki, B., Dueñas-Cid, D., & Przegalinska, A. (2024). *Research Handbook on Public Management and Artificial Intelligence*. Elgar Online: The online content platform for Edward Elgar Publishing. <https://doi.org/10.4337/9781802207347>.
13. Steen, M., Timan, T., & van de Poel, I. (2021). Responsible innovation, anticipation and responsiveness: case studies of algorithms in decision support in justice and security, and an exploration of potential, unintended, undesirable, higher-order effects. *AI and Ethics*. <https://doi.org/10.1007/s43681-021-00063-2>.

15. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2017). Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. *Science and Engineering Ethics*. <https://doi.org/10.1007/s11948-017-9901-7>.

References

1. Ministerstvo ta Komitet tsyfrovoy transformatsii Ukrainy [Ministry and Committee of Digital Transformation of Ukraine]. (n.d.). *Ofitsiyni sait*. Retrieved from <https://thedigital.gov.ua>
2. Idzi, F.M., & Gomes, R.C. (2022). Digital governance: government strategies that impact public services. *Global Public Policy and Governance*. <https://doi.org/10.1007/s43508-022-00055-w>
3. Bonavolontà, V., & D'Angelo, M. (2021). Digital transition and public administration in Italy: the experience of the Italian National Social Security Institution — INPS. *Ubezpieczenia Społeczne. Teoria i praktyka*, 150(3). <https://doi.org/10.5604/01.3001.0015.5236>
4. Lowe, C., Rigolini, J., Solbes Castro, L., & Bastagli, F. (2023). *Pathways toward digitalization in Social Protection and Labor (SPL) service delivery*. World Bank, Washington, D.C. <https://doi.org/10.1596/40473>
5. Unynets-Khodakivska, V., Prystupa, L., Ivanyshyna, O., Panura, I., & Tuchak, T. (2023). Implementation of digital technologies in Public Administration. *Revista de la Universidad del Zulia*, 14(39), 295–312. <https://doi.org/10.46925/rd-luz.39.16>
6. Khodadadi, A., Abbasspour, A. (2022). Modeling digital governance in virtual organizations in the public sector: A case study of the Social Security Insurance Organization. *Political Sociology of Iran*, Vol. 5, No. 12, Pp. 3231–3246. <https://doi.org/10.30510/psi.2022.339758.3407>.
7. Scupola, A., & Mergel, I. (2022). Co-production in digital transformation of public administration and public value creation: The case of Denmark. *Government Information Quarterly*, 39(1), 101650. <https://doi.org/10.1016/j.giq.2021.101650>
9. S. Kvitka, N. Novichenko, O. Bardakh. Artificial intelligence in municipal administration: vectors of development. *Public administration aspects*, 9(4), 85–94. <https://doi.org/10.15421/152140>
10. Author, Larsson, A., Teigland R., (2019). *Digital Transformation and Public Services* (Taylor & Francis). doi: 10.4324/9780429319297
11. Konceptualnist rozvytku shtuchnoho intelektu v Ukraini [Concept of artificial intelligence development in Ukraine]. (2020). Retrieved from <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80>
12. Sullivan-Paul, M. (2024). Why AI literacy is essential for public administration. *European Institute of Public Administration*. Retrieved from <https://www.eipa.eu/blog/ai-literacy-for-public-administration/>
13. Rzycki, B., Dueñas-Cid, D., & Przegalinska, A. (2024). *Research Handbook on Public Management and Artificial Intelligence*. Elgar Online: The online content platform for Edward Elgar Publishing. <https://doi.org/10.4337/9781802207347>
14. Steen, M., Timan, T., & van de Poel, I. (2021). Responsible innovation, anticipation and responsiveness: case studies of algorithms in decision support in justice and security, and an exploration of potential, unintended, undesirable, higher-order effects. *AI and Ethics*. <https://doi.org/10.1007/s43681-021-00063-2>
15. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2017). Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. *Science and Engineering Ethics*. <https://doi.org/10.1007/s11948-017-9901-7>

Стаття надійшла до редакції 26.05.2025

УДК 352:330.34

Короляк Остап Орестович

*аспірант кафедри регіонального та місцевого розвитку,
Інституту адміністрування, державного управління та професійного розвитку
НУ «Львівська політехніка»*

Koroliak Ostap

*Postgraduate Student of the Department of Regional and Local Development
Institute of Administration, Public Governance and Professional Development
Lviv Polytechnic National University
ORCID: 0009-0001-2331-3208*

DOI: 10.25313/2617-572X-2025-5-10973

ІНСТИТУЦІЙНА СПРОМОЖНІСТЬ ТЕРИТОРІАЛЬНИХ ГРОМАД ЯК ЧИННИК ЕКОНОМІЧНОГО РОЗВИТКУ УКРАЇНИ

INSTITUTIONAL CAPACITY OF TERRITORIAL COMMUNITIES AS A FACTOR OF ECONOMIC DEVELOPMENT OF UKRAINE

Анотація. Вступ. Децентралізація в Україні створила умови для розвитку територіальних громад, однак війна загострила виклики й актуалізувала питання їх інституційної спроможності. Сьогодні саме здатність громад ефективно управляти ресурсами, підтримувати підприємництво та реалізовувати проекти розвитку визначає темпи їх економічного відновлення та перспективи сталого розвитку.

Мета. Метою статті є обґрунтування ролі інституційної спроможності територіальних громад як визначального чинника їх економічного розвитку та формування практичних підходів до зміцнення інституційного потенціалу громад в умовах післявоєнного відновлення України.

Матеріали та методи. Основу дослідження становлять аналітичні звіти, наукові праці, присвячені питанням розвитку місцевої економіки, управління в умовах нестабільності та інституційної спроможності, а також матеріали міжнародних програм підтримки місцевого розвитку в Україні.

У процесі дослідження застосовано системний підхід – для комплексного аналізу факторів інституційної спроможності громад; методи аналізу і синтезу – для узагальнення теоретичних положень і практичного досвіду, а також для виявлення ключових залежностей між рівнем інституційної спроможності та економічною стійкістю громад в умовах війни і відбудови; порівняльний аналіз – для оцінки особливостей реалізації національних і міжнародних програм підтримки громад (зокрема DOBRE, U-LEAD); метод логічного узагальнення – для формулювання висновків та розробки рекомендацій.

Результати. У статті окреслено поняття інституційної спроможності територіальної громади та виокремлено її ключові складові: організаційно-управлінську, кадрову, фінансову, нормативно-правову. Обґрунтовано прямий зв'язок між рівнем інституційної спроможності та економічним розвитком громад, зокрема у контексті залучення інвестицій, підтримки місцевого підприємництва і ефективного освоєння ресурсів на відбудову. Виявлено позитивний вплив міжнародних програм DOBRE та U-LEAD на підвищення спроможності громад. Доведено, що сильні інституції сприяють швидшому відновленню громад після воєнних руйнувань та формують основу для їх сталого економічного зростання.

Перспективи. Перспективними напрямками є розробка системи кількісних і якісних індикаторів для комплексного оцінювання інституційної спроможності громад, дослідження моделей ефективного залучення інвестицій через зміцнення локальних інституцій, а також аналіз результативності різних механізмів підтримки місцевого підприємництва у громадах на етапі повоєнної відбудови.

Ключові слова: територіальні громади, інституційна спроможність, економічний розвиток, місцеве самоврядування, підприємництво, післявоєнне відновлення, децентралізація.

Summary. Introduction. Decentralization in Ukraine has created conditions for the development of territorial communities; however, the war has intensified existing challenges and emphasized the importance of their institutional capacity. Today, the

ability of communities to effectively manage resources, support entrepreneurship, and implement development projects determines the pace of their economic recovery and prospects for sustainable growth.

Purpose. The article aims to substantiate the role of institutional capacity of territorial communities as a key factor in their economic development and to propose practical approaches for strengthening the institutional potential of communities in the context of Ukraine's post-war recovery.

Materials and Methods. The study is based on analytical reports and scholarly works related to local economic development, governance under instability, and institutional capacity, as well as materials from international programs supporting local development in Ukraine. The research employs a systems approach to comprehensively analyze the factors influencing institutional capacity; methods of analysis and synthesis to summarize theoretical foundations and practical experiences and to identify key correlations between the level of institutional capacity and the economic resilience of communities during war and reconstruction; comparative analysis to assess national and international support programs (particularly DOBRE and U-LEAD); and logical generalization to draw conclusions and formulate recommendations.

Results. The article defines the concept of institutional capacity of territorial communities and identifies its key components: organizational and managerial, human resources, financial, and legal frameworks. A direct correlation is established between the level of institutional capacity and the economic development of communities, especially in the areas of investment attraction, local entrepreneurship support, and effective use of reconstruction resources. The positive impact of international programs such as DOBRE and U-LEAD on strengthening local capacity is confirmed. It is argued that strong institutions facilitate faster recovery of communities from war-related destruction and lay the foundation for sustainable economic growth.

Prospects. Promising directions include the development of a system of quantitative and qualitative indicators for comprehensive assessment of institutional capacity, research into models of effective investment attraction through institutional strengthening, and analysis of the effectiveness of mechanisms for supporting local entrepreneurship during the post-war reconstruction phase.

Key words: territorial communities, institutional capacity, economic development, local self-government, entrepreneurship, post-war recovery, decentralization.

Постановка проблеми. Децентралізація влади в Україні, розпочата у 2014 році, була спрямована на формування спроможних територіальних громад, здатних самостійно вирішувати питання місцевого значення та забезпечувати свій розвиток [1]. У результаті адміністративно-територіальної реформи утворено понад 1400 об'єднаних територіальних громад, яким передано значні повноваження й ресурси. Однак повномасштабна війна, розв'язана Росією у 2022 році, спричинила величезні втрати для місцевої економіки та інфраструктури: багато громад зазнали руйнувань, втратили значну частину доходів, скоротилась інвестиційна активність.

У цих умовах на перший план виходить питання інституційної спроможності громад — їхньої здатності ефективно діяти в кризових ситуаціях і забезпечувати відновлення розвитку. Дослідження показують, що як матеріальні ресурси (інфраструктура, фінанси), так і нематеріальні чинники — зокрема якість управління — впливають на здатність громад долати сучасні загрози [4]. Місцеве самоврядування постало перед викликом одночасно відбудовувати зруйноване та закладати основи для подальшого зростання, що неможливо без належного інституційного потенціалу.

Особливо важливою є роль місцевого бізнесу у підтримці життєдіяльності громад під час війни та у повоєнний період. Малий і середній бізнес на місцях формує економічний фундамент громади — створює робочі місця, генерує доходи до місцевого бюджету, бере участь у процесах відбудови [4]. Під час воєнного стану підприємці потребують підтрим-

ки і сприятливих умов з боку місцевої влади, аби продовжувати діяльність або переорієнтувати бізнес на нові потреби (наприклад, виробництво товарів для оборони, надання послуг внутрішньо переміщеним особам тощо). Відтак, інституційна спроможність територіальних громад — передусім здатність органів місцевого самоврядування ефективно управляти ресурсами, підтримувати підприємництво й реалізовувати проекти розвитку — стає визначальним чинником їхнього економічного відродження.

Проблема підвищення інституційної спроможності громад набуває особливої актуальності у повоєнний період. Від того, наскільки дієздатними є місцеві інституції, залежить успішність реалізації планів відновлення інфраструктури, створення нових робочих місць, залучення інвестицій та донорської допомоги на місцевому рівні. Натомість, недоліки інституційного розвитку (дефіцит компетентних кадрів, слабкі управлінські практики, відсутність стратегічного планування, корупційні прояви тощо) можуть стати серйозною перешкодою для економічного зростання навіть за наявності фінансової підтримки [21, 22].

Таким чином, виникає науково-практичне завдання — визначити, як саме інституційна спроможність територіальних громад впливає на їхній економічний розвиток та які заходи дозволять зміцнити цю спроможність у сучасних умовах України.

Аналіз останніх досліджень і публікацій. Проблематика розвитку територіальних громад та їхньої спроможності привертає значну увагу науковців. Питання соціально-економічного розвитку громад

в умовах децентралізації досліджували такі українські вчені, як Ю. Барський, В. Поліщук, З. Герасимчук, С. Дорогунцов, Я. Жаліло, В. Зайчикова, О. Кириленко, І. Луніна, Л. Макаренко, С. Слухай, та інші. Зокрема, С. Чернов і Н. Муштинська розглядали об'єднання територіальних громад як механізм забезпечення їх ресурсної спроможності, необхідної для розвитку сільських територій [3].

Дослідники відзначають, що укрупнення громад та передача їм ресурсів має підвищити фінансову і організаційну базу розвитку, проте на практиці рівень спроможності різних громад залишається нерівномірним [4]. І. Котов у своїй роботі акцентував увагу на проблемах державного управління сталим розвитком територіальних громад в умовах кризових ситуацій, підкреслюючи необхідність посилення інституційного потенціалу на місцях для подолання наслідків воєнних викликів [12].

Також актуальними є наукові напрацювання щодо ролі малого бізнесу у розвитку громад. Зокрема, І. Романюк наголошував на важливості розвитку підприємництва та альтернативних видів діяльності сільського населення як чинника підвищення зайнятості й добробуту в сільських громадах [11].

Серед зарубіжних дослідників варто відзначити праці, присвячені децентралізації та інституційній спроможності на місцевому рівні. Так, у теорії фіскального федералізму (Р. Масгрейв, С. Оутс, Ч. Тібу та ін.) обґрунтовано переваги передачі ресурсів і повноважень на місця для ефективнішого задоволення потреб громади [5]. Концепція «спроможності громад» та «*saracity building*» розвивалася в працях зарубіжних експертів з публічного управління і розвитку територій, зокрема розглядалася взаємодія між місцевою владою, бізнесом і громадськістю в забезпеченні розвитку територій (М. Белл, С. Роуз-Екerman, Дж. Родден та ін.) [2].

Водночас специфічно питання інституційної спроможності об'єднаних громад в українських реаліях, особливо на тлі післявоєнного відновлення, поки що вивчене недостатньо. Більшість досліджень зосереджені або на фінансових аспектах місцевого розвитку, або на аналізі окремих інструментів (інвестиційна діяльність, державна підтримка тощо), тоді як цілісний підхід до оцінки інституційної спроможності громади як комплексу чинників розвитку потребує подальшого опрацювання. Таким чином, існує потреба заповнити цю наукову прогалину та зосередити увагу на інституційних передумовах економічного розвитку територіальних громад.

Мета і завдання дослідження. Метою статті є обґрунтування ролі інституційної спроможності територіальних громад як ключового чинника їх економічного розвитку та формування практичних підходів до зміцнення інституційного потенціалу громад в умовах післявоєнного відновлення України. Для досягнення поставленої мети передбачено виконання таких завдань: уточнити зміст поняття

«інституційна спроможність територіальної громади» та окреслити її основні складові; проаналізувати стан інституційної спроможності територіальних громад України в умовах децентралізації та повномасштабної війни; з'ясувати, яким чином інституційна спроможність органів місцевого самоврядування впливає на економічний розвиток громад, зокрема на здатність залучати інвестиції та підтримувати місцеве підприємництво; дослідити успішні практики та програми, спрямовані на підвищення інституційної спроможності громад, зокрема міжнародні проекти DOBRE, U-LEAD та інші, і оцінити їх ефективність; сформулювати практичні рекомендації щодо посилення інституційної спроможності територіальних громад з метою стимулювання їх економічного зростання, особливо у період післявоєнної відбудови.

Виклад основного матеріалу. У науковій літературі інституційну спроможність територіальної громади розглядають як здатність місцевих інституцій (насамперед органів місцевого самоврядування) ефективно реалізовувати свої повноваження, забезпечувати надання якісних публічних послуг, залучати й утримувати необхідні ресурси для розвитку громади [7, 8, 10]. Іншими словами, це комплексний показник того, наскільки «дієздатною» є громада як самостійний суб'єкт розвитку. Поняття спроможності громади було закріплено на законодавчому рівні в ході децентралізації: згідно із Методикою формування спроможних територіальних громад [4], спроможна громада — це громада, яка має достатній кадровий, фінансовий та інфраструктурний потенціал для виконання завдань місцевого самоврядування. Таким чином, можна виокремити кілька ключових складових інституційної спроможності:

- Організаційно-управлінський потенціал — наявність ефективної структури управління громадою, чіткий розподіл повноважень, налагоджені внутрішні процеси планування, виконання рішень і контролю. Важливим аспектом тут є стратегічне бачення розвитку громади та наявність стратегічних документів (стратегія розвитку, плани відновлення тощо).
- Кадровий ресурс — достатня кількість кваліфікованих працівників в органах місцевого самоврядування, їх професійна компетентність, можливість навчання і підвищення кваліфікації. Представники місцевої влади мають володіти необхідними знаннями і навичками у сферах управління проектами, фінансами, земельними ресурсами, комунікації з громадою тощо.
- Фінансові можливості — спроможність громади формувати достатню доходну базу місцевого бюджету, ефективно розпоряджатися фінансовими ресурсами, залучати додаткові кошти (інвестиції, гранти). В умовах децентралізації бюджети громад суттєво зросли, проте рівень фінансової спроможності різниться: є громади-донори та

громади-реципієнти дотацій, які здебільшого отримують базові дотації з державного бюджету. Це свідчить про нерівномірність економічної бази громад.

- Нормативно-правове забезпечення — наявність необхідної локальної нормативної бази (статут громади, регламенти, програми), дотримання законодавства, здатність органів місцевого самоврядування реалізовувати надані законом повноваження. Сюди ж можна віднести прозорість і підзвітність влади, відсутність корупційних бар'єрів, налагодженість механізмів участі громадськості.
- Соціальний капітал та партнерські мережі — хоча це нематеріальна складова, він теж є частиною інституційної спроможності. Мається на увазі рівень довіри мешканців до місцевої влади, їх залученість у процеси розвитку громади (громадські слухання, участь у проєктах), а також налагоджена співпраця громади з бізнесом, громадськими організаціями, сусідніми громадами, вищим рівнем влади. Широке партнерство розширює можливості громади у вирішенні своїх проблем.

Від усіх цих компонент залежить успішність громади у досягненні цілей розвитку. Якщо якась зі складових є «слабкою ланкою» (наприклад, брак фахівців чи неефективність управлінських процедур), громада може не реалізувати свій економічний потенціал навіть за сприятливих зовнішніх умов.

Економічний розвиток територіальної громади проявляється у зростанні місцевої економіки — збільшенні обсягів виробництва і послуг, створенні нових підприємств і робочих місць, зростанні доходів населення та бюджету, підвищенні якості життя мешканців. Інституційна спроможність виступає важливим чинником, що визначає темпи і сталість цього розвитку. Зокрема, якісне місцеве управління є передумовою ефективного використання ресурсів громади. Громади, які мають належний фаховий рівень управлінців та практикують сучасні підходи (стратегічне планування, проєктний менеджмент, публічно-приватне партнерство), досягають кращих результатів у соціально-економічному розвитку [23, 24].

Досвід впровадження реформи децентралізації підтвердив, що формальна передача фінансів і повноважень громадам ще не гарантує їх розвитку — усе залежить від спроможності громад ефективно ними розпорядитися [25]. Так, одні громади вже за перші роки після об'єднання продемонстрували значне зростання місцевих бюджетів, реалізували інфраструктурні проєкти, залучили інвесторів, тоді як інші — використовували кошти неефективно або взагалі не змогли освоїти виділені субвенції через відсутність проєктної підготовки. Отже, інституційна спроможність є тим внутрішнім ресурсом, що визначає здатність громади до розвитку.

Недарма серед критеріїв оцінки інвестиційної привабливості конкретної громади виокремлюють саме рівень її інституційно-управлінської спромож-

ності [4]. Для потенційного інвестора важливо, щоб у громаді були зрозумілі «правила гри», забезпечувалась підтримка з боку місцевої влади, відсутність зайвих бюрократичних бар'єрів. Залучення інвестицій — один із ключових шляхів економічного розвитку — прямо залежить від того, чи спроможна громада професійно організувати цю діяльність.

Згідно з експертними оцінками, інвестиційний потенціал громади формується не лише за рахунок матеріальних ресурсів (вільні земельні ділянки, трудові ресурси, інфраструктура), а й визначається інституційними чинниками — зокрема, спроможністю органів місцевого самоврядування забезпечити якісний супровід інвестора та оперативно реагувати на потреби бізнесу [9].

Інституційна спроможність також визначає ефективність використання коштів розвитку. Наприклад, у післявоєнний період громади отримуватимуть значні ресурси на відбудову (як з державного бюджету, так і від міжнародних партнерів). Але освоєння цих коштів потребує наявності проєктно-кошторисної документації, прозорих процедур закупівель, контролю якості робіт — тобто інституційних передумов. Громади, що мають підготовлені команди і налагоджені процеси, швидше та якісніше реалізують проєкти відбудови, тим самим відновлюючи економічну активність. Натомість там, де місцева влада не готова або не спроможна виконувати такі функції, процес відновлення гальмуватиметься, а економічні втрати будуть затяжними.

Окремо слід підкреслити роль інституційної спроможності у підтримці місцевого підприємництва. Мікро- та малі підприємства часто найбільше страждають від потрясінь (таких як війна чи пандемія), але водночас вони є гнучкими й можуть швидко відновитися за наявності належних умов. Місцева влада через свої інструменти може істотно вплинути на бізнес-клімат у громаді. До таких інструментів належать: встановлення пільгових місцевих податків і зборів для малого бізнесу; надання комунального майна в оренду на спрощених умовах; створення інфраструктури підтримки (центри надання адміністративних послуг, бізнес-центри, індустріальні парки); проведення навчань і консультацій для підприємців; сприяння кооперації бізнесу (кластерів) тощо.

В умовах війни багато громад стикнулися з необхідністю релокації бізнесу (прийому підприємств, що виїхали з прифронтових зон) та підтримки своїх виробників, аби зберегти робочі місця. Ті громади, що налагодили партнерство з бізнес-спільнотою та оперативно впровадили програми підтримки (гранти для місцевого бізнесу, ваучери, сприяння в пошуку нових ринків збуту), змогли пом'якшити негативний вплив війни на економіку. Як зазначається у публікації, підготовленій спільно з програмою «U-LEAD з Європою», місцевий бізнес під час війни потребує особливої підтримки, адже саме він

«підтримує економіку громади, створює робочі місця, долучається до процесів відбудови» [6]. Отже, інституційно спроможна громада — це та, в якій вибудовано ефективну систему взаємодії влади і бізнесу, що дозволяє спільно вирішувати економічні проблеми та використовувати нові можливості.

В Україні за останні роки реалізовано низку програм, спрямованих на розвиток потенціалу місцевого самоврядування та економічний розвиток громад. Серед найбільш масштабних — програма USAID DOBRE [16] (Decentralization Offering Better Results and Efficiency), що тривала у 2016–2021 роках і охопила понад 100 громад у 10 областях України. Програма DOBRE була націлена на всебічне зміцнення спроможності новостворених об'єднаних громад: надавалася експертна підтримка у розробці стратегій розвитку громад, проводились тренінги для посадовців місцевого самоврядування з фінансового менеджменту, просторового планування, залучення громадян, впроваджувалися проекти місцевого економічного розвитку за грантової підтримки [6]. За результатами цієї програми багато громад-партнерів DOBRE затвердили якісні стратегічні плани, створили або реорганізували структури економічного розвитку (наприклад, відділи залучення інвестицій, агенції розвитку), реалізували інфраструктурні проекти, що стало поштовхом для економічного розвитку (ремонт доріг, створення центрів надання адміністративних послуг, модернізація систем водопостачання тощо). Важливим здобутком стало налагодження практики бюджетування за участі громадськості та підвищення прозорості управління, що зміцнило довіру бізнесу і мешканців. Отриманий досвід нині використовується в інших громадах, зокрема через наступну програму USAID «HOVERLA», яка продовжує підтримку децентралізації.

Ще одним ключовим проектом є «U-LEAD з Європою» [6] — спільна програма Європейського Союзу та його країн-членів, яка реалізується з 2016 року і триває дотепер. Спочатку головний акцент U-LEAD було зроблено на створенні системи центрів надання адміністративних послуг у громадах, що само по собі підвищує інституційну спроможність через покращення якості послуг та адміністративної спроможності громад. Надалі програма охопила ширший спектр напрямів: навчання для муніципальних службовців, підтримка розробки місцевих стратегій розвитку, обміни досвідом між громадами, експертний супровід у впровадженні секторіальних реформ на місцевому рівні. Завдяки U-LEAD сотні об'єднаних громад отримали сучасні центри надання адміністративних послуг, тисячі чиновників підвищили кваліфікацію, було започатковано мережі взаємодії між громадами. Зокрема, в економічній сфері U-LEAD підтримує ініціативи з місцевого економічного розвитку: проведення аналізу економічного потенціалу громад, реалізацію пілотних проектів (створення кластерів, залучення інвесторів),

розробку маркетингових стратегій громад тощо. Ці заходи допомагають громадам краще зрозуміти свої конкурентні переваги і будувати ефективні стратегії зростання.

Окрім зазначених, в Україні реалізуються й інші програми та проекти міжнародної підтримки. Наприклад, програма «Мери за економічне зростання» (EU «Mayors for Economic Growth»), ініціатива ЄС, спрямована на підтримку муніципалітетів у розробці та фінансуванні проектів місцевого розвитку. Проекти технічної допомоги від ПРООН та інших агенцій ООН були зосереджені на відновленні громад у постраждалих від конфлікту регіонах Сходу України, що включало компоненти зміцнення інституційного потенціалу (створення агенцій розвитку, навчання в сфері управління відновленням). Швейцарсько-український проект DESPRO (2007–2017) у ранній період реформи також робив вагомий внесок у розвиток спроможності громад у сфері надання послуг (водопостачання, поводження з відходами) та міжмуніципального співробітництва. Кожна з цих ініціатив по-різному вирішувала проблеми інституційної слабкості: кадрові, організаційні, фінансові. Важливо, що міжнародні програми не лише надають одноразову підтримку (техніку, фінансування проектів), а й впроваджують нові стандарти управління, навчають сучасних методик, сприяють партнерству між владою, громадою і бізнесом. Приміром, завдяки програмам підтримки у деяких громадах створено локальні інституції розвитку — агенції місцевого розвитку, бізнес-центри, об'єднання підприємців. Хоча поки що такі інституції не всюди стали впливовими гравцями (часто такі установи представляють лише одну сторону і не забезпечують справжнього тристороннього партнерства «влада–бізнес–громада» [6]), їх поява — крок до посилення інституційного середовища громади.

Досвід інших країн показує, що саме усвідомлення місцевою владою необхідності нових підходів до економічного розвитку спонукає створювати спеціалізовані установи і механізми для їх реалізації. В Україні цей процес тільки набирає обертів, але вже очевидно, що громади з проактивною позицією у створенні інституцій розвитку (комунальних підприємств, агенцій, фондів підтримки бізнесу тощо) демонструють кращі результати [18, 19, 20].

Повномасштабна війна 2022 року стала випробуванням на міцність для інституційної спроможності українських громад. Ті з них, що мали вищий рівень самодостатності та налагоджені процеси управління, виявилися стійкішими до кризового впливу. Здатність громад швидко мобілізувати внутрішні ресурси, перебудувати роботу адміністрації на кризовий режим, підтримувати населення і бізнес визначалась, зокрема, згуртованістю місцевої влади та її компетентністю. Дослідження факторів стійкості громад під час війни підтверджує: не лише матеріальні ресурси, але й нематеріальні (людський

капітал, рівень залученості громади, якість управлінських рішень) впливають на те, чи спроможна громада впоратися з викликами [4]. Наприклад, на заході України чимало громад успішно прийняли десятки тисяч внутрішньо переміщених осіб, організували для них житло, роботу, інтеграцію — це стало можливим завдяки ефективній координації зусиль влади, волонтерів, місцевого бізнесу. Водночас окремі менш спроможні громади зіткнулися з управлінськими труднощами, перевантаженням ресурсів або браком координації і потребували суттєвої підтримки ззовні.

Повоєнне відновлення ставить нові завдання: необхідно не просто відбудувати зруйноване, але й закласти основи для сучасного економічного розвитку — створення інноваційних виробництв, розвиток малого і середнього бізнесу, інтеграцію в європейські ринки. Тут роль інституційної спроможності буде вирішальною. Громади мають навчитися ефективно управляти проектами відбудови, прозоро розподіляти ресурси фондів відновлення, залучати приватні інвестиції у відбудову та розвиток. Злагоджена робота місцевої адміністрації з центральними органами влади, міжнародними донорами — теж питання інституційної спроможності, яка включає, зокрема, наявність кваліфікованих кадрів, володіння іноземними мовами, навички проектної діяльності та дотримання вимог донорів тощо.

Отже, від інституційної спроможності територіальних громад значною мірою залежить успіх економічного відродження України загалом. Сильні громади здатні стати осередками зростання, точками притягання інвестицій і населення, тоді як слабкі ризикують перетворитися на депресивні зони. Розуміння цього визначає актуальність заходів з подальшого зміцнення інституційної спроможності — як на рівні кожної громади, так і через державну регіональну політику та міжнародну підтримку.

Висновки та перспективи подальших досліджень. Інституційна спроможність територіальних громад є фундаментальною умовою їхнього сталого економічного розвитку. Проведений аналіз показав, що громади, які мають вищий інституційний потенціал — ефективний управлінський апарат, кваліфіковані кадри, налагоджені процедури, партнерські зв'язки — значно успішніші у залученні інвестицій, розвитку місцевого бізнесу та забезпеченні економічного зростання. Натомість слабкий інституційний потенціал здатен нівелювати навіть переваги сприятливого ресурсного середовища. Особливо це проявилось в умовах воєнного часу: інституційно сильні громади виявилися більш стійкими та здатними швидко адаптуватися до нових викликів.

Результати дослідження підтверджують, що для повоєнного відновлення економіки України важливо зосередити увагу не лише на фінансових вливаннях у громади, але й на розвитку їхнього інституційно-

го потенціалу. В практичному вимірі це означає інвестування в людський капітал місцевого самоврядування (навчання, обмін досвідом, підвищення престижу служби в органах місцевої влади), удосконалення нормативної бази та процедур (спрощення регулювання для бізнесу на місцевому рівні, запровадження цифрових рішень в управлінні громадою), стимулювання міжмуніципальної кооперації (спільна реалізація проектів, що перевищують можливості однієї громади).

Необхідно продовжувати і масштабувати кращі практики, напрацьовані в рамках програм DOBRE, U-LEAD та інших: інституційний аудит громад, розробка дорожніх карт підвищення спроможності, підтримка створення агенцій місцевого розвитку, залучення громадян до ухвалення рішень. На державному рівні доцільно інтегрувати ці підходи в реалізацію Державної стратегії регіонального розвитку та планів повоєнної відбудови, забезпечивши координацію між центральною владою, громадами та міжнародними партнерами.

Місцеве підприємництво відіграватиме ключову роль у відновленні економіки, і місцеві інституції мають стати для нього не бар'єром, а союзником. Інституційно сильна громада здатна створити екосистему, де бізнес почувається захищено і має можливості для зростання — від наявності елементарних умов (інфраструктура, швидкі адміністративні послуги) до спільних стратегічних ініціатив (створення кластерних об'єднань, брендинг території, просування інвестиційних можливостей громади).

Перспективи подальших досліджень вбачаються в розробці кількісних індикаторів для вимірювання рівня інституційної спроможності територіальних громад та методик комплексної оцінки її впливу на соціально-економічні показники розвитку. Це дозволило б виявляти «вузькі місця» та точково спрямовувати зусилля на їх усунення. Також потребують вивчення питання оптимального поєднання різних інструментів підтримки громад: фінансової допомоги, навчальних програм, дорадництва — з точки зору досягнення довгострокового ефекту саме у нарощуванні власної спроможності громади. Важливим напрямом є порівняння українського досвіду з практиками інших країн, що переживали подібні виклики (наприклад, післявоєнне відновлення балканських країн, відновлення після природних катастроф тощо) — це допоможе запозичити успішні моделі інституційного розвитку.

Таким чином, зміцнення інституційної спроможності територіальних громад слід розглядати як стратегічне завдання на шляху до сталого економічного розвитку України. Інвестування в сильні місцеві інституції — це інвестування в майбутнє, де громади будуть самодостатніми, конкурентоспроможними та здатними забезпечити гідний рівень життя своїх мешканців.

Література

1. Швидюк С. Состоятельная территориальная община по-украински: теоретическая модель и практика создания. *Eastern Review*. 2017. Т. 6. С. 37–48.
2. Rose-Ackerman S. *Corruption and Government: Causes, Consequences, and Reform*. Cambridge: Cambridge University Press, 1999. 266 p.
3. Чернов С.І., Мушинська Н.Ю. Об'єднання територіальних громад як механізм забезпечення ресурсної спроможності сільських територій. *Теорія та практика державного управління*. 2016. Вип. 3(54). С. 172–177.
4. VoxUkraine. *Фактори стійкості громад під час війни: дослідження впливу економіки, управління та залученості*. 2023. URL: <https://voxukraine.org/factory-stijkosti-gromad-pid-chas-vijny-doslidzhennya-vplyvu-ekonomiky-upravlinnya-ta-zaluchenosti> (дата звернення: 20.04.2025).
5. Tiebout C.M. A Pure Theory of Local Expenditures. *Journal of Political Economy*. 1956. Vol. 64, No. 5. P. 416–424.
6. Програма «U-LEAD з Європою». URL: <https://u-lead.org.ua/ua> (дата звернення: 20.04.2025).
7. Фонд «Східна Європа». Програма підтримки розвитку місцевого самоврядування. URL: <https://eef.org.ua/what-we-do/local-development/> (дата звернення: 20.04.2025).
8. Інститут громадянського суспільства. Як громадам залучати інвестиції. URL: <https://www.csi.org.ua/news/yak-terytorialnij-gromadi-organizuvaty-robotu-iz-zaluchennya-investycij/> (дата звернення: 20.04.2025).
9. Шейко Ю.О. Стимулювання розвитку малого підприємництва в регіоні: автореф. дис. канд. екон. наук: 08.00.05. Луцьк, 2021. 20 с.
10. Овсяник О.М. Роль підприємництва в економічному розвитку регіонів України. *Бізнес Інформ*. 2020. № 12. С. 34–39.
11. Романюк І.А. Розвиток підприємництва та альтернативних видів діяльності сільського населення. *Економіка. Управління. Бізнес*. 2014. № 1. С. 117–122.
12. Котов І.В. Проблеми державного управління сталим розвитком територіальних громад в умовах кризових ситуацій. *Інвестиції: практика та досвід*. 2023. № 18. С. 216–220.
13. Про затвердження Державної стратегії регіонального розвитку на 2021–2027 роки : Постанова КМУ від 5 серпня 2020 р. № 695. URL: <https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text> (дата звернення: 29.03.2025).
14. Державна служба зайнятості. Програма мікрогрантів на створення або розвитку бізнесу. URL: <https://www.dcz.gov.ua/storinka/mikrohranty> (дата звернення: 20.04.2025).
15. GIZ. Підтримка громад у післявоєнному відновленні: міжнародний досвід та українські реалії. URL: <https://www.giz.de/en/worldwide/117182.html> (дата звернення: 20.04.2025).
16. Програма USAID DOBRE. Decentralization Offering Better Results and Efficiency. URL: <https://decentralization.gov.ua/dobre> (дата звернення: 20.04.2025).
17. Барський Ю.М., Поліщук В.Г. Фінансові інструменти стимулювання сталого розвитку регіону. *Економічні науки: збірник наукових праць Луцького національного технічного університету. Серія «Облік і фінанси»*. 2010. Вип. 7 (25). Ч. 4. С. 4–12.
18. Герасимчук З.В. Інституційні засади розвитку територіальних громад. *Економіка України*. 2015. № 9. С. 45–52.
19. Дорогунцов С.І. Регіональна економіка : підручник. К. : КНЕУ, 2001. 312 с.
20. Жаліло Я.А. Економічна політика держави: стратегічний підхід. К. : НІСД, 2012. 384 с.
21. Зайчикова В.В. Інституційна спроможність місцевого самоврядування в Україні. *Державне управління: теорія та практика*. 2018. № 1. С. 23–30.
22. Кириленко О.П. Фінансові основи місцевого самоврядування. К. : Центр учбової літератури, 2016. 240 с.
23. Луніна І.О. Місцеві бюджети в Україні: проблеми та шляхи їх вирішення. *Фінанси України*. 2005. № 1. С. 15–22.
24. Макаренко Л.М. Інституційна спроможність територіальних громад: теоретичні аспекти. *Регіональна економіка*. 2019. № 2. С. 112–120.
25. Слухай С.М. Бюджетна децентралізація: світовий досвід та українські реалії. К. : Інститут бюджету та соціально-економічних досліджень, 2014. 260 с.

References

1. Shvydyuk, S. (2017). "Sostoitel'naia terytorial'naia obshchina po-ukrains'ky: teoretychna model' i praktyka sozdaniya" [*Capable territorial community in Ukrainian: theoretical model and practice of creation*]. *Eastern Review*, 6, pp. 37–48.
2. Rose-Ackerman, S. (1999). *Corruption and Government: Causes, Consequences, and Reform*. Cambridge: Cambridge University Press.
3. Chernov, S. I., Mushchynska, N. Yu. (2016). Amalgamation of Territorial Communities as a Mechanism of Ensuring Resource Capability of Rural Areas. *Theory and Practice of Public Administration*, 3(54), pp. 172–177.
4. VoxUkraine (2023). "Faktyory stijkosti hromad pid chas viiny: doslidzhennia vplyvu ekonomiky, upravlinnia ta zaluchenosti" [*Factors of community resilience during war: study of the impact of economy, governance and engagement*]. URL: <https://voxukraine.org/factory-stijkosti-gromad-pid-chas-vijny-doslidzhennya-vplyvu-ekonomiky-upravlinnya-ta-zaluchenosti> (accessed 20 April 2025).

5. Tiebout C.M. A Pure Theory of Local Expenditures. *Journal of Political Economy*. 1956. Vol. 64, No. 5. P. 416–424.
6. U-LEAD with Europe Programme. URL: <https://u-lead.org.ua/ua> (accessed: 20 April 2025).
7. East Europe Foundation. Local Development Support Program. URL: <https://eef.org.ua/what-we-do/local-development/> (accessed: 20 April 2025).
8. Civil Society Institute. How Communities Can Attract Investment. URL: <https://www.csi.org.ua/news/yak-terytorialnij-gromadi-organizuvaty-robotu-iz-zaluchennya-investycij/> (accessed: 20 April 2025).
9. Sheiko, Yu. O. (2021). Stimulating the Development of Small Business in the Region: PhD Thesis. Lutsk.
10. Ovsyanik, O. M. (2020). The Role of Entrepreneurship in the Economic Development of the Regions of Ukraine. *Business Inform*, 12, pp. 34–39.
11. Romanyuk, I. A. (2014). Development of Entrepreneurship and Alternative Types of Rural Population Activity. *Economics. Management. Business*, 1, pp. 117–122.
12. Kotov, I. V. (2023). Problems of Public Administration of Sustainable Development of Territorial Communities in Crisis Situations. *Investments: Practice and Experience*, 18, pp. 216–220.
13. Cabinet of Ministers of Ukraine. (2020). On Approval of the State Regional Development Strategy for 2021–2027. Resolution No. 695. URL: <https://zakon.rada.gov.ua/laws/show/695-2020-п#Text> (accessed: 29 March 2025).
14. State Employment Service of Ukraine. (2025). Microgrants Programme for Business Creation and Development. URL: <https://www.dcz.gov.ua/storinka/mikrohranty> (accessed: 20 April 2025).
15. GIZ. (2024). Supporting Communities in Post-War Recovery: International Experience and Ukrainian Realities. URL: <https://www.giz.de/en/worldwide/117182.html> (accessed: 20 April 2025).
16. USAID DOBRE Program. Decentralization Offering Better Results and Efficiency. URL: <https://decentralization.gov.ua/dobre> (accessed: 20 April 2025).
17. Barskyi, Y. M. and Polishchuk, V. H. (2010). Financial Instruments for Stimulating Sustainable Regional Development. *Economic Sciences: Collection of Scientific Works of Lutsk National Technical University. Series "Accounting and Finance"*, 7(25), Part 4, pp. 4–12.
18. Herasymchuk, Z. V. (2015). Institutional Foundations for the Development of Territorial Communities. *Economy of Ukraine*, (9), pp. 45–52.
19. Dorohuntsov, S. I. (2001). *Regional Economy: Textbook*. Kyiv: KNEU.
20. Zhalilo, Ya. A. (2012). *State Economic Policy: Strategic Approach*. Kyiv: NISD.
21. Zaichykova, V. V. (2018). Institutional Capacity of Local Self-Government in Ukraine. *Public Administration: Theory and Practice*, (1), pp. 23–30.
22. Kyrylenko, O. P. (2016). *Financial Foundations of Local Self-Government*. Kyiv: Center for Educational Literature.
23. Lunina, I. O. (2005). Local Budgets in Ukraine: Problems and Solutions. *Finance of Ukraine*, (1), pp. 15–22.
24. Makarenko, L. M. (2019). Institutional Capacity of Territorial Communities: Theoretical Aspects. *Regional Economy*, (2), pp. 112–120.
25. Slukhai, S. M. (2014). *Budget Decentralization: Global Experience and Ukrainian Realities*. Kyiv: Institute for Budget and Socio-Economic Research.

Стаття надійшла до редакції 12.05.2025

Матвіїшин Євген Григорович

*доктор економічних наук,
професор кафедри регіонального та місцевого розвитку,
Національний університет «Львівська політехніка»*

Matviishyn Yevhen

*Doctor of Economic Sciences, Professor of the
Department of Regional and Local Development,
Lviv Polytechnic National University*

Маринчук Олександр Васильович

*студент ОП «Менеджмент просторового розвитку»
Національного університету «Львівська політехніка»*

Marynychuk Oleksandr

*Student of the Spatial Development Management Educational Program
Lviv Polytechnic National University*

DOI: 10.25313/2617-572X-2025-5-11020

РОЗВИТОК СИСТЕМ НАДАННЯ ПОСЛУГ ВОДОПОСТАЧАННЯ З ВИКОРИСТАННЯМ МЕХАНІЗМУ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА

DEVELOPMENT OF WATER SUPPLY SERVICE SYSTEMS USING THE PUBLIC-PRIVATE PARTNERSHIP MECHANISM

Анотація. Вступ. В Україні якісне водопостачання наразі охоплює лише 65% населення. Для досягнення цілей сталого розвитку актуальним є пошук ефективних рішень у сфері надання послуг водопостачання, зокрема через поєднання ресурсів державного і приватного секторів.

Мета. Метою дослідження є розкриття підходів до розвитку систем надання послуг водопостачання в Україні на засадах співпраці державного і приватного секторів.

Матеріали і методи. Матеріалами дослідження є: законодавство щодо водопостачання, розробки містобудівної документації, ведення підприємницької діяльності, державно-приватного партнерства, відновлення інфраструктури, а також публікації з питань співпраці державного і приватного секторів у різних країнах. У процесі дослідження було використано наступні методи: теоретичного узагальнення та групування (для характеристики систем водопостачання в містах і сільській місцевості); формалізації, аналізу та синтезу (для опису перешкод розвитку систем водопостачання, які зумовлені наявністю магістральних інженерно-транспортних споруд у межах громад, і новаціями законодавства щодо господарської діяльності в Україні); логічного узагальнення результатів (для формулювання висновків).

Результати. Забезпечення населення якісними послугами водопостачання вимагає від органів місцевого самоврядування впровадження раціональних підходів до розвитку відповідної інфраструктури. Це зокрема вимагає врахування положень комплексного плану просторового розвитку території громади або концепції інтегрованого розвитку, де визначено напрями використання територіальних ресурсів. Одним з можливих інструментів удосконалення водопостачання є залучення приватного сектора через договори державно-приватного партнерства або створення кооперативів, які можуть ефективно працювати для забезпечення водою віддалених населених пунктів або формування локальних підсистем у межах громади. Доцільним може бути об'єднання ресурсів кількох малих територіальних громад у межах міжмуніципального співробітництва для розподілу ризиків і спільної реалізації проєктів розвитку систем водопостачання.

Перспективи. Перспективним напрямом подальших досліджень є вивчення специфіки організації водопостачання в громадах, інфраструктура яких зазнала значних пошкоджень унаслідок воєнних дій.

Ключові слова: державний сектор, кооперативи, місцеве самоврядування, приватний сектор, просторовий розвиток, системи водопостачання, сталий розвиток.

Summary. Introduction. In Ukraine, high-quality water supply currently covers only 65% of the population. To achieve sustainable development goals, it is important to find effective solutions in the provision of water services, in particular by combining the resources of the public and private sectors.

Purpose. The aim of the study is to explore approaches to the development of water supply service systems in Ukraine based on public-private sector cooperation.

Materials and methods. The materials used in this study include legislation related to water supply, urban planning documentation, entrepreneurial activity, public-private partnerships, and infrastructure recovery, as well as publications on public-private cooperation in various countries. The following methods were employed in the research: theoretical generalization and classification (to characterize water supply systems in urban and rural areas); formalization, analysis, and synthesis (to describe the barriers to the development of water supply systems caused by the presence of major engineering and transport infrastructure within communities, as well as recent legislative innovations concerning economic activity in Ukraine); and logical generalization of results (to formulate conclusions).

Results. Ensuring access to high-quality water supply services requires local self-government bodies to implement rational approaches to the development of the relevant infrastructure. This, in particular, necessitates taking into account the provisions of the community's Comprehensive Spatial Development Plan or the Integrated Development Concept, which define the directions for the use of territorial resources. One possible instrument for improving water supply systems is the involvement of the private sector through public-private partnership agreements or the establishment of cooperatives, which may operate effectively in supplying remote settlements or in developing localized subsystems within a community. A reasonable solution may also involve pooling the resources of several small territorial communities within the framework of intermunicipal cooperation to distribute risks and jointly implement water supply development projects.

Discussion. A promising direction for further research is the study of the specific features of organizing water supply in communities whose infrastructure has suffered significant damage as a result of military operations.

Key words: public sector, cooperatives, local self-government, private sector, spatial development, water supply systems, sustainable development.

Постановка проблеми. В Україні задекларовано досягнення Цілей сталого розвитку та схвалено цільові значення й іншу інформацію за індикаторами досягнення на період до 2030 року [1]. Для цілі 6 «Чиста вода та належні санітарні умови» серед завдань її досягнення визначено «забезпечення доступу населення до послуг з централізованого питного водопостачання належної якості». За даними Рахункової палати України, централізованим водопостачанням забезпечено 65% населення країни, причому 98% міст та 23% сіл мають такі системи [2]. Централізоване водопостачання станом на 2021 рік було відсутнє у 16989 сільських населених пунктах [3, с. 64]. Російська військова агресія погіршила умови діяльності у сфері надання цих необхідних для добробуту населення послуг. Повоєнна відбудова, серед іншого, також вимагатиме пошуку дієвих підходів до розвитку систем надання послуг водопостачання для забезпечення цих базових потреб населення. Перспективним тут може стати поєднання зусиль і можливостей державного і приватного секторів, зокрема з використанням досвіду інших країн.

Аналіз останніх досліджень і публікацій. Згідно з результатами зарубіжних досліджень, у густонаселених регіонах оптимальним підходом до надання послуг з водопостачання та водовідведення є їх організація через комунальні підприємства, тоді як у сільській місцевості доцільніше використовувати кооперативні моделі управління

[4]. До речі, в Україні теж є приклади кооперативів із надання відповідних послуг [5], серед яких: питне водопостачання за допомогою пунктів розливу питної води (зокрема пересувних); питне водопостачання за допомогою індивідуальних і колективних пристроїв підготовки питної води; питне постачання через централізовані мережі водопостачання.

Організаційні підходи до водопостачання в європейських країнах значною мірою сформувалися під впливом історичних передумов і культурних особливостей. У звіті про проведене дослідження директор Інституту водних проблем та меліорації НААН України М. Яцюк зазначив, що умовно тут можна виокремити чотири основні моделі управління системами водопостачання [6, с. 67–68]:

1. *Модель прямого державного управління* характеризується тим, що усі функції з надання послуг і управління системами водопостачання здійснюються безпосередньо уповноваженим державним органом. Цей підхід був домінантним у більшості європейських країн у попередні десятиліття.

2. *Модель делегованого державного управління* передбачає, що органи державної влади призначають спеціалізованих управлінських суб'єктів для виконання відповідних функцій. При цьому такі суб'єкти зазвичай залишаються у державній (муніципальній) власності, хоча в окремих випадках у країнах Європейського Союзу допускається часткове приватне володіння корпоративними правами.

3. *Модель делегованого приватного управління* реалізується через укладення договорів між органами влади та приватними компаніями, які на визначений строк отримують право управляти водопровідно-каналізаційним господарством. Незважаючи на передачу функцій управління, власність на інфраструктуру зберігається за державними або муніципальними структурами.

4. *Модель прямого приватного управління* передбачає повну передачу повноважень щодо управління та власності на відповідні об'єкти приватним операторам. Державні органи в цьому випадку виконують виключно наглядові й регуляторні функції. Такий підхід реалізований лише в кількох європейських країнах, зокрема в Англії та Чехії.

У країнах Європи ефективне функціонування систем водопостачання та водовідведення в різних організаційних формах забезпечується завдяки їх ефективному просторовому розвитку, що сприяє підвищенню якості послуг. Словенські науковці підкреслюють, що крім матеріальних переваг (доступу до питної води), позитивними результатами спільного вирішення проблем забезпечення водою є нематеріальні ефекти, такі як зміцнення соціальної згуртованості громади та формування її ідентичності [7]. У США приблизно 2000 водопровідних і каналізаційних об'єктів експлуатувалися на засадах державно-приватного партнерства — спільними зусиллями приватних підприємств і муніципалітетів. Така співпраця взаємовигідна: у 2023 році 15 найбільших водоканалів у США інвестували майже 5,5 млрд. дол. у громадські водопровідні системи (ці кошти надійшли з приватного сектору, а не з муніципального бюджету) [8]. У країнах, що розвиваються, Світовий банк сприяв залученню інвестицій у проекти державно-приватного партнерства; зокрема у сектор водопостачання впродовж 2015–2020 років було залучено 4 млрд. дол. США на 46 проєктів [9, с. 54]. Загалом розглянуті дослідження підтверджують поширеність різноманітних форм надання послуг водопостачання в Україні та за кордоном через спільні зусилля державного і приватного секторів.

Виділення невирішених раніше частин загальної проблеми. Попри різноманітність способів доставки питної води споживачам комплексно вирішити завдання забезпечення доступу населення до послуг з централізованого питного водопостачання належної якості в Україні можливо через розвиток систем надання цих послуг у населених пунктах і територіальних громадах на засадах партнерства державного і приватного секторів. Особливу увагу потрібно приділити питанням розвитку цих систем в умовах децентралізації державної влади в Україні та з урахуванням наслідків російської збройної агресії.

Формулювання цілей статті. Метою дослідження є розкриття підходів до розвитку систем надання послуг водопостачання в Україні з використанням механізму державно-приватного партнерства.

Виклад основного матеріалу. Відповідно до законодавства, система питного водопостачання — це сукупність технічних засобів, включаючи мережі, споруди, устаткування (пристрої), для централізованого та нецентралізованого питного водопостачання [10]. Розвиток систем надання послуг водопостачання може утруднюватися різноманітними перешкодами — організаційними, географічними, нормативно-правовими, технічними тощо. Так, за відсутності технічних можливостей для надання послуг централізованого водопостачання виконавець послуги відмовляє у приєднанні. Можливість доступу до таких послуг в майбутньому визначається генеральним планом відповідного населеного пункту щодо систем централізованого питного водопостачання та централізованого водовідведення [11]. Відповідно до порядку розроблення містобудівної документації, генеральні плани населених пунктів входять до складу комплексного плану просторового розвитку території територіальної громади [12]. У цій документації, серед іншого, відображаються функціональні зони території конкретної громади. Тому розвиток систем надання послуг водопостачання пов'язаний також зі станом розробки в територіальних громадах генеральних планів населених пунктів і комплексного плану просторового розвитку території територіальної громади (далі — КППРТТГ), який одночасно відображає містобудівні обмеження та питання землекористування. Не всі територіальні громади підготували цей складний документ до встановленого терміну — 1 січня 2025 року. Через такий стан справ відповідно до законопроекту № 12283 [13] повсюдне впровадження комплексних планів просторового розвитку територій територіальних громад планують відтермінувати. Якщо територіальна громада не має затвердженого КППРТТГ, вважаємо за доцільне, щоб вона використовувала для планування розвитку систем водопостачання концепцію інтегрованого розвитку її території, яку формують із застосуванням принципів партисипації, міждисциплінарності та просторового представлення [14]. Цей документ можна сформулювати з меншими затратами часу та коштів і на його основі оцінити можливості використання територіальних ресурсів для розвитку водопровідних мереж у громаді.

Механізм державно-приватного партнерства в сфері надання послуг водопостачання ґрунтується на нормативно-правовій і методичній базі, яка в Україні вже достатньо розроблена та продовжує оновлюватися. Так, у зв'язку зі значними руйнуваннями через повномасштабне російське вторгнення та потребою у відбудові різноманітних об'єктів інфраструктури триває робота з реалізації плану відбудови для України. Зокрема було прийнято за основу проєкт Закону України «Про внесення змін до деяких законодавчих актів України щодо вдосконалення механізму залучення приватних інвестицій з використанням механізму державно-приватного

партнерства для пришвидшення відновлення зруйнованих війною об'єктів та будівництва нових об'єктів, пов'язаних з післявоєнною перебудовою економіки України», який включено до порядку денного сесії Верховної Ради України на 2025 рік [15]. Цей законопроект передбачає, серед іншого, впровадження типу проєктів державно-приватного партнерства, заснованих на платежах із бюджету, де держава не передає інвестору ризик попиту, умовно кажучи — оплачує «інфраструктуру в розстрочку» для післявоєнного відновлення України.

Доцільність застосування механізму державно-приватного партнерства в сфері водопостачання десятиліттями обговорюється вітчизняними і зарубіжними дослідниками (наприклад, огляд стану справ у різних країнах зробила І.І. Крилова [16], а узагальнення поглядів — Р. Байлі [17]). Основний аспект — чутливість до цього питання з погляду доступності цих послуг для різних верств населення. Прихильники залучення в цю сферу приватного сектора дотримуються погляду, що державно-приватне партнерство сприяє покращенню якості послуг і розширенню доступу, оскільки приватні компанії зазвичай володіють інноваційними підходами, сучасними технологіями та мають кращий менеджмент. Як аргументи прихильники наводять позитивні приклади реалізації відповідних проєктів у інших країнах, наприклад, у Франції [18], Австралії, США [19], низці країн Центрально-Східної Європи [20], деяких країн, що розвиваються, [21] тощо. Широку дискусію в Україні щодо долі комунальних підприємств (саме вони надають більшу частину послуг водопостачання) викликало прийняття на початку 2025 року Закону України «Про особливості регулювання підприємницької діяльності окремих видів юридичних осіб та їх об'єднань у перехідний період» [22]. Відповідно до коментаря Верховної Ради України, цей законодавчий акт значно розширює можливості територіальних громад: «Закон дозволяє громадам створювати юридичні особи для забезпечення ефективного управління власністю та реалізації соціальних ініціатив. ... дозволяє громадам по всій території України гнучко використовувати корпоратизацію як інструмент для: залучення міжнародних інвесторів до участі в капіталі; модернізації основних засобів; отримання кредитування за європейськими ставками для корпоратизованих підприємств» [23]. Експерти й раніше розглядали подібні напрями підвищення ефективності роботи комунальних підприємств [24, с. 10]: приватизацію їх активів, передачу в концесію чи використання інших інструментів державно-приватного партнерства, реформу корпоративного управління і трансформацію в іншу організаційно-правову форму.

В Україні є позитивні приклади залучення приватного сектора до надання послуг водопостачання. Так, у грудні 2003 року Одеська міська рада передала цілісний майновий комплекс водоканалу

в оренду на 49 років приватній структурі — ТОВ «Інфокс». Утворення «Інфоксводоканалу» стало першим в Україні прикладом оренди комунального підприємства приватним інвестором [25]. Прикладом використання концесійних угод в галузі водопостачання є укладання у 2008 році такої угоди між Бердянською міською радою та ТОВ «Чиста вода — Бердянськ» (концесіонер) про надання в управління майна цілісного майнового комплексу ДКП «Бердянський міськводоканал» терміном на 30 років. Щоправда, у 2011 році угоду було розірвано [26]. Це свідчить про необхідність вираженого підходу як до укладання договорів ДПП, так і до контролю за діяльністю в межах таких договорів.

Особлива увага до проблем водопостачання на рівні територіальних громад почала приділятися під час і після проведення реформи децентралізації державної влади в Україні: постало завдання налагодити належне управління та розвиток розрізних систем водопостачання. Територіальні громади, що об'єднали численні населені пункти на значних відстанях, зіткнулися з викликом забезпечення якісного надання послуг з водопостачання, а подекуди і з несанкціонованим споживанням води. Тому для підвищення ефективності підприємств, які надають послуги з водопостачання, забезпечення стабільної доставки води мешканцям сільських територій, раціонального використання водних ресурсів потрібно постійно приділяти увагу технічному оновленню цих систем, застосовувати передові технології, зокрема автоматизацію. Наприклад, проблему несанкціонованого споживання води в громадах можна вирішити через локалізований збір даних і встановлення додаткових лічильників на окремих вулицях чи гілках водопровідної мережі. Це дає змогу диспетчерам, аналізуючи зібрані дані, виявляти зони з найбільшими втратами води.

Перешкодою розвитку системи водопостачання в територіальній громаді може бути фізична неможливість об'єднати водопроводи в одну мережу. Наприклад, через територію громади можуть проходити магістральні інженерно-технічні споруди, в межах яких не дозволяються роботи з прокладання труб. На рис. 1 наведено приклад території Бібрської міської територіальної громади (Львівська область), яку перетинають два міжнародні трубопроводи й одна лінія електропередач (ЛЕП-750). Таке розташування зумовлює потребу вирішення проблеми водопостачання населених пунктів громади відокремленими мережами з власними джерелами води. Тут може виявитися доцільною організація надання послуг в кількох групах населених пунктів окремими підсистемами водопостачання через утворення кооперативів. За суттю, це теж є залученням приватного сектора до вирішення суспільної проблеми.

Для малих територіальних громад доцільним є застосування підходу, за якого фінансове навантаження та потенційні ризики реалізації проєктів

розподіляються між кількома громадами. Інституційною основою для такого механізму може слугувати Закон України «Про співробітництво територіальних громад», який у статті 14 передбачає можливість створення спільного органу управління у формі департаменту, управління, відділу тощо [27]. За участю приватного учасника за договором, укладеним в рамках державно-приватного партнерства, територіальні громади зможуть швидше отримати доступ до важливих об'єктів інфраструктури, підвищити якість життя та залучити нові інвестиції. Важливо, щоб такі проекти були ретельно плановані та враховували просторово-географічні умови конкретного регіону і територіальних громад, а також їх повоєнний стан.

Висновки із цього дослідження і подальші перспективи в цьому напрямку. Виконання завдання забезпечення доступу населення до послуг з централізованого питного водопостачання належ-

ної якості вимагає від органів місцевого самоврядування пошуку раціональних способів розвитку систем надання послуг водопостачання. При цьому потрібно опиратися на містобудівну документацію, яка визначає функціональні зони територій громад. Якщо територіальна громада не має розробленого комплексного плану просторового розвитку її території, то на період до його затвердження запропоновано брати до уваги простіший документ — концепцію інтегрованого розвитку території громади, де визначаються можливості використання територіальних ресурсів. Залучення приватного сектора до надання послуг водопостачання може здійснюватися за договорами державно-приватного партнерства та через утворення кооперативів. Другий варіант може бути доцільнішим, якщо потрібно забезпечити водопостачанням віддалені населені пункти громади, або якщо організовуються окремі підсистеми водопостачання в межах громади. Враховуючи, що

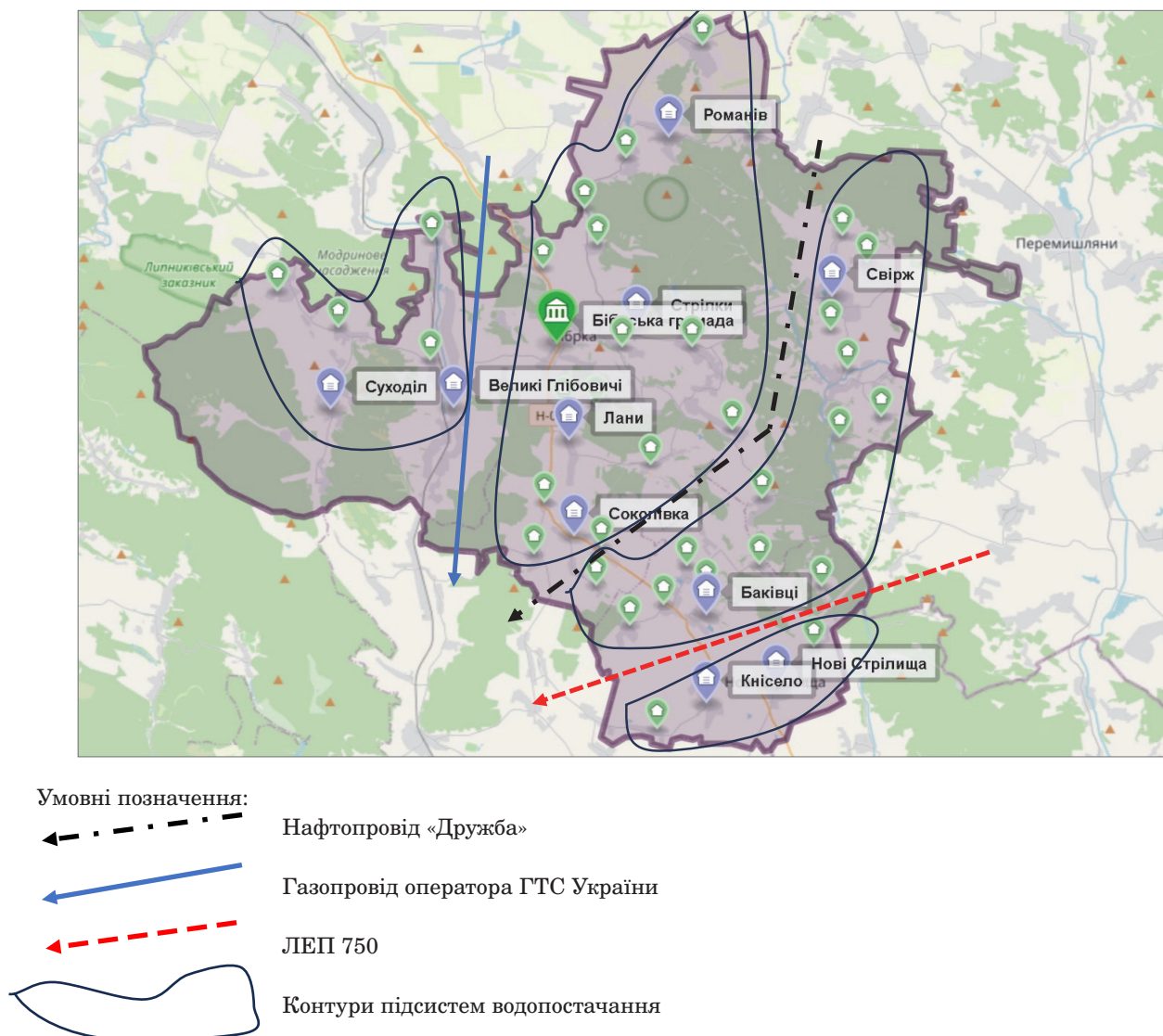


Рис. 1. Варіант майбутнього просторового розвитку системи водопостачання у Бібрській міській територіальній громаді з утворенням чотирьох підсистем

Джерело: узагальнено авторами

для приватного партнера привабливішими є масштабні проекти, малі територіальні громади можуть об'єднати ресурси для організації спільної системи водопостачання, опираючись на положення статті 14 Закону України «Про співробітництво територіальних громад», що дає можливість розподілити потенційні ризики реалізації проектів державно-

приватного партнерства між кількома громадами та приватним партнером. Напрямами подальших досліджень можуть стати особливості надання послуг водопостачання в територіальних громадах, які зазнали значних руйнувань інфраструктури внаслідок російської збройної агресії та віднесені до територій відновлення.

Література

1. Деякі питання забезпечення досягнення Цілей сталого розвитку в Україні : розпорядження Кабінету Міністрів України від 29 листопада 2024 р. № 1190-п/ URL: <https://zakon.rada.gov.ua/laws/show/1190-2024-%D1%80#Text> (дата звернення: 16.05.2025).
2. Звіт про результати аудиту ефективності виконання заходів, спрямованих на досягнення цілі 6 «Забезпечення доступності та сталого управління водними ресурсами та санітарією» Цілей сталого розвитку України на період до 2030 року. Затверджений рішенням Рахункової палати від 06.06.2023 № 12–7Р. URL: <https://rp.gov.ua/FinControl/FinReports/?id=1246> (дата звернення: 16.05.2025).
3. Спільний звіт за 2024 рік про результати координованого аудиту щодо Цілі 6 Цілей сталого розвитку Організації Об'єднаних Націй, схвалений Рішенням Рахункової палати від 05.11.2024 № 51-1. URL: https://rp.gov.ua/upload-files/IntCooperation/IntAudits/2024/SDG6_JR_ua.pdf (дата звернення: 16.05.2025).
4. Deane B., Mac Domhnaill B. The Alliance of Community-Owned Water Services in Europe: Opportunities and Challenges Based on the Irish Perspective. *Water*. 2021. 13(22). 3181. <https://doi.org/10.3390/w13223181>.
5. Обслуговуючий кооператив «Дашковецьке джерело». URL: <https://www.dashkovetske-dzherelo.com.ua/about> (дата звернення: 16.05.2025).
6. Яцюк М. Проведення досліджень з підвищення ефективності управління водними ресурсами і системами водопостачання/водовідведення та розробка аналітичної записки для уряду України. Звіт. Київ : Українська Водна Асоціація, 2023. 104 с. URL: https://ukrainian-water-association.org/wp-content/uploads/2023/07/UWA_Water_Management_Report.pdf (дата звернення: 16.05.2025).
7. Pipan P., Šmid Hribar M., Urbanc M. Motivation, robustness and benefits of water commons: Insights from small drinking water supply systems. *Acta geographica Slovenica*. 2023. 63–3. <https://doi.org/10.3986/AGS.11592>.
8. Benefits of working with a water company. *National Association of Water Companies*. URL: <https://nawc.org/resources/benefits-of-working-with-a-water-company/> (дата звернення: 16.05.2025).
9. Круглов В. Розвиток системи державно-приватного партнерства в сучасних умовах. *Науковий вісник: Державне управління*. 2021. № 3(9). С. 50–67. [https://doi.org/10.32689/2618-0065-2021-3\(9\)-50-67](https://doi.org/10.32689/2618-0065-2021-3(9)-50-67).
10. Про питну воду та питне водопостачання : Закон України від 10 січня 2002 року № 2918-III (назва Закону в редакції Закону № 2887-IX від 12.01.2023). URL: <https://zakon.rada.gov.ua/laws/show/2918-14#Text> (дата звернення: 16.05.2025).
11. Правила користування системами централізованого питного водопостачання та централізованого водовідведення в населених пунктах України (у редакції наказу Міністерства розвитку громад та територій України від 19 квітня 2021 року № 97). URL: <https://zakon.rada.gov.ua/laws/show/z0936-08#Text> (дата звернення: 16.05.2025).
12. Порядок розроблення, оновлення, внесення змін та затвердження містобудівної документації, постановою Кабінету Міністрів України від 1 вересня 2021 р. № 926 (в редакції постанови Кабінету Міністрів України від 31 грудня 2024 р. № 1557). URL: <https://zakon.rada.gov.ua/laws/show/1557-2024-%D0%BF#Text> (дата звернення: 16.05.2025).
13. Проект Закону про внесення змін до деяких законів України щодо продовження термінів дії документів з планування територій № 12283 від 3 грудня 2024 р. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/45368> (дата звернення: 16.05.2025).
14. Порядок формування Концепції інтегрованого розвитку території територіальної громади, затверджений Наказом Міністерства розвитку громад та територій України 22 вересня 2022 року № 172. URL: <https://zakon.rada.gov.ua/laws/show/z1421-22#Text> (дата звернення: 16.05.2025).
15. Проект Закону про внесення змін до деяких законодавчих актів України щодо вдосконалення механізму залучення приватних інвестицій з використанням механізму державно-приватного партнерства для пришвидшення відновлення зруйнованих війною об'єктів та будівництва нових об'єктів, пов'язаних з післявоєнною перебудовою економіки України. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=7508&conv=9> (дата звернення: 16.05.2025).
16. Крилова І.І. Управління у сфері водопостачання та водовідведення. Світовий досвід. *Публічне управління і адміністрування в Україні*. 2019. 9. С. 44–52. URL: <https://pag-journal.iei.od.ua/archives/2019/9-2019/10.pdf> (дата звернення: 16.05.2025).
17. Bailey R. Water is a human right. How privatization gets water to the poor. *Reason*. 2005. URL: <https://reason.com/2005/08/17/water-is-a-human-right/> (дата звернення: 16.05.2025).

18. Neto F. Water privatization and regulation in England and France: a tale of two models. *Natural Resources Forum*. 1998. 22 (2). 107–117. URL: <https://doi.org/10.1111/j.1477-8947.1998.tb00718.x>.
19. Wheeler S., Loch A., Crase L., Young M., Grafton R. Developing a Water Market Readiness Assessment Framework. *Journal of Hydrology*. 2017. 552. <https://doi.org/10.1016/j.jhydrol.2017.07.010>.
20. Винницький Б., Лендзель М., Онищук Б., Серварі П. Досвід та перспективи впровадження державно-приватних партнерств в Україні та за кордоном. Київ : «К.І.С.», 2008. 146 с. URL: https://regionet.org.ua/files/PPP_Report_CIDA_2008_ua.pdf (дата звернення: 16.05.2025).
21. Segerfeldt F. Private Water Saves Lives. CATO Institute. 2005. URL: <https://www.cato.org/commentary/private-water-saves-lives> (дата звернення: 16.05.2025).
22. Про особливості регулювання підприємницької діяльності окремих видів юридичних осіб та їх об'єднань у перехідний період : Закон України від 9 січня 2025 року № 4196-IX. URL: <https://zakon.rada.gov.ua/laws/show/4196-20#Text> (дата звернення: 21.05.2025).
23. Парламент ухвалив Закон про особливості регулювання підприємницької діяльності окремих видів юридичних осіб та їх об'єднань у перехідний період (реєстр. № 6013). Прес-служба Апарату Верховної Ради України. 9 січня 2025 року. URL: <https://www.rada.gov.ua/news/razom/257481.html> (дата звернення: 16.05.2025).
24. Прохоров Б., Лонецький О., Вартовник І. Як побороти неефективність комунальних підприємств? Аналітична записка. *Центр економічної стратегії*. 2020. 43 с. URL: <https://ces.org.ua/wp-content/uploads/2020/08/> (дата звернення: 16.05.2025).
25. Одеському водоканалу — 150 років! *Одеське життя*. 22.09.2023. URL: <https://odessa-life.od.ua/uk/news-uk/odeskomu-vodokanalu-150-rokiv> (дата звернення: 16.05.2025).
26. Про анулювання ліцензії на право провадження діяльності з централізованого водопостачання та водовідведення, виданої ТОВ «Чиста вода — Бердянськ»: постанова Національної комісії регулювання електроенергетики України від 17 червня 2011 року № 1059. URL: <https://zakon.rada.gov.ua/rada/show/v1059227-11#Text> (дата звернення: 16.05.2025).
27. Про співробітництво територіальних громад : Закон України від 17 червня 2014 року № 1508-VII. URL: <https://zakon.rada.gov.ua/laws/show/1508-18#Text> (дата звернення: 21.05.2025).

References

1. Deiaki pytannia zabezpechennia dosiahnennia Tsilei staloho rozvytku v Ukraini: rozporiadzhennia Kabinetu Ministriv Ukrainy vid 29 lystopada 2024 r. № 1190-p/. URL: <https://zakon.rada.gov.ua/laws/show/1190-2024-%D1%80#Text> [in Ukrainian].
2. Zvit pro rezultaty audytu efektyvnosti vykonannya zakhodiv, spriamovanykh na dosiahnennia tsili 6 “Zabezpechennia dostupnosti ta staloho upravlinnia vodnymy resursamy ta sanitariieiu” Tsilei staloho rozvytku Ukrainy na period do 2030 roku. Zatverdzhnyi rishenniam Rakhunkovoi palaty vid 06.06.2023 № 12-7P. URL: <https://rp.gov.ua/FinControl/FinReports/?id=1246> [in Ukrainian].
3. Spilnyi zvit za 2024 rik pro rezultaty koordynovanoho audytu shchodo Tsili 6 Tsilei staloho rozvytku Orhanizatsii Obiednanykh Natsii, skhvalenyi Rishenniam Rakhunkovoi palaty vid 05.11.2024 № 51-1. URL: https://rp.gov.ua/upload-files/IntCooperation/IntAudits/2024/SDG6_JR_ua.pdf [in Ukrainian].
4. Deane, B. & Mac Domhnaill, B. The Alliance of Community-Owned Water Services in Europe: Opportunities and Challenges Based on the Irish Perspective. *Water*. 2021. 13(22). 3181. <https://doi.org/10.3390/w13223181>.
5. Obsluhovuiuchy kooperatyv “Dashkovetske dzherelo”. URL: <https://www.dashkovetske-dzherelo.com.ua/about> [in Ukrainian].
6. Yatsiuk, M. Provedennia doslidzhen z pidvyshchennia efektyvnosti upravlinnia vodnymy resursamy i systemamy vodopostachannia/vodovidvedennia ta rozrobka analitychnoi zapysky dlia uriadu Ukrainy. Zvit. Kyiv: Ukrainska Vodna Asotsiatsiia, 2023. 104 p. URL: https://ukrainian-water-association.org/wp-content/uploads/2023/07/UWA_Water_Management_Report.pdf [in Ukrainian].
7. Pipan, P., Šmid Hribar, M. & Urbanc, M. Motivation, robustness and benefits of water commons: Insights from small drinking water supply systems. *Acta geographica Slovenica*. 2023. 63-3. <https://doi.org/10.3986/AGS.11592>.
8. Benefits of working with a water company. *National Association of Water Companies*. URL: <https://nawc.org/resources/benefits-of-working-with-a-water-company/>.
9. Kruhlov, V. Rozvytok systemy derzhavno-pryvatnoho partnerstva v suchasnykh umovakh. *Naukovyi visnyk: Derzhavne upravlinnia*. 2021. № 3(9). Pp. 50–67. URL: [https://doi.org/10.32689/2618-0065-2021-3\(9\)-50-67](https://doi.org/10.32689/2618-0065-2021-3(9)-50-67) [in Ukrainian].
10. Pro pytnu vodu ta pytne vodopostachannia: Zakon Ukrainy vid 10 sichnia 2002 roku № 2918-III (nazva Zakonu v redaktsii Zakonu № 2887-IX vid 12.01.2023). URL: <https://zakon.rada.gov.ua/laws/show/2918-14#Text> [in Ukrainian].
11. Pravyla korystuvannia systemamy tsentralizovanoho pytnoho vodopostachannia ta tsentralizovanoho vodovidvedennia v naselenykh punktakh Ukrainy (u redaktsii nakazu Ministerstva rozvytku hromad ta terytorii Ukrainy vid 19 kvitnia 2021 roku № 97). URL: <https://zakon.rada.gov.ua/laws/show/z0936-08#Text> [in Ukrainian].
12. Poriadok rozroblennia, onovlennia, vnesennia zmin ta zatverdzhennia mistobudivnoi dokumentatsii, postanovoi Kabinetu Ministriv Ukrainy vid 1 veresnia 2021 r. № 926 (v redaktsii postanovy Kabinetu Ministriv Ukrainy vid 31 hrudnia 2024 r. № 1557). URL: <https://zakon.rada.gov.ua/laws/show/1557-2024-%D0%BF#Text> [in Ukrainian].

13. Projekt Zakonu pro vnesennia zmin do deiakyykh zakoniv Ukrainy shchodo prodovzhennia terminiv dii dokumentiv z planuvannia terytorii № 12283 vid 3 hrudnia 2024 r. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/45368> [in Ukrainian].
14. Poriadok formuvannia Kontseptsii intehrovanooho rozvytku terytorii terytorialnoi hromady, zatverdzhenyi Nakazom Ministerstva rozvytku hromad ta terytorii Ukrainy 22 veresnia 2022 roku № 172. URL: <https://zakon.rada.gov.ua/laws/show/z1421-22#Text> [in Ukrainian].
15. Proekt Zakonu pro vnesennia zmin do deiakyykh zakonodavchykh aktiv Ukrainy shchodo vdoskonalennia mekhanizmu zaluchennia pryvatnykh investytsii z vykorystanniam mekhanizmu derzhavno-pryvatnoho partnerstva dlia pryshvydshennia vidnovlennia zruinovanykh viinoiu ob'ektiv ta budivnytstva novykh ob'ektiv, poviazanykh z pisliavoiennoiu perebudovoiu ekonomiky Ukrainy. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=7508&conv=9> [in Ukrainian].
16. Krylova, I. I. Upravlinnia u sferi vodopostachannia ta vodovidvedennia. Svitovyi dosvid. *Publichne upravlinnia i administruvannia v Ukraini*. 2019. 9. Pp. 44–52. URL: <https://pag-journal.iei.od.ua/archives/2019/9-2019/10.pdf> [in Ukrainian].
17. Bailey, R. Water is a human right. How privatization gets water to the poor. *Reason*. 2005. URL: <https://reason.com/2005/08/17/water-is-a-human-right/>.
18. Neto, F. Water privatization and regulation in England and France: a tale of two models. *Natural Resources Forum*. 1998. 22 (2). 107–117. <https://doi.org/10.1111/j.1477-8947.1998.tb00718.x>.
19. Wheeler, S., Loch, A., Crase, L., Young, M. & Grafton, R. Developing a Water Market Readiness Assessment Framework. *Journal of Hydrology*. 2017. 552. <https://doi.org/10.1016/j.jhydrol.2017.07.010>.
20. Vynnytskyi B., Lendel M., Onyshchuk B., Sehvari P. Dosvid ta perspektyvy vprovadzhennia derzhavno-pryvatnykh partnerstv v Ukraini ta za kordonom. Kyiv: "K.I.S.", 2008. 146 p. URL: https://regionet.org.ua/files/PPP_Report_CIDA_2008_ua.pdf [in Ukrainian].
21. Segerfeldt, F. Private Water Saves Lives. CATO Institute. 2005. URL: <https://www.cato.org/commentary/private-water-saves-lives>.
22. Pro osoblyvosti rehuliuвання pidpriemnytskoi diialnosti okremykh vydiv yurydychnykh osib ta yikh obiednan u perekhidnyi period: Zakon Ukrainy vid 9 sichnia 2025 roku № 4196-IX. URL: <https://zakon.rada.gov.ua/laws/show/4196-20#Text> [in Ukrainian].
23. Parlament ukhvalyv Zakon pro osoblyvosti rehuliuвання pidpriemnytskoi diialnosti okremykh vydiv yurydychnykh osib ta yikh obiednan u perekhidnyi period (reiestr. № 6013). Pres-sluzhba Aparatu Verkhovnoi Rady Ukrainy. 9 sichnia 2025 roku. URL: <https://www.rada.gov.ua/news/razom/257481.html> [in Ukrainian].
24. Prokhorov B., Lonevskyi O., Vartovnyk I. Yak poboroty neefektyvnist komunalnykh pidpriemstv? Analitychna zapyska. *Tsentr ekonomichnoi stratehii*. 2020. 43 p. URL: <https://ces.org.ua/wp-content/uploads/2020/08/>.
25. Odeskomu vodokanal — 150 rokiv! *Odeske zhyttia*. 22.09.2023. URL: <https://odessa-life.od.ua/uk/news-uk/odeskomu-vodokanal-150-rokiv> [in Ukrainian].
26. Pro anuliuвання litsenzii na pravo provadzhennia diialnosti z tsentralizovanoho vodopostachannia ta vodovidvedennia, vydanoi TOV "Chysta voda — Berdiansk": postanova Natsionalnoi komisii rehuliuвання elektroenerhetyky Ukrainy vid 17 chervnia 2011 roku № 1059. URL: <https://zakon.rada.gov.ua/rada/show/v1059227-11#Text> [in Ukrainian].
27. Pro spivrobitnytstvo terytorialnykh hromad: Zakon Ukrainy vid 17 chervnia 2014 roku № 1508-VII. URL: <https://zakon.rada.gov.ua/laws/show/1508-18#Text> [in Ukrainian].

Стаття надійшла до редакції 23.05.2025

Марискевич Андрій Тарасович

*аспірант кафедри економіки та публічного управління
Львівського національного університету імені Івана Франка*

Maryskevych Andrii

*Postgraduate Student of the Department of Economics and Public Administration
Ivan Franko National University of Lviv*

ORCID: 0009-0002-0585-2889

DOI: 10.25313/2617-572X-2025-5-10958

ПУБЛІЧНЕ УПРАВЛІННЯ СТАЛИМ РОЗВИТКОМ РЕГІОНІВ

PUBLIC MANAGEMENT OF SUSTAINABLE DEVELOPMENT OF REGIONS

Анотація. Вступ. Забезпечення сталого розвитку регіонів в умовах сучасних трансформацій українського суспільства має спиратися на ефективне публічне управління, здатне збалансувати економічні, соціальні та екологічні пріоритети. Зростаюча складність суспільно-економічних процесів актуалізує питання формування нової моделі взаємодії між державою, громадою та природним середовищем. Це передбачає впровадження інноваційних механізмів управління, спрямованих на зміцнення інституційної спроможності органів публічної влади та посилення участі громадськості в ухваленні рішень. Таким чином, публічне управління виступає не лише координатором економічного зростання, а й рушієм сталих змін, що мають забезпечити довгострокову перспективу розвитку українських регіонів.

Матеріали і методи. Матеріалами дослідження є наукові публікації українських і зарубіжних дослідників, присвячені проблематиці сталого розвитку, децентралізації та публічного управління у сфері регіонального розвитку.

У процесі дослідження використано загальнонаукові та спеціальні методи: аналіз і синтез, порівняльний метод, метод прогнозування.

Мета статті. Дослідити роль публічного управління у забезпеченні економічного зростання та сталого розвитку регіонів України в умовах сучасних викликів, охарактеризувати основні управлінські механізми, що сприяють реалізації політики регіонального розвитку. Завдання: розкрити поняття сталого розвитку у контексті публічного управління; проаналізувати основні інструменти та механізми публічного управління, спрямовані на забезпечення економічного зростання регіонів; оцінити вплив децентралізації та стратегічного планування на сталий розвиток територій; визначити напрями удосконалення публічного управління з метою забезпечення збалансованого розвитку регіонів.

Аналіз останніх досліджень та публікацій. Вагомий внесок у дослідження в сфері публічного управління сталим розвитком регіонів зробили такі науковці: Комаха Л. [8], Мовчанюк А. [10], Sachs J. [3], Павленко О. [12], Рагімов Ф. [13], Капінос Г. [7], Ларіонова К. [7] та інші.

Результати. Сталий розвиток розглядається як новітня концептуальна основа модернізації системи публічного управління в Україні, що трансформує традиційну адміністративну модель у напрямі орієнтації на довгострокову збалансованість економічних, соціальних та екологічних цілей. У результаті дослідження виявлено, що сучасні виклики – війна, внутрішнє переміщення населення, руйнація інфраструктури – вимагають переосмислення ролі публічного управління у забезпеченні регіонального розвитку.

Запропоновано розглядати публічне управління сталим розвитком регіонів як комплексний процес, що включає стратегічне планування, просторову інтеграцію, інституційне забезпечення та участь громадськості.

Запропоновано модель публічного управління сталим розвитком регіонів, яка базується на чотирьох ключових компонентах: інституційному, фінансовому, соціальному та технологічному. Кожен із цих компонентів є взаємопов'язаним та взаємодіє для забезпечення сталого розвитку, зокрема через зміцнення інституційної спроможності на всіх рівнях управління, активне залучення фінансових ресурсів, підтримку соціальних ініціатив та впровадження технологічних інновацій.

Перспективним напрямом подальших досліджень у межах цієї тематики є аналіз реалізації цілей сталого розвитку крізь призму сучасних викликів, зокрема в умовах воєнного стану, постконфліктного відновлення, кліматичних змін та демографічної кризи.

Ключові слова: публічне управління, сталий розвиток, економічне зростання, цілі сталого розвитку, складові сталого розвитку, регіональний розвиток, державна політика, органи влади, місцеве самоврядування.

Summary. Introduction. Ensuring sustainable development of regions in the conditions of modern transformations of Ukrainian society should be based on effective public administration, capable of balancing economic, social and environmental priorities. The growing complexity of socio-economic processes actualizes the issue of forming a new model of interaction between the state, community and the natural environment. This involves the introduction of innovative management mechanisms aimed at strengthening institutional support for public authorities and increasing public participation in decision-making. Thus, public administration acts not only as a coordinator of economic growth, but also as a destroyer of sustainable changes that have a sufficiently long-term perspective for the development of Ukrainian regions.

Materials and methods. The materials of the study are scientific publications of Ukrainian and foreign researchers devoted to the issues of sustainable development, decentralization and public administration in the field of regional development.

The study used general scientific and special methods: analysis and synthesis, comparative method, forecasting method.

The purpose of the article. To investigate the role of public administration in ensuring economic growth and sustainable development of the regions of Ukraine in the face of modern challenges, to characterize the main management mechanisms that contribute to the implementation of regional development policy. Tasks: to reveal the concept of sustainable development in the context of public administration; to analyze the main tools and mechanisms of public administration aimed at ensuring economic growth of regions; to assess the impact of decentralization and strategic planning on the sustainable development of territories; to identify areas for improving public administration in order to ensure balanced development of regions.

Analysis of recent research and publications. A significant contribution to research in the field of public administration for sustainable development of regions was made by the following scientists: Komakha L. [8], Movchanyuk A. [10], Sachs J. [3], Pavlenko O. [12], Ragimov F. [13], Kapinos G. [7], Larionova K. [7] and others.

Results. Sustainable development is considered as the newest conceptual basis for the modernization of the public administration system in Ukraine, which transforms the traditional administrative model towards a long-term balance of economic, social and environmental goals. The study revealed that modern challenges – war, internal population displacement, destruction of infrastructure – require a rethinking of the role of public administration in ensuring regional development.

It is proposed to consider public administration of sustainable development of regions as a complex process that includes strategic planning, spatial integration, institutional support and public participation.

A model of public governance for sustainable regional development is proposed, which is based on four key components: institutional, financial, social, and technological. Each of these components is interconnected and interacts to ensure sustainable development, in particular through strengthening institutional capacity at all levels of government, active involvement of financial resources, support for social initiatives, and implementation of technological innovations.

A promising direction for further research within this topic is the analysis of the implementation of sustainable development goals through the prism of modern challenges, in particular in the context of martial law, post-conflict recovery, climate change and demographic crisis.

Key words: public administration, sustainable development, economic growth, sustainable development goals, components of sustainable development, regional development, state policy, authorities, local government.

Постановка проблеми. У сучасних умовах публічне управління відіграє ключову роль у формуванні стратегічних пріоритетів розвитку держави, зокрема на регіональному рівні. Економічне зростання та сталий розвиток регіонів України залежать від здатності органів публічної влади ефективно реалізовувати управлінські рішення з урахуванням соціально-економічної специфіки територій, ресурсного потенціалу та екологічних обмежень. Проте на практиці спостерігається нерівномірність регіонального розвитку, низька ефективність використання стратегічних документів, обмеженість інституційної спроможності місцевих органів влади, а також слабка інтеграція принципів сталого розвитку у систему публічного управління. В умовах воєнного стану, посилення соціально-економічних викликів і необхідності післявоєнного відновлення особливої актуальності набуває питання удосконалення механізмів публічного управління, які здатні забезпечити збалансований розвиток регіонів на довгострокову перспективу. Це зумовлює необхідність наукового переосмислення ролі публічного управлін-

ня як ключового інструмента впливу на регіональні процеси зростання і трансформації.

Мета статті. Дослідити роль публічного управління у забезпеченні економічного зростання та сталого розвитку регіонів України в умовах сучасних викликів, охарактеризувати основні управлінські механізми, що сприяють реалізації політики регіонального розвитку. Мета статті передбачає наступні **завдання**: розкрити поняття сталого розвитку у контексті публічного управління; проаналізувати основні інструменти та механізми публічного управління, спрямовані на забезпечення економічного зростання регіонів; оцінити вплив децентралізації та стратегічного планування на сталий розвиток територій; визначити напрями удосконалення публічного управління з метою забезпечення збалансованого розвитку регіонів.

Аналіз останніх досліджень та публікацій. Вагомий внесок у дослідження в сфері публічного управління сталим розвитком регіонів зробили такі науковці: Комаха Л. [8] (використано підходи до розгляду еволюції концепції сталого розвитку в дискурсі

публічного управління, зокрема наголошено на територіальній специфіці як ключовому вимірі сучасних стратегій), Мовчанюк А. [10] (висловлено ідею про публічне управління як стратегічний інструмент формування сталості територій та інтегрування Цілей сталого розвитку у місцеву політику), Sachs J. [3] (виокремлено фундаментальні положення про взаємозв'язок між економічним зростанням, соціальною інклюзією та екологічною стабільністю як основу сучасного розуміння сталого розвитку), Павленко О. [12] (висвітлено інституційне забезпечення регіонального управління, зокрема в контексті децентралізації та підвищення ролі місцевих органів влади), Рагімов Ф. [13] (сформульовано підходи до відновлення регіонів у повоєнний період як бази для формування нової парадигми публічного управління в умовах криз і трансформацій), Капінос Г. [7] та Ларіонова К. [7] (обґрунтовано необхідність посилення інституційної спроможності державного управління сталим розвитком, що відображено у побудові моделі багаторівневого управління).

Матеріали і методи. Матеріалами дослідження є наукові публікації українських і зарубіжних дослідників, присвячені проблематиці сталого розвитку, децентралізації та публічного управління у сфері регіонального розвитку.

У процесі дослідження використано загальнонаукові та спеціальні методи: аналіз і синтез, порівняльний метод, метод прогнозування.

Виклад основного матеріалу. Сталий розвиток регіонів як об'єкт публічного управління є складним багатовимірним процесом, який передбачає гармонійне поєднання соціальної, економічної та екологічної складових. У світовій практиці сталий розвиток закріплено як стратегічний орієнтир державної політики, що забезпечує збалансоване використання ресурсів, соціальну справедливість і довгострокову екологічну безпеку [3].

Багров М. трактує сталий розвиток як «...гармонізацію співвіднесень трьох підсистем системи цивілізації — соціуму, економіки та довкілля» [6].

Більш розширене трактування визначення сталого розвитку простежується у працях О. Ханової, зокрема дослідник трактує його як «...систему взаємоузгоджених управлінських, економічних, соціальних, природоохоронних заходів, спрямованих на формування системи суспільних відносин на засадах довіри, партнерства, солідарності, консенсусу, етичних цінностей, безпечного навколишнього середовища, національних джерел духовності» [15]

Концепція сталого розвитку в державному управлінні — це стратегічний підхід, спрямований на забезпечення збалансованого зростання суспільства, збереження природних ресурсів та підвищення якості життя мешканців [8].

Доцільно звернути увагу на те, що одним із головних завдань публічного управління у сфері сталого розвитку регіонів є формування та реалізація

ефективної регіональної політики, яка відповідає як національним, так і локальним викликам. Зокрема, це передбачає планування просторового розвитку, інвестицій в інфраструктуру, стимулювання зелених інновацій, розвиток людського потенціалу та підтримку місцевого самоврядування.

У звітах ООН, зокрема в «Transforming our world: the 2030 Agenda for Sustainable Development», підкреслюється, що саме регіональний рівень є ключовим для реалізації більшості із 17 Цілей сталого розвитку (ЦСР), оскільки саме в регіонах найвиразніше проявляються соціальні диспропорції, екологічні загрози та економічні дисбаланси [5].

У вітчизняному контексті національна модель управління сталим розвитком зазнала значних змін після прийняття Національної стратегії сталого розвитку України до 2030 року. Вона акцентує увагу на децентралізації, розширенні повноважень місцевих громад, а також інтеграції ЦСР у регіональні стратегії розвитку [9].

Як слушно звертають увагу дослідники, в рамках сьогоденних подій в Україні, світовій спільності доводиться переосмислити глобальні цілі сталого розвитку. Останніми роками в усіх розвинутих країнах найбільший фокус уваги був спрямований на екологію та довкілля. Але, як показала війна в Україні, без базового миру, сталого розвитку економіки, справедливості, цінування життя та прав людини до всього іншого можна просто не дожити, тому першочерговими пріоритетами сталого розвитку під час війни стали — соціально-економічні цілі розвитку держави [7].

Окремої уваги заслуговує проблема адаптації регіональної політики до умов війни. Повномасштабне вторгнення Росії у 2022 році загострило потребу в мобілізації ресурсів для гуманітарної допомоги, зміцнення інституційної спроможності регіонів, а також відновлення інфраструктури й промислового потенціалу. Публічне управління в таких умовах повинно враховувати як короткострокові потреби безпеки, так і довгострокові цілі сталого розвитку [4].

Інструментарій публічного управління сталим розвитком охоплює стратегічне планування, бюджетування, екологічне нормування, моніторинг та оцінювання ефективності політик, а також залучення громадськості до процесів прийняття рішень. Наприклад, ефективна реалізація політик «зеленого зростання» можлива лише за умов прозорої системи управління, яка передбачає партнерство між державою, бізнесом і громадянським суспільством [1].

На регіональному рівні важливими є інтегровані підходи до планування — як це передбачено, наприклад, у системі просторового розвитку ЄС (Territorial Agenda 2030), де регіони розглядаються як «лабораторії» для сталих трансформацій, адаптованих до локальних умов [2].

В Україні прикладами практичного втілення сталого розвитку на регіональному рівні можна

вважати реалізацію проєктів з енергоефективності в рамках Фонду енергоефективності, розвиток системи «розумних міст», запровадження інструментів оцінки впливу на довкілля (ОВД) тощо [14].

Варто зазначити, що інституційна спроможність регіонів значною мірою залежить від якості управлінських кадрів. Тому актуальним залишається завдання підготовки та підвищення кваліфікації фахівців з питань публічного управління сталим розвитком, зокрема в умовах післявоєнного відновлення [11].

У контексті децентралізації та реформування системи публічного управління особливої актуальності набуває питання інституційного забезпечення сталого розвитку регіонів. Павленко О. П. зазначає, що формування ефективної інституційної структури є ключовим чинником у забезпеченні сталого розвитку, оскільки дозволяє адаптувати управлінські рішення до специфіки кожного регіону та забезпечити участь місцевих громад у процесах прийняття рішень [12].

У період повоєнного відновлення регіонів особливого значення набуває формування нової парадигми публічного управління, яка враховує сучасні виклики та потреби територій. Рагімов Ф. акцентує увагу на необхідності розробки та впровадження комплексного механізму державного управління на регіональному рівні, що забезпечить ефективне функціонування системи публічного управління в умовах протидії

зовнішнім загрозам та сприятиме впровадженню інноваційних форм і методів діяльності [13].

У відповідь на нові виклики, зумовлені війною, глобальними змінами клімату, економічною нестабільністю та потребами відновлення, публічне управління сталим розвитком регіонів потребує нової моделі, що передбачає комплексне бачення й координацію ключових сфер.

Виходячи зі сказаного вище, вважаємо за доцільне запропонувати інтегровану модель публічного управління сталим розвитком регіонів у післявоєнний період, котра складається з чотирьох взаємопов'язаних компонентів: інституційного, фінансового, соціального та технологічного (рис. 1).

Інституційний компонент є фундаментом ефективного управління. Він передбачає децентралізацію, зміцнення управлінської спроможності регіонів, підвищення якості кадрового потенціалу, розвиток локального самоврядування та впровадження принципів прозорості й підзвітності. У сучасних умовах акцент робиться на формуванні нових моделей взаємодії між владою, бізнесом та громадянським суспільством у рамках партнерського управління.

Фінансовий компонент забезпечує ресурсну основу сталого розвитку. Йдеться про програмно-цільове бюджетування з урахуванням Цілей сталого розвитку, прозоре управління державними коштами, ефективне використання міжнародної технічної



Рис. 1. Інтегрована модель публічного управління сталим розвитком регіонів у післявоєнний період

Джерело: розроблено автором

допомоги, розвиток публічно-приватного партнерства та створення спеціалізованих регіональних фондів. У післявоєнний період особливо актуальними стають інструменти підтримки інфраструктурних проєктів та гуманітарного відновлення.

Соціальний компонент орієнтований на підвищення якості життя населення та зменшення соціальних ризиків. Його ключовими напрямками є подолання бідності, підтримка вразливих груп (зокрема ВПО), розвиток освіти, охорони здоров'я, забезпечення участі громадян у процесах прийняття рішень на місцевому рівні. У контексті публічного управління це вимагає створення умов для активного залучення громадськості до стратегічного планування розвитку регіонів.

Технологічний компонент забезпечує інноваційний супровід процесів сталого розвитку. Він включає цифрову трансформацію публічного управління, впровадження «зелених» та енергоефективних технологій, розвиток систем «розумних міст», підтримку інноваційних екосистем. Особливої уваги заслуговують технології для моніторингу екологічного стану, екоосвіти та інтеграція ESG-підходів у місцеву політику.

Центральним елементом моделі виступає мета — досягнення сталого розвитку регіонів, що передбачає збалансоване поєднання економічного зростання, соціальної справедливості та екологічної безпеки. Ефективність досягнення цієї мети можлива лише за умови синергії між усіма компонентами моделі. Зміни в одній сфері неминуче впливають на інші, що зумовлює необхідність системного й адаптивного підходу до публічного управління.

Запропонована модель може бути практичним орієнтиром для органів влади в процесі розробки та реалізації регіональних стратегій відновлення та розвитку. Вона також надає аналітичну рамку для подальших наукових досліджень, спрямованих на поглиблення розуміння процесів сталого розвитку в умовах посткризового відновлення України.

Таким чином, публічне управління сталим розвитком регіонів в Україні повинно трансформуватись відповідно до нових реалій — від концепції «ке-

рування згори» до моделі адаптивного, прозорого і партнерського управління, що базується на інтеграції глобальних і локальних пріоритетів сталого розвитку.

Висновки та перспективи подальших досліджень. З огляду на сучасні виклики, вважаємо, що у повоєнний період питання відновлення інфраструктури, подолання бідності, забезпечення екологічної безпеки та посилення інституційної спроможності регіонів постануть як першочергові проблеми у сфері публічного управління. У нових умовах особливої актуальності набуває необхідність перегляду стратегічних підходів до регіонального розвитку із врахуванням довгострокових орієнтирів сталості, адаптивності та інклюзивності.

У рамках реалізації цих завдань пропонується модель публічного управління сталим розвитком регіонів, яка базується на чотирьох ключових компонентах: інституційному, фінансовому, соціальному та технологічному. Кожен із цих компонентів є взаємопов'язаним та взаємодіє для забезпечення сталого розвитку, зокрема через зміцнення інституційної спроможності на всіх рівнях управління, активне залучення фінансових ресурсів, підтримку соціальних ініціатив та впровадження технологічних інновацій. Зокрема, на регіональному рівні важливим є інтерфейс між органами місцевого самоврядування, державними структурами, бізнесом і громадським сектором, що забезпечує інтегроване планування розвитку та стійкість до зовнішніх шоків.

Перспективним напрямом подальших досліджень у межах даної тематики є аналіз реалізації цілей сталого розвитку крізь призму сучасних викликів, зокрема в умовах воєнного стану, постконфліктного відновлення, кліматичних змін та демографічної кризи. Особливу увагу слід приділити вивченню моделей багаторівневого управління, які дозволяють ефективно поєднувати зусилля центральної влади, органів місцевого самоврядування, бізнесу і громадянського суспільства задля досягнення економічного зростання та сталого розвитку регіонів.

Література

1. European Environment Agency (EEA). Sustainable Development in the EU — 2023 Monitoring Report. URL: <https://www.eea.europa.eu/publications/sustainable-development-in-the-eu> (дата звернення: 30.04.2025).
2. European Union. Territorial Agenda 2030: A Future for all Places. URL: <https://territorialagenda.eu> (дата звернення: 30.04.2025).
3. Sachs J.D. The Age of Sustainable Development. Columbia University Press. URL: <https://cup.columbia.edu/book/the-age-of-sustainable-development/9780231173148> (дата звернення: 30.04.2025).
4. UNDP Ukraine (2023). Ukraine: Resilience and Recovery in the Face of War. URL: <https://www.undp.org/ukraine/publications> (дата звернення: 30.04.2025).
5. United Nations (2015). Transforming our world: the 2030 Agenda for Sustainable Development. URL: <https://sdgs.un.org/2030agenda> (дата звернення: 30.04.2025).
6. Баргов М.В., Костріков С.В., Черваньов І.Г. До питання формалізації інвайронментального виміру сталого соціально-економічного розвитку суспільства. *Геополітика і екогеодинаміка регіонів*. 2008. В. 1–2. С. 5–15.

7. Капінос Г., Ларіонова К. Проблеми управління сталим розвитком України. *Modeling the development of the economic systems*. 2023. С. 93–103. URL: <https://doi.org/10.31891/mdes/2023-7-13> (дата звернення: 30.04.2025).
8. Комаха Л. Evolution of the concept of sustainable development in public administration discourse: territorial context. *Державне управління*. 2024. 2(20). С. 25–28.
9. Міністерство економіки України. *Національна доповідь «Цілі сталого розвитку: Україна»* (2017). URL: <https://me.gov.ua/Documents/Detail?lang=uk-UA&id=29cb28bb-f78d-4eae-9c89-e7aefc26183e> (дата звернення: 30.04.2025).
10. Мовчанюк А. Публічне управління як стратегічний інструмент для забезпечення сталого розвитку територій. *Економіка та суспільство*. 2024. 60. <https://doi.org/10.32782/2524-0072/2024-60-50>.
11. НАДС. Підготовка публічних службовців у сфері управління розвитком регіонів. URL: <https://nads.gov.ua> (дата звернення: 30.04.2025).
12. Павленко О. П. Інституційне забезпечення публічного управління регіонами. *Вісник ХНАУ ім. В. В. Докучаєва. Серія «Економічні науки»*. 2021. Т. 2, № 2. С. 299–310.
13. Рагімов Ф. Сталий розвиток регіонів в умовах повного відновлення в контексті формування наукової парадигми публічного управління. *Публічне управління та місцеве самоврядування*. 2023. Вип. 1. С. 46–52.
14. Фонд енергоефективності України. URL: <https://eefund.org.ua> (дата звернення: 30.04.2025).
15. Ханова О. В., Скібіна С. О. Сталий розвиток країн ЄС: методика й індикатори оцінювання. *Проблеми економіки*. 2017. № 3. С. 20–32.

References

1. European Environment Agency (EEA). Sustainable Development in the EU — 2023 Monitoring Report. URL: <https://www.eea.europa.eu/publications/sustainable-development-in-the-eu>.
2. European Union. Territorial Agenda 2030: A Future for all Places. URL: <https://territorialagenda.eu>.
3. Sachs J. D. The Age of Sustainable Development. Columbia University Press. URL: <https://cup.columbia.edu/book/the-age-of-sustainable-development/9780231173148>.
4. UNDP Ukraine (2023). Ukraine: Resilience and Recovery in the Face of War. URL: <https://www.undp.org/ukraine/publications>.
5. United Nations (2015). Transforming our world: the 2030 Agenda for Sustainable Development. URL: <https://sdgs.un.org/2030agenda>.
6. Bahrov M. V., Kostrikov S. V., Chervanov I. H. Do pytannia formalizatsii invayronmentalnoho vymiru staloho sotsialno-ekonomichnoho rozvytku suspilstva. Heopolitykai ekoheodynamika rehioniv. 2008. V. 1–2. S. 5–15.
7. Kapinos H., Larionova K. Problemy upravlinnia stalym rozvytkom Ukrainy. *Modeling the development of the economic systems*. 2023. S.93–103. URL: <https://doi.org/10.31891/mdes/2023-7-13>.
8. Komakha L. Evolution of the concept of sustainable development in public administration discourse: territorial context. *Derzhavne upravlinnia*. 2024. 2(20). S. 25–28.
9. Ministerstvo ekonomiky Ukrainy. *Natsionalna dop-8d-4eae-9c89-e7aefc26183e*.
10. Movchaniuk A. Publichne upravlinnia yak stratehichni instrument dlia zabezpechennia staloho rozvytku terytorii. *Ekonomika ta suspilstvo*. 2024. 60. <https://doi.org/10.32782/2524-0072/2024-60-50>.
11. NADS. Pidhotovka publichnykh sluzhbovtsiv u sferi upravlinnia rozvytkom rehioniv. URL: <https://nads.gov.ua>.
12. Pavlenko O. P. Instytutsiine zabezpechennia publichnoho upravlinnia rehionamy. *Visnyk KhNAU im. V. V. Dokuchaieva. Seriiia «Ekonomichni nauky»*. 2021. Т. 2, № 2. S. 299–310.
13. Rahimov F. Stalyi rozvytok rehioniv v umovakh povoiennoho vidnovlennia v konteksti formuvannia naukovoї paradyhmy publichnoho upravlinnia. *Publichne upravlinnia ta mistseve samovriaduvannia*. 2023. Vyp. 1. S. 46–52.
14. Fond enerhoefektyvnosti Ukrainy. URL: <https://eefund.org.ua>.
15. Khanova O. V., Skibina S. O. Stalyi rozvytok krain YeS: metodyka y indykatory otsiniuvannia. *Problemy ekonomiky*. 2017. № 3. S. 20–32.

Стаття надійшла до редакції 07.05.2025

Івлієва Ольга Михайлівна

*кандидат педагогічних наук, доцент,
доцент кафедри математики, інформатики та інформаційної діяльності
Ізмаїльський державний гуманітарний університет*

Ivliieva Olga

*Candidate of Pedagogical Sciences, Associate Professor,
Associate Professor of the Department of Mathematics, Informatics and Information Activities
Izmail State University of Humanities*

ORCID:0000-0003-3525-322X

Мізіук Вікторія Анатоліївна

*кандидат педагогічних наук, доцент,
доцент кафедри математики, інформатики та інформаційної діяльності
Ізмаїльський державний гуманітарний університет*

Miziuk Viktoriia

*Candidate of Pedagogical Sciences, Associate Professor,
Associate Professor of the Department of Mathematics, Informatics and Information Activities
Izmail State University of Humanities*

ORCID: 0000-0001-8291-6597

Драгієва Людмила Василівна

*кандидат педагогічних наук, доцент,
доцент кафедри математики, інформатики та інформаційної діяльності
Ізмаїльський державний гуманітарний університет*

Drahiieva Liudmyla

*Candidate of Pedagogical Sciences, Associate Professor,
Associate Professor of the Department of Mathematics, Informatics and Information Activities,
Izmail State University of Humanities*

ORCID: 0000-0002-0892-086X

DOI: 10.25313/2617-572X-2025-5-10954

СОЦІАЛЬНО-ГУМАНІТАРНІ АСПЕКТИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ВИКЛАДАЧІВ МАТЕМАТИЧНИХ ДИСЦИПЛІН У КОНТЕКСТІ СУЧАСНОЇ ОСВІТНЬОЇ ПОЛІТИКИ

SOCIAL AND HUMANITARIAN ASPECTS OF PROFESSIONAL TRAINING OF TEACHERS OF MATHEMATICAL DISCIPLINES IN THE CONTEXT OF MODERN EDUCATIONAL POLICY

Анотація. Вступ. Концептуальна парадигма сучасності зумовлює інноватику рішень у сфері підготовки майбутніх спеціалістів. Потребує доопрацювання узагальнена концепція відтворення навичок та вмінь крізь призму швидких логічних рішень, враховуючи досвід провідних держав світу та акцентуючи увагу на постулатах сучасних інноваційних перетворень у системі освіти.

Мета. Метою статті є дослідження соціально-гуманітарних аспектів професійної підготовки викладачів математичних дисциплін у контексті сучасної освітньої політики.

Методи і матеріали. В процесі дослідження використано теоретичні (методи аналогії і порівняння, абстрактно-логічний) та емпіричні (педагогічний експеримент, педагогічне прогнозування) методи.

Результати. У статті проаналізовано та узагальнено фактори негативного впливу, що ускладнюють парадигму професійної підготовки викладачів математичних дисциплін (масовий характер підготовки майбутніх спеціалістів, недостатність умов для індивідуального самовираження у професійній діяльності, недостатність годин у навчальних планах на вивчення курсів з методики викладання у вищій школі, недостатність використання сучасних освітніх технологій у навчанні), компоненти формування сучасної інноваційної компетентності високого професійного рівня підготовки майбутнього викладача математичних дисциплін (наприклад, – мотиваційний компонент, змістовний компонент, операційний компонент, інтегративний компонент).

Перспективи. Сформовано стратегічне бачення сучасних принципів формування компетентностей професійної підготовки викладачів математичних дисциплін у контексті новітньої освітньої політики. Зокрема, наголошено на необхідності застосування нових технологій та інноваційних рішень у педагогічній діяльності, забезпечення відповідності освітньої діяльності змісту освіти, забезпечення моделювання технологій професійної діяльності, створення інноваційного освітнього середовища із включенням учнів у процес безпосереднього викладання.

Ключові слова: освітня політика, професійні компетенції, математична освіта, соціальні аспекти викладання, гуманізація технічної освіти.

Summary. Introduction. The conceptual paradigm of modernity determines the innovation of solutions in the field of training future specialists. The generalized concept of reproducing skills and abilities through the prism of quick logical solutions needs to be refined, taking into account the experience of leading countries of the world and focusing on the postulates of modern innovative transformations in the education system.

Purpose. The purpose of the article is to study the socio-humanitarian aspects of the professional training of teachers of mathematical disciplines in the context of modern educational policy.

Materials and methods. In the research process, theoretical (methods of analogy and comparison, abstract-logical) and empirical (pedagogical experiment, pedagogical forecasting) methods were used.

Results. The article analyzes and summarizes the factors of negative influence that complicate the paradigm of professional training of teachers of mathematical disciplines (the mass nature of training of future specialists, the lack of conditions for individual self-expression in professional activity, the lack of hours in the curricula for studying courses on teaching methods in higher education, the lack of use of modern educational technologies in teaching), the components of the formation of modern innovative competence of a high professional level of training of a future teacher of mathematical disciplines (for example, the motivational component, the content component, the operational component, the integrative component).

Discussion. A strategic vision of modern principles of forming competencies of professional training of teachers of mathematical disciplines in the context of the latest educational policy has been formed. In particular, the need to apply new technologies and innovative solutions in pedagogical activity, ensuring compliance of educational activity with the content of education, ensuring modeling of technologies of professional activity, and creating an innovative educational environment with the inclusion of students in the process of direct teaching has been emphasized.

Key words: educational policy, professional competencies, mathematical education, social aspects of teaching, humanization of technical education.

Постановка проблеми. Соціальні та гуманітарні аспекти професійної підготовки викладачів математичних дисциплін мають вирішальне значення для сприяння всебічному та цілісному підходу до освіти. У буремних умовах сьогодення викладачі відіграють надважливу роль у формуванні інтелектуального та соціального розвитку своїх учнів, тому важливо, щоб вони були оснащені необхідними навичками та знаннями. Від глибини та всеохоплюючої характеристики означених навичок та вмінь формується узагальнене концептуальне уявлення щодо прогресивних тенденцій розвитку сфери освіти в Україні в цілому, її трансформаційних перетворень та інноватики.

У контексті сучасної освітньої політики акцент все більше зміщується в бік студентоцентричного підходу. Відповідне положення зумовлює формування концептуальних засад на розвитку навичок

критичного мислення, креативності та здібностей до вирішення складних проблем. Викладачі математичних дисциплін повинні мати змогу адаптувати свої методи навчання до різноманітних стилів викладення матеріалу, враховуючи як наявні, так і потенційні здібності своїх учнів. Це вимагає глибокого розуміння соціальних та культурних факторів, які можуть впливати на процес навчання в цілому. Крім того, професійна підготовка викладачів математичних дисциплін також повинна включати сильний етичний вимір. Вчителі повинні усвідомлювати етичні наслідки своєї педагогічної практики та прагнути створити безпечне та інклюзивне навчальне середовище для всіх учнів. Виховуючи емпатію, співчуття та повагу до різноманітності, вчителі можуть допомогти створити позитивне та сприятливе навчальне середовище, яке всебічно сприяє інтелектуальному та емоційному розвитку

учнів. Загалом, соціальні та гуманітарні аспекти професійної підготовки викладачів математичних дисциплін є важливими для забезпечення того, щоб викладачі були підготовлені до задоволення сучасних інноваційних розширених потреб учнів, які постійно змінюються, у сучасному освітньому ландшафті. Інтегруючи ці аспекти у свою педагогічну практику, вчителі можуть суттєво впливати на рівень та якість життя своїх учнів, сприяючи розвитку інклюзивного інноваційного суспільства.

Аналіз останніх досліджень і публікацій.

Дослідженням аспектів професійної підготовки викладачів математичних дисциплін у контексті сучасної освітньої політики опікувалось багато науковців, зокрема: Манькусь І., Дармосюк В., Васильєва Л., Недбаєвська Л., Карпова О., Остапівська І., Свистун Н., Теслюк С., Руденко Н., Рудницька Н., Акуленко І. [2–10] та інші.

Проведені наукові дослідження вчених (Дінжос Р. [1], Манькусь І. [1]) засвідчують відтворення інноваційної парадигми рішень, що зумовлює перехід від знаннево-просвітницької парадигми природничо-математичної освіти до парадигми продуктивного навчання. Відповідний перехід обумовлює формування інноватики знань та вмінь учнів, що характеризується не відтворенням можливості засвоєння ними результатів проведеного наукового дослідження в рамках викладання математичних дисциплін, а безпосередньою участю учнів в самому експерименті, формуванні висновків щодо його проведення та обумовлення інноваційності рішень. Означені постулати акцентують увагу на формуванні спектру необхідних компетентностей учнів.

Аналіз сучасних наукових досліджень парадигми соціально-гуманітарних аспектів професійної підготовки викладачів математичних дисциплін, у контексті освітньої політики, наголошує на необхідності удосконалення технологічної компетентності викладачів.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження соціально-гуманітарних аспектів професійної підготовки викладачів математичних дисциплін у контексті сучасної освітньої політики.

Матеріали і методи. Матеріалами дослідження є праці вітчизняних та закордонних авторів, що проводять свої науково-практичні дослідження у царині вивчення аспектів професійної підготовки викладачів математичних дисциплін.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування; формалізації, аналізу та синтезу; логічного узагальнення результатів наукового дослідження.

Виклад основного матеріалу дослідження.

Освоєння сучасних форм професійної підготовки фахівців забезпечує інноватику професійних рішень та концепцію відтворення парадигми освітньої діяльності у нову площину — стратегічного мислення та бачення пріоритетів. Наприклад, використання в сучасних умовах компетентнісного, STEM-орієнтованого підходів з моделюванням ситуацій професійної діяльності при підготовці майбутніх викладачів математичних дисциплін обумовлює інноватику рішень, розширюючи спектр можливостей та стратегічних орієнтирів прогресивного професійного розвитку.

Крім того, активізація рішень в контексті трансдисциплінарного підходу, при підготовці майбутніх викладачів математичних дисциплін, забезпечує розширенню спектру навичок та вмінь і, у зв'язку з цим, обумовлює інноваційність сучасного викладання.

Однак, у світовій практиці вважається найбільш прогресивним та новаторським контекстний підхід, що спирається на теорію та технології знаковоконтекстного навчання.

В університетах наразі існує проблематика аспектів підготовки інноваційних спеціалістів, що

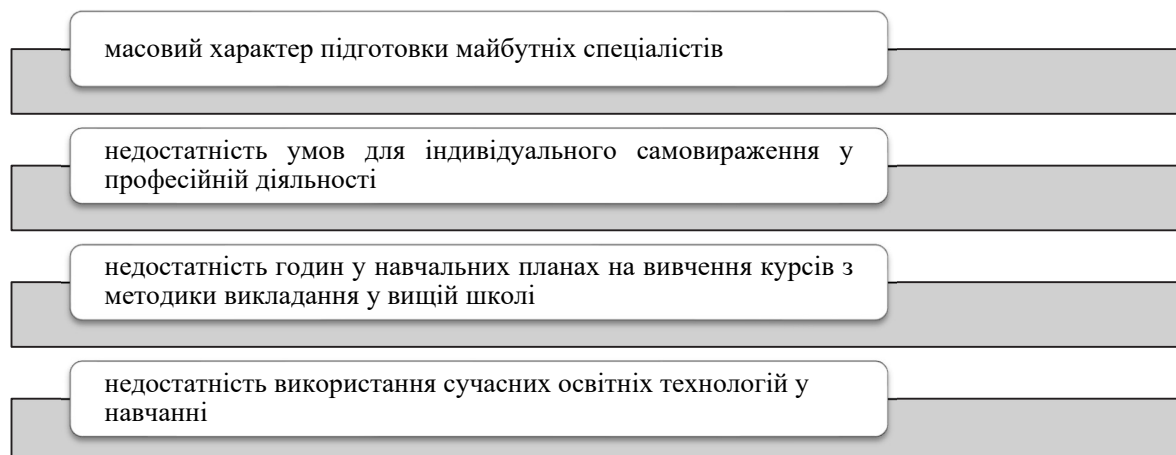


Рис. 1. Перелік узагальнених факторів негативного впливу, що ускладнюють парадигму професійної підготовки викладачів математичних дисциплін

Джерело: авторська розробка

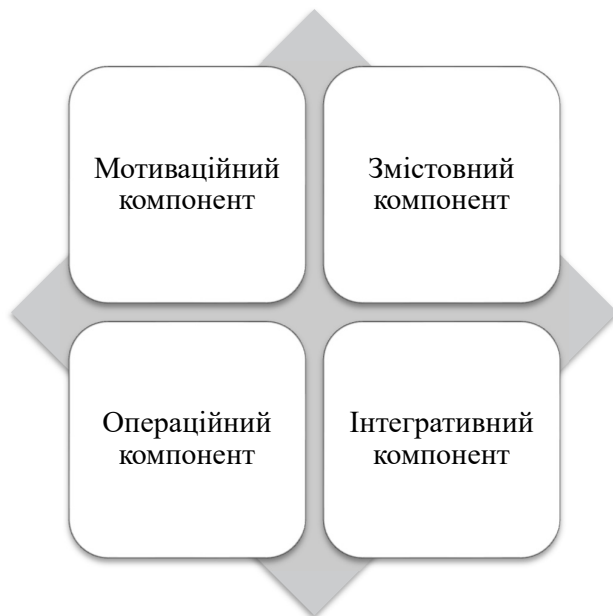


Рис. 2. Компоненти формування сучасної інноваційної компетентності високого професійного рівня підготовки майбутнього викладача математичних дисциплін

Джерело: авторська розробка

обумовлено негативним впливом певних факторів. Перелік узагальнених факторів негативного впливу, що ускладнюють парадигму професійної підготовки викладачів математичних дисциплін наведено на рис. 1.

В сучасних умовах реформування освітньої політики необхідним є врахування наступних компонентів:

- розробка сучасної інноваційної моделі педагогічної професії;
- визначення стратегічних шляхів професійного розвитку і підвищення кваліфікації педагогічних працівників.

Технологічна компетентність високого професійного рівня підготовки майбутнього викладача математичних дисциплін характеризується наявністю певних компонентів (рис. 2).

Синергетичний ефект взаємодії означених компонентів формування сучасної інноваційної компетентності високого професійного рівня підготовки майбутнього викладача математичних дисциплін віддзеркалює інноватику парадигми навчання, ґрунтуючись на постулатах переформатування бачення та стратегічних орієнтирів здобуття навичок та вмінь. З метою забезпечення формування високого рівня підготовки майбутніх викладачів математичних дисциплін важливо зосередитися на декількох ключових елементах. По-перше, вирішальним є забезпечення міцної основи математичних понять і теорій. Це включає не лише вивчення змісту, але й розуміння основних принципів і застосувань. По-друге, слід наголосити на практичному досвіді та навичках вирішення проблем різноманітного характеру.

Дослідження означеної проблематики є важливим з метою забезпечення професійної підготовки майбутніх фахівців, враховуючи відповідні принципи (рис. 3).

Майбутні викладачі математики повинні мати можливість працювати над реальними проблемами, займатися математичним моделюванням і розвивати критичне мислення. Крім того, необхідний сильний

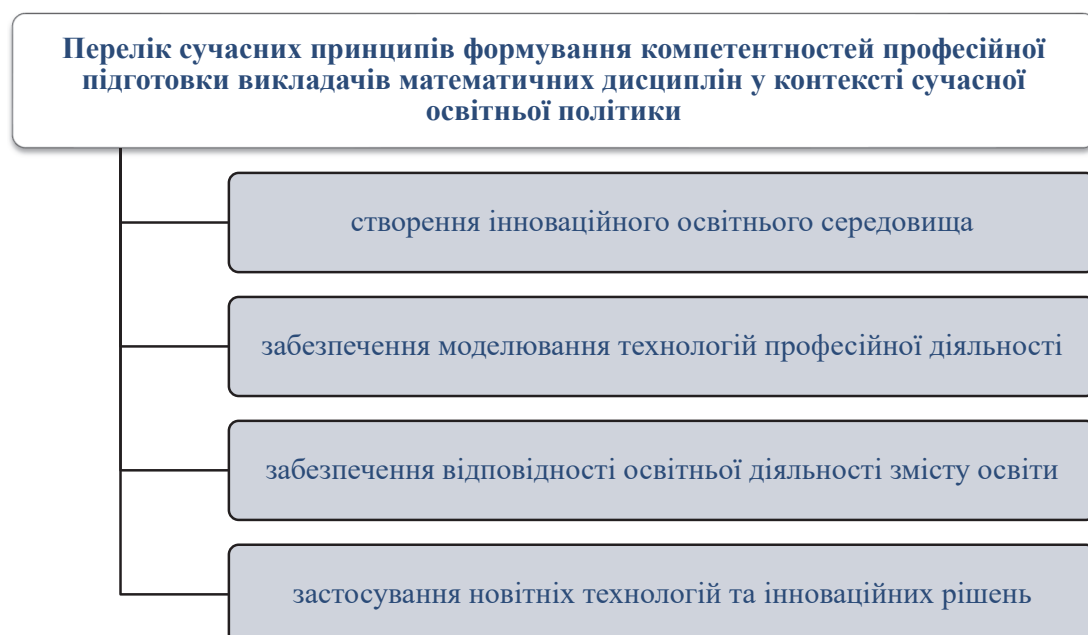


Рис. 3. Перелік сучасних принципів формування компетентностей професійної підготовки викладачів математичних дисциплін у контексті сучасної освітньої політики

Джерело: авторська розробка

акцент на педагогічній підготовці. Викладачі повинні розуміти, як ефективно доносити математичні поняття до учнів різного рівня підготовки та стилів навчання. Це включає використання сучасних методів навчання, технологій та інструментів для покращення навчального досвіду. Нарешті, безперервний професійний розвиток та навчання протягом усього життя є важливими для того, щоб бути обізнаними у площині досягнень у галузі математики та освіти. Заохочення вчителів до участі в дослідженнях, участі в семінарах та співпраці з однолітками може сприяти їх постійному зростанню та ефективності. Включивши

ці елементи у підготовку та розвиток майбутніх вчителів математики, ми можемо забезпечити їх повну підготовку до натхнення та навчання наступного покоління учнів математичним дисциплінам.

Висновки. Компіляція професійної підготовки майбутніх фахівців та педагогічної освіти зумовлюють синергетичний ефект інноватики знань, вмінь та навичок в сучасному буремному турбулентному світі. Студентоцентризм та педагогічне партнерство забезпечують комплексність поглядів на сучасну освітню діяльність та є необхідними для ефективного її впровадження.

Література

1. Дінжос Р.В., Недбаєвська Л.С., Манькусь І.В. STEM-майданчики як компонент розвитку нової української школи. *Питання удосконалення змісту і методики викладання природничо-математичних дисциплін у середній і вищій школі*, 2018. № 24. С. 5–7.
2. Манькусь І.В., Дармосюк В.М., Васильєва Л.Я. Інноваційне освітнє середовище як фактор підвищення якості вищої освіти. *Інженерні та освітні технології*, 2019. Т. 7, № 3. С. 40–49. DOI: 10.30929/23079770.2019.07.03.04.
3. Манькусь І.В., Недбаєвська Л.С. Технологія майстер-класу джерело формування професійних компетентностей викладача. *Витоки педагогічної майстерності*. 2017. № 1. С. 229–233.
4. Манькусь І.В., Недбаєвська Л.С., Дармосюк В.М. Впровадження STEM-майданчиків як сучасних освітніх середовищ у професійній діяльності вчителя. *Фізико-математична освіта*. 2019. № 1 (19). С. 130–134. DOI: 10.31110/2413-1571-2019-019-1-020.
5. Карпова О.Ю. Особливості використання ІКТ на уроках математики в початковій школі в контексті Нової української школи. *Редакційна колегія*. 2011. № 8–9. С. 73–80.
6. Остапйовська І., Свистун Н., Теслюк С. Використання інформаційних технологій для навчання початкового курсу математики. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Розділ II. Теорія навчання*. 2017. 2 (351). С. 30–40.
7. Руденко Н.М. Інтерактивні технології навчання на уроках математики у початковій школі: від планування до результату. *Педагогічна освіта: теорія і практика. Психологія. Педагогіка: збірник наукових праць*. 2019. № 32. С. 22–28.
8. Рудницька Н.Ю. Сучасні технології навчання математики у початковій школі в контексті впровадження ідей Нової української школи. Система підготовки майбутніх фахівців у контексті становлення Нової української школи: монографія. Житомир : Вид. О.О. Євенок, 2019. 344 с.
9. Акуленко І.А. Діагностування якості методичної підготовки майбутнього вчителя математики засобами навчально-методичних задач. *Науковий вісник Миколаївського національного університету імені В.О. Сухомлинського. Педагогічні науки: збірник наукових праць*. 2020. № 2(37). С. 19–27.
10. Skvortsova S., Britskan T., Symonenko T., Haievets Y. Interactive tools for creating educational content for primary school. *INTED-2022 Proceedings: students*. 2022. P. 9005–9014. URL: <https://library.iated.org/view/SKVORTSOVA2022INT> (дата звернення: 01.05.2025).

References

1. Dinzhos, R. V. & Nedbaievskia, L. S. & Mankus, I. V. (2018). STEM-majdanchy'ky' yak komponent rozvy'tku novoyi ukrayins'koyishkoly' [STEM platforms as a component of the development of a new Ukrainian school]. *Py'tannya udoskonalennya zmistu i metody'ky' vy'kladannya pry'rodny'cho-matematy'chny'x dy'scy'plin u serednij i vy'shhij shkoli — Issues of improving the content and teaching methods of natural and mathematical disciplines in secondary and high school*, 24, 5–7 [in Ukraine].
2. Mankus, I. V. & Darmosiyk, V. M. & Vasylieva, L. Ya. (2019) Innovatsiine osvitnie seredovyshe yak faktor pidvyshchennia yakosti vyshchoi osvity [Innovative educational environment as a factor in improving the quality of higher education] *Inzhenerni ta osvitni tekhnologii* — *Engineering and Educational Technologies*, 7(3), 40–49 [in Ukraine].
3. Mankus, I. V. & Nedbaievskia, L. S. (2017). Tekhnologiya majsterklasu dzherelo formuvannya profesijnny'x kompetentnostej vy'kladacha [The technology of the master class is the source of the formation of the professional competence of the teacher]. *Vy'toky' pedagogichnoyi majsternosti — The sources of pedagogical skills*, 1, 229–233 [in Ukraine].
4. Mankus I. V., & Nedbaievskia L. S., & Darmosiyk V. M. (2019). Vprovadzhennia STEM-majdanchykyv yak suchasnykh osvitnikh seredovyshech u profesiinii diialnosti vchytelia [Implementation of STEM — platforms as a modern educational

environment in professional activities of teacher]. *Fizyko matematychna osvita — Physical & Mathematical education*, 1(19), 130–134 [in Ukraine].

5. Karpova, O. Yu. (2011). Osoblyvosti vykorystannia IKT na urokakh matematyky v pochatkovii shkoli v konteksti Novoi ukrainskoi shkoly [Features of using ICT in mathematics lessons in primary school in the context of the New Ukrainian School]. *Redaktsiina kolehiia — Editorial Boar*, 8–9, 73–80 [in Ukrainian].

6. Ostapovska, I., Svystun, N., Tesliuk, S. (2017). Vykorystannia informatsiinykh tekhnolohii dlia navchannia pochatkovoho kursu matematyky [Using information technologies for teaching the primary course of mathematics]. *Naukovyi visnyk Shhidnoievropeiskoho natsionalnoho universytetu imeni Lesi Ukrayinky — Scientific Bulletin of the Lesya Ukrainka Eastern European National University*, 2 (351), 30–40 [in Ukrainian].

7. Rudenko, N. M. (2019). Interaktyvni tekhnolohii navchannia na urokakh matematyky u pochatkovii shkoli: vid planuvannia do rezultatu [Interactive teaching technologies in mathematics lessons in primary school: from planning to results]. *Pedahohichna osvita — Pedagogical education*, 32, 22–28 [in Ukrainian].

8. Rudnytska, N. Yu. (2019). Suchasni tekhnolohii navchannia matematyky u pochatkovii shkoli v konteksti vprovadzhennia idei Novoi ukrainskoi shkoly [Modern technologies of teaching mathematics in primary school in the context of implementing the ideas of the New Ukrainian school]. *Systema pidhotovky maibutnikh fakhivtsiv u konteksti stanovlennia Novoi ukrainskoi shkoly: monohrafiia — The system of training future specialists in the context of the formation of the New Ukrainian school: monograph*. Zhytomyr: Publishing house of O. O. Yevenok [in Ukrainian].

9. Akulenko, I. A. (2017). Diahnostuvannia yakosti metodychnoi pidhotovky maibutnoho vchytelia matematyky zasobamy navchalno-metodychnykh zadach [Diagnostics the quality of future mathematics teacher's methodological training by means of educational and methodological tasks]. *Scientific Bulletin of the Mykolaiv National University named after V. O. Sukhomlynsky. Pedagogical Sciences: Collection of Scientific Works*, 2(37), 19–27 [in Ukrainian].

10. Skvortsova, S., Britskan, T., Symonenko, T., Haievets, Y. (2022). Interactive tools for creating educational content for primary school. *INTED-2022 Proceedings: students*. PP. 9005–9014. Retrieved from <https://library.iated.org/view/SKVORTSOVA2022INT> (access date: 01/05/2025).

Стаття надійшла до редакції 05.05.2025

УДК 355.4:355.02(477+569.4)

Tesnikov Oleksandr

Lieutenant Colonel,

*Senior Lecturer of the Department of Logistics Management
of the Operational Faculty*

National Academy of the National Guard of Ukraine

Тесніков Олександр Михайлович

підполковник,

*старший викладач кафедри управління логістикою оперативного факультету
Національна академія Національної гвардії України*

ORCID: 0000-0002-4693-0428

Fursova Viktoriya

Candidate of Economic Sciences, Associate Professor,

Associate Professor of the Department of Management and Business Administration

National Aerospace University "Kharkiv Aviation Institute"

Фурсова Вікторія Анатоліївна

кандидат економічних наук, доцент,

доцент кафедри менеджменту та бізнес-адміністрування

Національний аерокосмічний університет

«Харківський авіаційний інститут»

ORCID: 0000-0002-4841-3416

DOI: 10.25313/2617-572X-2025-5-10974

MANAGEMENT OF MILITARY LOGISTICS IN THE NATIONAL SECURITY SYSTEM: THE EXPERIENCE OF UKRAINE AND ISRAEL

УПРАВЛІННЯ ВІЙСЬКОВОЮ ЛОГІСТИКОЮ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ДОСВІД УКРАЇНИ ТА ІЗРАЇЛЮ

Summary. Introduction. In the context of modern warfare, particularly hybrid and high-intensity conflicts, military logistics plays a pivotal role not only in supporting frontline operations but also in shaping the overall defense capabilities of a state. The effectiveness of logistical systems directly influences strategic sustainability, combat readiness, and operational continuity. Ukraine's ongoing war with Russia and Israel's long-standing experience in conflict management offer valuable empirical grounds for comparative analysis of military logistics in diverse geopolitical and operational environments.

Purpose. This paper aims to analyze the structural features, strategic priorities, and innovation-based mechanisms of military logistics in Ukraine and Israel to identify applicable models for strengthening national logistical resilience.

Materials and Methods. The study uses comparative and content analysis of legislative frameworks, defense ministry reports, academic articles, and open data.. A SWOT analysis was conducted to identify the risks and opportunities within the logistics systems of Ukraine and Israel. Additionally, the method of logical generalization was used to formulate conclusions and recommendations.

Results. The study reveals the operational features of the military logistics systems of Israel and Ukraine under conditions of armed conflict. The financial dimensions of logistics, including sources of funding in both countries, have been analyzed. Key advantages of the Israeli model have been identified, such as decentralization, the use of digital technologies, the autonomy of logistical units, and the active integration of the dual-use startup ecosystem. These factors contribute to enhanced flexibility, rapid mobilization, and reliability of supply within the Israel Defense Forces.

At the same time, both the strengths and existing weaknesses of Ukraine's logistics system have been identified. Despite significant achievements in digitalization and the effective mobilization of volunteer resources, the study reveals issues related

to insufficient autonomy of combat units, limited material and technical resources, and the inefficiency of outdated public procurement mechanisms.

The study proposes the adaptation of effective elements of the Israeli model to the context of Ukraine's protracted conflict by implementing innovative managerial and digital solutions. Simultaneously, it is recommended that Israel consider Ukraine's experience in decentralized mobilization and the involvement of the civil sector in ensuring national defense capabilities.

Discussion. Israel's experience underscores the importance of civil-military cooperation and technology transfer in logistics modernization. Key lessons for Ukraine include building decentralized logistics hubs, introducing AI and blockchain tools, and expanding public-private innovation ecosystems tailored to battlefield needs.

Conclusion. Applying select Israeli practices to Ukraine can significantly enhance logistical autonomy, responsiveness, and adaptability. Strengthening logistics is essential for national security and effective military operation sustainability.

Key words: military logistics, national security, hybrid warfare, defense innovations, IDF, Armed Forces of Ukraine, dual-use technologies, decentralized management, civil-military partnership.

Анотація. Вступ. У сучасних умовах гібридних і повномасштабних війн військова логістика виступає ключовим компонентом забезпечення боєздатності, стійкості та мобільності збройних сил. Від ефективності логістичного управління значною мірою залежить результативність бойових дій, оперативне реагування на загрози та загальна обороноздатність держави. Війна в Україні, як і багаторічний досвід Ізраїлю у протидії зовнішнім загрозам, формують унікальне підґрунтя для порівняльного аналізу логістичних систем в умовах воєнного стану.

Мета. Метою дослідження є проведення порівняльного аналізу логістичних систем України та Ізраїлю з акцентом на структурні особливості, інноваційні рішення та адаптивні механізми, що забезпечують оперативність, ефективність і стійкість тилового забезпечення в умовах війни. Дослідження також має на меті окреслити можливості імплементації ізраїльського досвіду в український контекст.

Матеріали й методи. У роботі використано методи якісного контент-аналізу нормативно-правових актів, звітів, наукових джерел і відкритої аналітики. Для виявлення ризиків та можливостей розвитку логістичних систем України та Ізраїлю застосовано SWOT-аналіз, а також метод логічного узагальнення для формулювання висновків і рекомендацій.

Результати. У дослідженні розкрито особливості функціонування систем військової логістики Ізраїлю та України в умовах збройного конфлікту. Проаналізовано фінансовий аспект щодо джерел фінансування логістики в обох країнах. Визначено ключові переваги ізраїльської моделі, зокрема децентралізацію, використання цифрових технологій, автономність логістичних підрозділів та активну інтеграцію стартап-екосистеми подвійного призначення. Зазначені чинники сприяють підвищенню гнучкості, швидкості мобілізації та надійності постачання у Збройних силах Ізраїлю. Водночас з'ясовано як ключові переваги, так і наявні недоліки української логістичної системи: попри суттєві досягнення у сфері цифровізації та ефективної мобілізації волонтерського ресурсу, виявлено проблеми, пов'язані з недостатнім рівнем автономності бойових підрозділів, обмеженістю матеріально-технічних ресурсів і неефективністю механізмів державних закупівель. Запропоновано адаптацію ефективних елементів ізраїльської моделі до умов тривалого конфлікту в Україні шляхом впровадження інноваційних управлінських та цифрових рішень. Водночас Ізраїлю рекомендовано врахувати український досвід у сфері децентралізованої мобілізації та залучення громадянського сектору до процесів забезпечення обороноздатності держави.

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на створенні в Україні єдиної IT-орієнтованої системи логістичного управління, запровадженні блокчейн-технологій для прозорого обліку ресурсів, використанні штучного інтелекту для прогнозування потреб та оптимізації маршрутів, а також формуванні пілотних центрів інновацій на базі цивільно-військового партнерства. Адаптація ізраїльських рішень до українських умов може сприяти підвищенню автономності, стійкості та ефективності логістичної системи у тривалому конфлікті.

Висновки. Зіставлення ізраїльського та українського досвіду дозволяє сформулювати концептуальні орієнтири для розвитку військової логістики в Україні. Впровадження сучасних управлінських та технологічних рішень може значно посилити спроможності тилового забезпечення, підвищити ефективність управління ресурсами й забезпечити стійкість оборонної системи у тривалому конфлікті.

Ключові слова: військова логістика, національна безпека, гібридна війна, оборонні інновації, ЦАХАЛ, Збройні Сили України, технології подвійного призначення, децентралізоване управління, цивільно-військове партнерство.

Formulation of the problem. Modern armed conflicts demonstrate that effective military logistics plays a decisive role in achieving both operational and strategic success. Under conditions of dynamic combat environments and technological evolution, it is precisely logistical support that enables armed forces to maintain combat readiness, mobility, and resilience. In the context of the war in Ukraine, which began in 2022, the issue of logistical and rear

support has gained particular significance. Simultaneously, the experience of Israel — a country with longstanding expertise in defense and logistical operations — offers valuable insights into effective logistical models under wartime conditions. This highlights the relevance of the present study.

Analysis of Recent Research and Publications. Contemporary academic research confirms the increasing importance of military logistics as a core component

of defense capability in the context of hybrid warfare. Ukrainian and international scholars have focused on the experiences of countries involved in protracted conflicts — particularly Israel — and the feasibility of adapting their practices to the Ukrainian context. The works of Z. V. Hbur [14] and V. M. Bilichenko [15] explore the principles of operation of the Israel Defense Forces (IDF), including centralized command, technological autonomy, and human resource management, all of which have significant potential for implementation within the Armed Forces of Ukraine. I. Mitronov [16] emphasizes the necessity of modernizing material and technical support in response to the challenges of hybrid warfare, highlighting the role of logistical innovation and digital transformation of the rear. International studies (e.g., D. Brodet [4]; J. A. Gross [18]) focus on the innovative character of Israel's military economy, support for dual-use startups, and rapid technological deployment in the defense sector. Publications by E. Jaffe et al. [20] and Col T. Rasmussen [21] detail the efficiency of medical evacuation logistics and the involvement of civil actors in logistical support. Nevertheless, there remains a lack of integrated analysis that combines Ukrainian and Israeli experiences to construct a flexible and resilient logistics model.

The purpose of the study is to conduct a comparative analysis and identify the key features of military logistics in Ukraine and Israel, with the aim of determining effective strategies, innovative approaches, and prospects for enhancing national rear support systems in wartime conditions.

Presentation of the main material of the study. Military logistics refers to the comprehensive system responsible for supplying the armed forces with material resources, equipment, food, fuel, ammunition, medical assistance, transportation, and maintenance and repair operations. Its primary functions include supply, distribution, transportation, storage, and evacuation. Key criteria for effective logistics are timeliness, flexibility, reliability, and adaptability. A well-functioning logistics system ensures the continuity of combat operations and the operational autonomy of units in field conditions.

Structure of Military Logistics in Ukraine and Israel. Following the onset of Russia's full-scale aggression in 2022, Ukraine began a substantial transformation of its military logistics system. As of January 1, 2022, the **Logistics Forces** acquired the status of a separate branch within the Armed Forces of Ukraine. They were established on the basis of the **Logistics Forces Command**, which had been created in 2018 through the merger of the Rear and Armament structures. This command is responsible for supplying the troops with weapons, equipment, fuel, food, medical supplies, and infrastructure [1; 2].

The main subdivisions include: **Armament of the Armed Forces of Ukraine**, which is tasked with the supply and maintenance of weaponry; **Rear Services**

of the Armed Forces of Ukraine, which ensure the provision of material and technical means, including fuel, food, and other resources [1].

The **Israel Defense Forces (IDF)** employ a centralized logistics structure through the *Technology and Logistics Directorate of the General Staff (ATAL)*. This body is responsible for material and technical supply, transportation, medical logistics, and combat support. Its core departments include: the Logistics and Operations Department; the Ground Forces Logistics Command Department; the Ground Forces Human Resources Department; the Ground Forces Technology and Maintenance Department; the Armed Forces and Infrastructure Department [3].

In addition, Israel has integrated advanced technological solutions into its military logistics framework. Notably, elite units such as *Lakat* and *MAMRAM* have been established within the IDF to develop and implement IT solutions directly within the military infrastructure.

Financial Component of Military Logistics. The effective functioning of rear support systems requires substantial financial investment. In 2023, Ukraine allocated over 50% of its national budget to the defense sector, including more than USD30.8 billion specifically earmarked for arms procurement. This level of funding was made possible through the mobilization of internal financial resources and significant support from international partners. Among these, the United States played a leading role by providing over USD9.3 billion in direct military aid to Ukraine's defense sector [4].

Israel's defense budget has consistently exceeded USD23 billion annually, with USD3.8 billion covered by U.S. military aid. During the active phase of operations against Hamas in 2023–2024, Israel temporarily increased defense spending to approximately USD48 billion, a significant share of which was directed toward logistics, personnel medical care, and infrastructure modernization [5–6].

Specific Features of the Logistics System under Wartime Conditions in Ukraine. With the onset of Russia's full-scale invasion of Ukraine in February 2022, logistics emerged as a critical component of military strategy. The Armed Forces of Ukraine faced numerous logistical challenges, including the destruction of infrastructure, the need for rapid scaling of supply lines along an extended front, and shortages of equipment and medical evacuation resources. Russian shelling caused significant damage to transport infrastructure, particularly in Kharkiv Oblast, affecting roads, railways, and bridges [7].

A distinctive feature of Ukraine's wartime logistics has been the extensive involvement of volunteer organizations in supporting the armed forces. This led to the emergence of a parallel logistics system that encompasses fundraising, procurement, delivery, and distribution of equipment. Furthermore, digital tools

Table 1

Financial Characteristics of Military Logistics in Ukraine and Israel in 2023

Indicator	Ukraine	Israel
Total defense budget (2023)	Over USD30.8 billion	USD23.6 billion
Share of defense budget in total state budget	Over 50%	Up to 20% (temporarily increased to USD48 billion)
Main sources of logistics funding	State budget, assistance from the USA, EU, and Japan	State budget, U.S. military aid (USD3.8 billion annually)
Key areas of logistics expenditure	Equipment, drones, fuel, medical support, repair and maintenance	Bases, transportation, medical support, infrastructure, ammunition
Institutions responsible for logistics	Command of the Logistics Forces of the Armed Forces of Ukraine	Technology and Logistics Directorate (ATAL), IDF General Staff

Source: Systematized by the authors based on [4–6]

have played a crucial role in ensuring efficient and transparent military logistics under current wartime conditions. Applications such as Diia, the public procurement system Prozorro, and the UNITED24 platform have demonstrated significant potential in mobilizing financial resources, enhancing transparency, and improving the speed of procurement (Table 2).

For instance, the *Diia* application facilitated the collection of over USD5.6 million for the needs of the Armed Forces of Ukraine, including the purchase of bulletproof vests, drones, and technical equipment, which were subsequently transferred to the *Come Back Alive* foundation [8]. The *Prozorro* system has enabled a considerable increase in military transport procurement, with over UAH 8.1 billion spent in 2024 alone — double the amount allocated the previous year [7]. In addition, *Prozorro* has been instrumental in reforming military food supply systems and in facilitating large-scale drone procurements at competitive prices, thereby reducing corruption and improving quality assurance [8–10].

The *UNITED24* platform has become a centralized mechanism for funding defense initiatives. Notably, the *Army of Drones* project led to a hundredfold increase in the production and delivery of unmanned aerial vehicles. Moreover, *UNITED24* has been used for direct procurement of weapons, ammunition, and medical supplies, enabling a rapid response to evolving frontline needs [11–13].

Thus, digital platforms have become an integral part of Ukraine's military logistics system, enhancing its transparency, flexibility, and efficiency amidst armed conflict.

Additionally, despite a shortage of professional logisticians, Ukraine has successfully adapted its military infrastructure. This includes the establishment of humanitarian aid storage hubs, mobile repair units, and the deployment of drones to deliver ammunition and medical supplies to hard-to-reach areas.

Israel's Military Logistics System. The Israel Defense Forces (IDF) possess one of the most advanced military logistics systems in the world. A defining

Table 2

Comparative Analysis of the Military Logistics Systems of Ukraine and Israel

Criterion	Ukraine	Israel
Technological Base	Partially modernized	Highly technological
Centralization of Management	Limited, with numerous bottom-up initiatives	Highly centralized
Role of Volunteers	Crucial	Primarily state-driven logistics
Unit Autonomy	Limited	72-hour autonomous provisioning
Flexibility	High due to civil society initiatives	High due to automation
Logistics Personnel Training	Insufficient (prior to 2022)	Systematic professional training
Electronic Logistics System	In the process of development and implementation	Fully automated TAV system
Cargo Identification System	Limited use	RFID implemented at all logistics stages
Military IT Units	Concentrated within Ukroboronprom (mainly civilian sector)	MAMRAM, Lakat, MAFAT — integrated into the military structure
Arms Exports	Limited	Among the global top 10 arms exporters
Conversion of Military Technologies	Initial stage	Active (startups, exports)

Source: systematized by the authors based on [5; 14–16; 18; 20; 21]

characteristic of this system is its ability to mobilize significant resources within extremely short timeframes (Table 3). Combat units are equipped with autonomous reserves sufficient for 72 hours of operations, allowing them to function independently even in the event of disrupted communications with the rear [14].

The foundation of Israeli military logistics lies in centralized planning, a high degree of automation, and deep integration of IT solutions. All logistical processes — supply, transportation, maintenance, and medical evacuation — are coordinated by the Logistics Corps of the IDF. Particular attention is paid to the protection of rear bases and transportation routes, which is critically important given the constant threat from terrorist groups [14–16].

Israel is actively incorporating innovative technologies into its logistics operations, such as delivery drones, logistical UAVs, and autonomous parachute delivery systems capable of navigating to their destination independently, as well as robotic warehouses and AI-based demand forecasting systems. These innovations significantly enhance response speed and minimize operational losses [17].

A key element of Israel's model is the principle of self-reliance through high-tech solutions. For instance, the MAMRAM unit develops proprietary software, satellite systems, and communications technologies. The Lakat unit focuses on IT solutions tailored to the operational needs of the military. Consequently, knowledge and technological advancements originating in the defense sector are frequently converted into civil-

ian startups — such as Check Point and Mirabilis — demonstrating the dual-use effect of military innovation on the national economy. IDF logistics also rely on the TAV electronic logistics management system, which ensures comprehensive control over material flows, and on the use of RFID tags for real-time cargo tracking. This enhances transparency, accuracy, loss reduction, and overall supply chain efficiency [18; 19].

The practical effectiveness of this system was demonstrated during Operation “Protective Edge” (2014), when, despite massive rocket attacks, the IDF maintained uninterrupted supply of ammunition and fuel [20]. The medical evacuation system also functioned effectively, particularly through the implementation of the “golden hour” principle, which facilitated rapid treatment and improved survival rates. The Israeli emergency medical service Magen David Adom (MDA) provided aid to 842 wounded civilians under continuous rocket fire and challenging security conditions, reflecting the high level of preparedness and responsiveness of the evacuation system. Moreover, studies showed that during this operation, the rate of irreversible losses among wounded Israeli soldiers did not exceed 6%, marking a significant improvement compared to previous conflicts. This underscores the operational efficiency of Israel's military logistics and medical systems and serves as a potential model for the Armed Forces of Ukraine [21].

A comparative SWOT analysis of the logistics systems of Ukraine and Israel (Table 3) highlights substantial differences in terms of centralization, tech-

Table 3

SWOT Analysis of Military Logistics Systems: Ukraine vs. Israel

Criterion	Ukraine	Israel
Strengths	High flexibility and adaptability due to volunteer movement and horizontal initiatives; active modernization since 2022 (establishment of Logistics Forces, digitalization); adoption of Western (NATO-compatible) standards.	Automated TAV system and RFID-based tracking; presence of MAMRAM, Lakat, and MAFAT units integrated within the army; high level of centralization and digital logistics.
Weaknesses	Issues with centralized management and logistical planning; insufficient training of logistics officers prior to 2022; low automation and lack of a unified digital logistics platform; limited integration of inventory and communication systems; dependence on external aid and imports.	High cost of maintaining technological superiority; limited human resources in the high-tech sector.
Opportunities	Implementation of Israeli solutions in rear support (e.g., digital inventory and control systems similar to Israel's TAV); development of domestic digital platforms; integration of civilian IT solutions into logistics; conversion of military technologies into civilian sectors (startups, production); cooperation with NATO partners, experience exchange, and standards integration.	Further conversion of military innovations into startups; development of defense industry export potential; integration of AI into logistics.
Threats	Persistent cyberattacks targeting logistics infrastructure; high wear and tear of infrastructure; destabilization of rear areas due to missile strikes; insufficient funding under economic strain; corruption risks in logistics chains; lack of transparency in rear operations; excessive fragmentation among state, volunteer, and private suppliers.	Geopolitical instability; asymmetric threats (terrorist attacks, rear-area missile strikes); potential resource depletion during protracted conflicts.

Source: systematized by the authors on [1–22]

nological infrastructure, and the organization of rear operations. Israel, owing to its advanced digital infrastructure and the direct integration of innovative units within the army structure, has a clear advantage in automated resource management, transparency of logistics processes, and the conversion of military technologies into economic assets. Ukraine, on the other hand, demonstrates high adaptability, efficiency of civil society initiatives, and a strong potential for adopting best practices. The primary task for the Ukrainian logistics system remains overcoming structural fragmentation, minimizing the impact of the human factor, and implementing modern digital solutions at all levels of rear operations management.

To enhance the efficiency of military logistics, Ukraine should implement a comprehensive set of measures aimed at increasing the adaptability, transparency, and resilience of its logistics system under wartime conditions. Specifically, it is recommended to:

- establish a unified digital logistics management system that incorporates modern IT solutions, including cloud platforms, blockchain technologies, and artificial intelligence (AI) components;
- develop the institution of military logisticians and introduce interdisciplinary training programs that reflect technological advancements and emerging cyber threats;
- integrate volunteer and civil society initiatives into the state rear support system by ensuring their accountability and coordination with official structures;
- increase the autonomy of combat units through the deployment of mobile warehouses, field logistics centers, and autonomous supply systems;
- strengthen the resilience of logistics routes and infrastructure against enemy attacks, disruptions, and communication loss by utilizing backup digital channels, satellite monitoring, and cybersecurity measures.

Particular attention should be paid to the implementation of advanced digital technologies in rear support systems. Notably, blockchain technologies enable the creation of transparent, secure, and traceable logistics chains, thereby minimizing risks of corruption, losses, and duplication. These tools are already being deployed in several NATO countries and have demonstrated their effectiveness in managing defense supplies. In addition, the application of artificial in-

telligence—particularly in forecasting unit needs, dynamically optimizing supply routes, and assessing risks—significantly enhances the responsiveness and flexibility of logistics operations in constantly changing combat environments.

In conclusion, modern military logistics must evolve from a supporting function into a strategic instrument of advantage, ensuring not only uninterrupted supply but also enabling rapid response, mobility, and information superiority in armed conflict.

Conclusions and Future Research Directions.

The comparative analysis of the military logistics systems of Ukraine and Israel demonstrates that the efficiency of logistical support in modern warfare is largely determined by the degree of digitalization, the adaptability of organizational structures, and the integration of civilian resources into the defense infrastructure. The deployment of decentralized and technologically autonomous logistics frameworks—grounded in digital platforms and public-private partnerships—enhances the mobility, flexibility, and resilience of supply chains under conditions of high uncertainty.

The research has revealed key advantages of the Israeli model, including centralized logistical control, automated inventory management, and the effective operation of specialized digital units. These components may serve as a reference point for Ukraine in developing a unified, transparent, and innovation-driven logistics management system. Conversely, Ukraine's experience in mobilizing volunteer initiatives, utilizing digital tools (such as Prozorro, Diia, and UNITED24), and establishing alternative logistics routes offers valuable insights for states operating in multi-front or resource-constrained scenarios.

Further research should concentrate on the conceptualization and implementation of an integrated digital logistics management platform designed to ensure transparency, real-time control, and predictive functionality. Particular emphasis should be placed on the application of artificial intelligence for demand forecasting and route optimization, blockchain technologies for secure and transparent resource accounting, and the development of adaptive models of civil-military cooperation in logistics. Such advancements would significantly improve the sustainability and effectiveness of rear support systems in protracted conflicts and hybrid warfare environments.

Література

1. Про Збройні Сили України : Закон України від 06.12.1991 № 1934-XII. URL: <https://zakon.rada.gov.ua/laws/show/1934-12#Text> (дата звернення: 05.05.2025).
2. Про основи національного спротиву : Закон України від 16.07.2021 № 1702-IX. URL: <https://zakon.rada.gov.ua/laws/show/1702-20#Text> (дата звернення: 05.05.2025).
3. Israel Defense Forces — Logistics Department. *IDF Official Website*. URL: <https://www.idf.il>. (дата звернення: 05.05.2025).

4. The transformation of Ukraine's arms industry amid war with Russia. *Defense News*. URL: <https://www.defense-news.com/industry/2023/12/06/the-transformation-of-ukraines-arms-industry-amid-war-with-russia/> (дата звернення: 06.05.2025).
5. Brodet D. Israel Under Fire — The Israeli Economy during the October 7, 2023 War and Its Aftermath. *Jerusalem Center for Security and Foreign Affairs (JCFA)*. 2024, September 25. URL: <https://jcfa.org/article/the-israeli-economy-during-the-october-7-2023-war-and-its-aftermath> (дата звернення: 06.05.2025).
6. Israel Defense Market Report Overview. *GlobalData*. URL: <https://www.globaldata.com/store/report/israel-defense-market-analysis/> (дата звернення: 05.05.2025).
7. Ukraine. Kharkivska oblast: outlook and anticipated impacts. *ACAPS*. 2024. 20 December. URL: https://www.acaps.org/fileadmin/Data_Product/Main_media/20241220_ACAPS_Thematic_report_Ukraine_Kharkivska_oblast_outlook.pdf (дата звернення: 07.05.2025).
8. Ukrainians raise \$5.6 million for the military through Diia app. *The Kyiv Independent*. 2023. December 6. URL: <https://kyivindependent.com/ukrainians-raise-5-6-million-for-the-military-through-diia-app> (дата звернення: 07.05.2025).
9. Дорогі авто чи пікапи для ЗСУ: які машини купували в Prozorro у 2024 році. *Transparency International Ukraine*. 2024. 10 квітня. URL: <https://ti-ukraine.org/news/dorogi-avto-chy-pikapy-dlya-zsu-yaki-mashyny-kupuvaly-v-prozorro-u-2024-rotsi> (дата звернення: 08.05.2025).
10. Битва за харчування для ЗСУ: чи можливо зламати старі схеми? *Transparency International Ukraine*. 2023. 13 березня. URL: <https://ti-ukraine.org/blogs/the-battle-for-food-supplies-for-the-armed-forces-of-ukraine-can-the-old-schemes-be-broken/> (дата звернення: 08.05.2025).
11. Звіт про вплив — напрям «Захист». UNITED24. 2024. URL: <https://u24.gov.ua/impact-report/defend> (дата звернення: 06.05.2025).
12. Каневський Г. Закупівельні агенції Міноборони зможуть використовувати кошти UNITED24 для потреб ЗСУ. *Міністерство оборони України*. 2024. 07 березня. URL: <https://mod.gov.ua/en/news/procurement-agencies-of-the-ministry-of-defence-will-be-able-to-use-united-24-funds-for-the-needs-of-the-armed-forces-hlib-kanevskyi> (дата звернення: 05.05.2025).
13. UNITED24 використовує платформу SAP для закупівлі ліків та броньованих медичних автомобілів. *SAP*. 2024. URL: <https://www.sap.com/latinamerica/asset/dynamic/2024/04/f408ed77-ba7e-0010-bca6-c68f7e60039b.html> (дата звернення: 08.05.2025).
14. Гбур З.В. Принципи роботи армії оборони Ізраїлю та їх імплементація в Україні. *Державне управління: удосконалення та розвиток*. 2021. № 7. DOI: 10.32702/2307-2156-2021.7.1 (дата звернення: 07.05.2025).
15. Біліченко В.М. Ізраїльський досвід формування кадрового потенціалу збройних сил. *Публічне урядування*. 2022. № 5 (33). С. 11–15. [https://doi.org/10.32689/2617-2224-2022-5\(33\)-1](https://doi.org/10.32689/2617-2224-2022-5(33)-1).
16. Мітронов І. Модернізація матеріально-технічне забезпечення військ в умовах сучасної (гібридної) війни. URL: <http://webcache.googleusercontent.com/search?q=cache:szU5rFjApqsJ: novilidery.com/sites/default/files/2018> (дата звернення: 06.05.2025).
17. Inside the IDF's 'three-dimensional' supply delivery chain. *Jerusalem Post*. URL: <https://www.jpost.com/israel-news/article-827928> (дата звернення: 05.05.2025).
18. Gross J.A. How Israel's military is prioritizing dual-use start-ups to accelerate defense tech. *Breaking Defense*. 2023. July 25. URL: <https://breakingdefense.com/2023/07/how-israels-military-is-prioritizing-dual-use-start-ups-to-accelerate-defense-tech> (дата звернення: 08.05.2025).
19. IDF logistics revolution: Robots and drones to deliver war supplies. *Jerusalem Post*. 2024. October 10. URL: <https://www.jpost.com/israel-news/article-827928> (дата звернення: 07.05.2025).
20. Jaffe E., Wacht O., Strugo R. Operation Protective Edge — A Unique Challenge for a Civilian EMS Agency. *Prehosp Disaster Med*. 2015. № 30(5). P. 539–542 (дата звернення: 05.07.2025).
21. Rasmussen Col T., Baer Dr. D., Doll R., Carvalho J. In the "Golden Hour". 2015. URL: <https://mtcc-sc.org/wp-content/uploads/2017/08/ALT-2015-The-Golden-Hour.pdf> (дата звернення: 07.05.2025).

References

1. Pro Zbroini Syly Ukrainy: Zakon Ukrainy (1991). [Law of Ukraine "On the Armed Forces of Ukraine"] No. 1934-XII. URL: <https://zakon.rada.gov.ua/laws/show/1934-12#Text> [in Ukrainian].
2. Pro osnovy natsionalnoho sprotyvku: Zakon Ukrainy (2021). [Law of Ukraine "On the Fundamentals of National Resistance"]. No. 1702-IX. URL: <https://zakon.rada.gov.ua/laws/show/1702-20#Text> [in Ukrainian].
3. Israel Defense Forces — Logistics Department (2023). *IDF Official Website*. URL: <https://www.idf.il/>.
4. The transformation of Ukraine's arms industry amid war with Russia (2023, December 6). *Defense News*. URL: <https://www.defensenews.com/industry/2023/12/06/the-transformation-of-ukraines-arms-industry-amid-war-with-russia/>
5. Brodet D. (2024, September 25). Israel Under Fire — The Israeli Economy during the October 7, 2023 War and Its Aftermath. *Jerusalem Center for Security and Foreign Affairs (JCFA)*. URL: <https://jcfa.org/article/the-israeli-economy-during-the-october-7-2023-war-and-its-aftermath>.

6. Israel Defense Market Report Overview (2023). *GlobalData*. URL: <https://www.globaldata.com/store/report/israel-defense-market-analysis/>.
7. Ukraine. Kharkivska oblast: outlook and anticipated impacts (2024, December 20). *ACAPS*. URL: https://www.acaps.org/fileadmin/Data_Product/Main_media/20241220_ACAPS_Thematic_report_Ukraine_Kharkivska_oblast_outlook.pdf.
8. Ukrainians raise \$5.6 million for the military through Diia app. (2023, December 6). *The Kyiv Independent*. URL: <https://kyivindependent.com/ukrainians-raise-5-6-million-for-the-military-through-diia-app>.
9. Dorohi avto chy pikapy dlia ZSU: yaki mashyny kupuvaly v Prozorro u 2024 rotsi (2024, April 10). [Expensive cars or pickups for the Armed Forces of Ukraine: What vehicles were purchased through Prozorro in 2024?]. *Transparency International Ukraine*. URL: <https://ti-ukraine.org/news/dorogi-avto-chy-pikapy-dlya-zsu-yaki-mashyny-kupuvaly-v-prozorro-u-2024-rotsi/> [in Ukrainian].
10. Bytva za kharchuvannia dlia ZSU: chy mozhlyvo zlamaty stari skhemy? (2023, March 13). [The battle for food supplies for the Armed Forces of Ukraine: Can the old schemes be broken?]. *Transparency International Ukraine*. URL: <https://ti-ukraine.org/blogs/the-battle-for-food-supplies-for-the-armed-forces-of-ukraine-can-the-old-schemes-be-broken/> [in Ukrainian].
11. Zvit pro vplyv — napriam “Zakhyst” (2024). [Impact report — “Defense” direction]. *UNITED24*. URL: <https://u24.gov.ua/impact-report/defend> [in Ukrainian].
12. Kanevskyi, H. (2024, March 7). Zakupivelni ahentsii Minoborony zmozhut vykorystovuvaty koshty UNITED24 dlia potreb ZSU [Procurement agencies of the Ministry of Defense will be able to use UNITED24 funds for the needs of the Armed Forces]. *Ministerstvo oborony Ukrainy*. URL: <https://mod.gov.ua/en/news/procurement-agencies-of-the-ministry-of-defence-will-be-able-to-use-united-24-funds-for-the-needs-of-the-armed-forces-hlib-kanevskyi> [in Ukrainian].
13. UNITED24 vykorystovuie platformu SAP dlia zakupivli likiv ta bronovanykh medychnykh avtomobiliv (2024). [UNITED24 uses SAP platform to purchase medicines and armored medical vehicles] *SAP*. URL: <https://www.sap.com/latinamerica/asset/dynamic/2024/04/f408ed77-ba7e-0010-bca6-c68f7e60039b.html> [in Ukrainian].
14. Hbur, Z. V. (2021). Pryntsypy roboty armii oborony Izrailiu ta yikh implementatsiia v Ukraini. [Principles of work of the Israeli defense army and their implementation in Ukraine]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*. № 7. URL: <https://doi.org/10.32702/2307-2156-2021.7.1> [in Ukrainian].
15. Bilichenko, V.M. (2022). Izrail'skyi dosvid formuvannia kadrovoho potentsialu zbroinykh syl. [The Israeli experience of forming the personnel potential of the armed forces]. *Publichne uriaduvannia*. № 5(33). Pp. 11–15. [https://doi.org/10.32689/2617-2224-2022-5\(33\)-1](https://doi.org/10.32689/2617-2224-2022-5(33)-1) [in Ukrainian].
16. Mitronov, I. (2018). Modernizatsiia materialno-tekhnichne zabezpechennia viisk v umovakh suchasnoi (hibridnoi) viiny [Modernization of logistical support of troops under conditions of contemporary (hybrid) warfare]. URL: <http://web-cache.googleusercontent.com/search?q=cache:szU5rFjApqsJ:novilidery.com/sites/default/files/2018> [in Ukrainian].
17. Inside the IDF's ‘three-dimensional’ supply delivery chain. *Jerusalem Post*. URL: <https://www.jpost.com/israel-news/article-827928>.
18. Gross, J.A. (2023, July 25.). How Israel's military is prioritizing dual-use start-ups to accelerate defense tech. *Breaking Defense*. URL: <https://breakingdefense.com/2023/07/how-israels-military-is-prioritizing-dual-use-start-ups-to-accelerate-defense-tech>.
19. IDF logistics revolution: Robots and drones to deliver war supplies (2024, October 10). *Jerusalem Post*. URL: <https://www.jpost.com/israel-news/article-827928>.
20. Jaffe, E., Wacht, O., & Strugo, R. (2015). Operation Protective Edge — A Unique Challenge for a Civilian EMS Agency. *Prehosp Disaster Med*. № 30(5). Pp. 539–542.
21. Rasmussen, Col T., Baer, Dr. D., Doll, R. & Carvalho, J. (2015). In the “Golden Hour”. URL: <https://mtcc-sc.org/wp-content/uploads/2017/08/ALT-2015-The-Golden-Hour.pdf>.

Стаття надійшла до редакції 12.05.2025

УДК 351.004.7:364

Залізняк Вікторія Петрівна

*доктор наук з державного управління, професор,
завідувач кафедри публічного управління та адміністрування
Державний торговельно-економічний університет*

Zalizniuk Viktoriia

*Doctor of Sciences in Public Administration, Professor,
The Head of Public Administration Department
State University of Trade and Economics*

ORCID: 0000-0002-7014-0207

DOI: 10.25313/2617-572X-2025-5-10972

ІННОВАЦІЙНІ ПІДХОДИ ДО ПУБЛІЧНОГО АДМІНІСТРУВАННЯ СФЕРИ СОЦІАЛЬНОГО ЗАХИСТУ: ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

INNOVATIVE APPROACHES TO PUBLIC ADMINISTRATION OF SOCIAL PROTECTION: IMPLEMENTATION OF DIGITAL TECHNOLOGIES

Анотація. Вступ. Цифровізація публічного адміністрування є не лише засобом підвищення ефективності та якості надання послуг у сфері соціального захисту. Вона дозволяє розбудовувати більш людиноцентричний підхід до надання послуг, підвищуючи участь населення в їх формуванні, доступність для громадян, зокрема вразливих груп, та інклюзивність.

Метою статті є проведення аналізу сучасного стану цифровізації публічного адміністрування сфери соціального захисту в Україні, обґрунтування необхідності та шляхів забезпечення інклюзивності і людиноцентричного підходу в публічному адмініструванні сфери соціального захисту, дослідження можливостей та ризиків концепції «digital welfare state» для України на прикладі Данії.

В роботі використано методи статистичного аналізу, описовий та порівняльний методи.

У результаті проведеного дослідження було охарактеризовано ключові напрями цифрової трансформації у сфері соціального захисту, зокрема: автоматизацію процесів, що дозволяє знизити навантаження на працівників сфери соціального захисту; використання штучного інтелекту з метою аналізу та прогнозування потреб громадян; впровадження мобільних застосунків для доступу до соціальних послуг; електронне урядування, яке значно підвищує ефективність комунікації між державою та громадянами. Відзначено, що модернізація публічного управління в системі забезпечення соціального захисту в результаті впровадження новітніх технологій сприяє реалізації концепції людиноцентризму та інклюзивності. Охарактеризовано прогрес у сфері цифровізації системи публічного адміністрування в Україні, зокрема, в контексті відповідності вимогам Європейського Союзу, діяльності Міністерства цифрової трансформації України, розробки Індексу цифрової трансформації регіонів тощо. Зазначено ключові технології, що задіяні в процесі цифровізації публічного сектору України, особливе місце серед яких посідають цифрові державні платформи. Зауважено про найбільш відомі державні цифрові платформи України, зокрема, Урядовий портал, портал «Дія», «Документ», Портал «Дія. Безбар'єрність» тощо. Досліджено особливості, можливості та ризики концепції «digital welfare state» на прикладі Данії і наведено рекомендації для реалізації подальших цифрових трансформацій у сфері соціального захисту в Україні.

Перспективи подальших досліджень можуть стосуватися вивчення досвіду інших країн, зокрема, територіально та культурно близьких до України (Польща, Чехія тощо), у сфері цифровізації публічного адміністрування сфери надання послуг соціального захисту.

Ключові слова: публічне адміністрування, сфера соціального захисту, людиноцентричний підхід до надання послуг, цифрові технології, інклюзивність, Дія, digital welfare state.

Summary. Introduction. The digitalization of public administration is not only a means of increasing the efficiency and quality of service provision in the field of social protection, but also allows for the development of a more people-centered approach

to service provision, enhanced public participation in its formation, increased accessibility for citizens, particularly vulnerable groups, and greater inclusiveness.

The purpose of this work is to analyze the current state of digitalization in public administration within the field of social protection in Ukraine, to substantiate the need for and ways to ensure inclusiveness and a people-centered approach in public administration in this field, and to explore the opportunities and risks associated with the concept of a "digital welfare state" for Ukraine, using Denmark as an example.

The work used statistical analysis methods, including descriptive and comparative methods.

As a result of the research, the key areas of digital transformation in the field of social protection were characterized, in particular: automation of processes, which allows reducing the burden on social protection workers; use of artificial intelligence to analyze and predict the needs of citizens; introduction of mobile applications for access to social services; e-government, which significantly increases the efficiency of communication between the state and citizens. It is noted that the modernization of public administration in the social protection system through the introduction of the latest technologies contributes to the implementation of the concept of human-centredness and inclusiveness. Progress in the field of digitalization of the public administration system in Ukraine is characterized, in particular, in the context of compliance with the requirements of the European Union, the activities of the Ministry of Digital Transformation of Ukraine, the development of the Digital Transformation Index of Regions, etc. Key technologies in the process of digitalization of the public sector of Ukraine are indicated, among which digital state platforms occupy a special place. The most famous state digital platforms of Ukraine are noted, in particular, the Government Portal, the "Diya" portal, eDocument, and the "Diya.Bezbariarnist" portal, etc. The features, opportunities and risks of the "digital welfare state" concept are studied using the example of Denmark, and recommendations are given for the implementation of further digital transformations in the field of social protection in Ukraine.

Prospects for further research may include examining the experiences of other countries, particularly those with similar territorial and cultural characteristics to Ukraine, such as Poland and the Czech Republic, in the context of digitalization of public administration and social protection services.

Key words: public administration, social protection sphere, people-centered approach to service provision, digital technologies, inclusiveness, Diya, digital welfare state.

Постановка проблеми. Упровадження цифрових технологій у публічне адміністрування сфери соціального захисту є поширеною практикою серед передових країн світу, яка доводить свою ефективність у результаті підвищення ефективності, прозорості та інклюзивності. В Україні цифровізація публічного адміністрування сфери соціального захисту демонструє значного прогресу в останні роки, але особливо актуальною ця тема дослідження стала в контексті триваючої у країні війни. Вона утворила значні виклики для системи соціального захисту України, зокрема, в результаті зростання навантаження на систему соціальної підтримки, посилення незахищеності вразливих груп населення, ускладнення верифікації інформації тощо [1]. Зазначене актуалізує дослідження сучасного стану, передового досвіду та перспектив розвитку впровадження цифрових технологій у публічному адмініструванні сфери соціального захисту.

Аналіз останніх досліджень і публікацій. Процеси інновацій і модернізації національних державних адміністрацій займають провідне місце в процесі цифрового переходу, який переживає світ, тому дана проблематика залишається актуальною серед наукової спільноти. Так, К. Лоу, Дж. Ріголіні та Л. Солбес Кастро зазначили, що у багатьох країнах технології зараз відіграють значну і постійно зростаючу роль у наданні послуг соціального захисту. Цифровізація відбулася на всіх етапах ланцюга надання послуг соціального захисту як завдяки новим способам використання даних, так і завдяки

трансформації процесів за допомогою нових технологічних пристроїв і платформ [2]. Цифрова трансформація соціальної сфери стала одним з визначальних напрямів державної цифрової стратегії, спрямованої на формування ефективної сервісної цифрової держави [3]. У дослідженні Ф. М. Ідзі та Р. К. Гомес було проаналізовано, як цифрова ера управління впливає на уряди, які соціальні контракти слід враховувати в моделі цифрового управління, та якими є основні перешкоди цифрового управління для розробки державної політики [4]. Результати дослідження наслідків цифрового переходу на державне управління в Італії, з урахуванням досвіду Італійського національного інституту соціального забезпечення, були представлені у статті В. Бонаволонти та М. Д'Анджело [5]. У свою чергу, В. Ходаківська та ін. обґрунтували напрямки активізації впровадження цифрових технологій у державному управлінні на основі доказів позитивних наслідків їх впровадження для різних рівнів влади та населення [6]. Модель державного управління в цифровому форматі на прикладі «віртуальних організацій» державного сектору запропонували А. Хоададі та А. Аббаспур [7]. А. Скупіла та І. Мергель дослідили, як державні адміністрації використовують спільне виробництво для цифрової трансформації надання державних послуг і створення суспільної цінності в цьому процесі [8].

Незважаючи на численні наукові роботи з даної проблематики важливо продовжувати науковий пошук, адже недостатньо дослідженими в національному науковому полі залишаються такі напрями,

як концепція «digital welfare state», потенціал її застосованості в Україні, можливості та ризики; забезпечення інклюзивності та людиноцентричного підходу в публічному адмініструванні сфери соціального захисту.

Формулювання цілей статті (постановка завдання). Метою є проведення аналізу сучасного стану цифровізації публічного адміністрування сфери соціального захисту в Україні, обґрунтування необхідності та шляхів забезпечення інклюзивності і людиноцентричного підходу в публічному адмініструванні сфери соціального захисту, дослідження можливостей та ризиків концепції «digital welfare state» для України на прикладі Данії.

Виклад основного матеріалу. Швидкий розвиток технологій зумовлює суттєві трансформації у різних галузях діяльності людей, і сфера соціального захисту не є виключенням. Інноваційні підходи з використанням інформаційно-комунікаційних технологій (далі ІКТ) сприяють підвищенню якості та доступності надання послуг, створенню нових можливостей для громадян, а також підвищенню загальної ефективності публічного адміністрування. Серед ключових напрямів, за якими відбуваються трансформації, виокремлюють:

- автоматизацію процесів, що дозволяє знизити навантаження на працівників сфери соціального захисту, оптимізуючи витрати часу на здійснення різних операцій. Для отримувачів послуг автоматизація означає підвищення їх доступності в результаті впровадження систем електронного документообігу й автоматизації сервісів, що мінімізує бюрократичні перешкоди. Прикладом автоматизації є подання електронних заявок на отримання соціальних послуг;
- використання штучного інтелекту (ШІ) з метою аналізу та прогнозування потреб громадян, що дозволяє розробляти більш ефективні програми підтримки. Наприклад, ШІ здатен передбачати потреби у соціальних послугах у різних регіонах залежно від місцевих соціальних, демографічних та інших чинників. Ще одним напрямом використання ШІ є виявлення за його допомогою випадків шахрайства у сфері соціального захисту;
- впровадження мобільних застосунків для доступу до соціальних послуг, що значно спрощує та підвищує зручність процесу їх отримання. Такі застосунки не лише надають інформацію про можливості отримання соціальних послуг, але і дозволяють подавати заявки онлайн і відстежувати їхній статус;
- електронне урядування, що значно підвищує ефективність комунікації між державою та громадянами, доступність соціальних послуг і
- прозорість управління.

Через єдині портали державних послуг громадянам надається інформація про їхні соціальні права й обов'язки, також вони можуть бути пристосовані до подачі документів і звернень за їх допомогою [9].

Більше того, створення інформаційних державних порталів може бути спрямоване на те, щоб делегувати частину функцій державного контролю суспільству та некомерційним організаціям, що підвищить як прозорість витрат, так і ступінь залучення населення до управлінських процесів. Це дозволяє більш ефективно застосовувати інструментів електронної демократії, участь громадян у процесах державного управління та прийняття державних рішень, ефективно використання ІКТ та підвищення ефективності системи надання адміністративних послуг у цілому [10].

Відтак, можна стверджувати, що модернізація публічного управління в системі забезпечення соціального захисту в результаті впровадження новітніх технологій сприяє реалізації концепції людиноцентризму, яка заснована на ідеї людини як центрального елементу будь-яких систем управління. У контексті соціального захисту це також означає, що громадяни не тільки отримують соціальні послуги, але і беруть активну участь у їх створенні. У світі існує чимало моделей систем соціального захисту, що пояснює існування численних підходів до модернізації цих систем. Проте можна виокремити деякі загальні принципи модернізації, згідно яких тією чи іншою мірою мають відбуватися процеси трансформації, зокрема: орієнтація на людину та забезпечення максимальної доступності послуг; інклюзивність, яка передбачає рівний доступ до послуг усіх верств населення, особливо найбільш уразливих; інноваційність і впровадження новітніх технологій для покращення якості надання послуг та прозорості управління; партнерство між державою та громадянами, що полягає в залученні останніх до процесів управління державою та прийняття державних рішень. Окрім того, людиноцентрична модель модернізації публічного управління в системі забезпечення соціального захисту має неодмінно враховувати такі аспекти, як підтримка вразливих соціальних груп, посилення довіри до держави шляхом забезпечення прозорості та підзвітності, гнучкості й адаптивності до поточних і потенційних викликів [11].

Останнє десятиріччя стало свідком суттєвого прогресу у сфері цифровізації системи публічного адміністрування в Україні. Зусилля нашої країни щодо виконання своїх зобов'язань у сфері електронних комунікаційних послуг були відзначені Європейським Союзом (ЄС), співпраця з яким відбувається, окрім іншого, в рамках загально-європейської Програми Digital Europe до 2027 року. Центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері цифровізації є Міністерство цифрової трансформації України (Мінцифри) [12]. Мінцифри є відповідальним за цифровізацію державних послуг (зокрема, додаток Дія), розвиток цифрової інфраструктури, впровадження електронного урядування, розвиток IT-галузі, кібербезпеку та захист даних, розвиток цифрової освіти

тощо. В умовах триваючої війни в Україні Мінцифри продовжує роботу над забезпеченням безперервності електронних послуг, цифровою допомогою внутрішньо переміщеним особам (ВПО) та особам, що постраждали від війни, запуском ініціатив на міжнародному рівні, протидією інформаційним загрозам і кібербезпекою. Регіональною командою Мінцифри було розроблено Індекс цифрової трансформації регіонів, що охоплює такі складові: інституційна спроможність, розвиток Інтернету, розвиток центрів надання адміністративних послуг (ЦНАП), упровадження режиму «без паперів», цифрова освіта, візитівка області, проникнення базових е-послуг, галузева цифрова трансформація, індивідуальні проекти Chief Digital Transformation Officers — заступників керівників центральних органів виконавчої влади, обласних, Київської та Севастопольської міських держадміністрацій з питань цифрового розвитку, цифрових трансформацій і цифровізації [13]. Станом на 2024 рік області України отримали такі результати за інтегральною оцінкою Індексу цифрової трансформації регіонів (рис. 1).

Основними технологіями в процесі цифровізації публічного сектору України є цифрові державні платформи, відкриті дані, електронна ідентифікація громадян, цифрове робоче місце, Інтернет речей, блокчейн тощо. Серед перелічених технологій цифрові державні платформи посідають окреме місце, адже часто інтегрують у собі всі інші зауважені інструменти. Більше того, саме через цифрові платформи громадяни отримують доступ до адміністративних послуг, довідкової інформації і комунікації із представниками органів влади. Цифрові платформи здатні підвищити якість надання послуг соціального захисту, оптимізувати внутрішні процеси та скоротити витрати. В Україні функціонують такі державні цифрові платформи, як Урядовий пор-

тал, портал «Дія», «Документ», Портал «Дія.Безбар'єрність», Платформи ««Допомога», «Взаємодія» та «Дія.Бізнес» (для допомоги з релокації бізнесу). У 2023 році урядом було схвалено постанову, яка зобов'язує державні органи забезпечити доступність веб сайтів згідно з міжнародними вимогами. Це дозволяє зробити ці веб ресурси більш інклюзивними, адже контент сайтів має бути доступним для людей із порушеннями зору, слуху чи моторики [12]. Ініціативи з вебдоступності реалізовані в межах проекту «Цифрові, інклюзивні, доступні: Підтримка цифровізації державних послуг в Україні (Проект підтримки Дія)». Цей проект, профінансований Швецією, реалізує Програма розвитку ООН (UNDP) в Україні. Друга фаза проекту почалася з 1 січня 2024 року. Мета проекту — подолання цифрового розриву між поколіннями та різними соціальними групами, забезпечуючи користування новими цифровими рішеннями й електронними послугами для кожного українця [14]. Безбар'єрність є основним принципом цифрової інклюзії, гарантуючи, що всі користувачі мають рівні можливості використовувати ІКТ для збільшення своєї продуктивності, покращення навичок та підвищення якості життя. Безбар'єрний державний портал «Дія.Цифрова освіта» сприяє зростанню інноваційного потенціалу країни, стимулюючи інтерес до навчання серед молоді, світчерів та ВПО, а також є доступним для людей з інвалідністю та старшого покоління [12]. У контексті війни в Україні забезпечення інклюзивності через цифрові державні портали набуває особливого значення, забезпечуючи більш ефективний соціальних захист ветеранів і їхніх сімей. На порталі «Дія» для ветеранів, членів їхніх сімей і сімей загиблих захисників доступні такі сервіси, як подання заяви про грант для створення або розвитку ветеранського бізнесу, подання заяви на призначення пенсії для військовослужбовця або

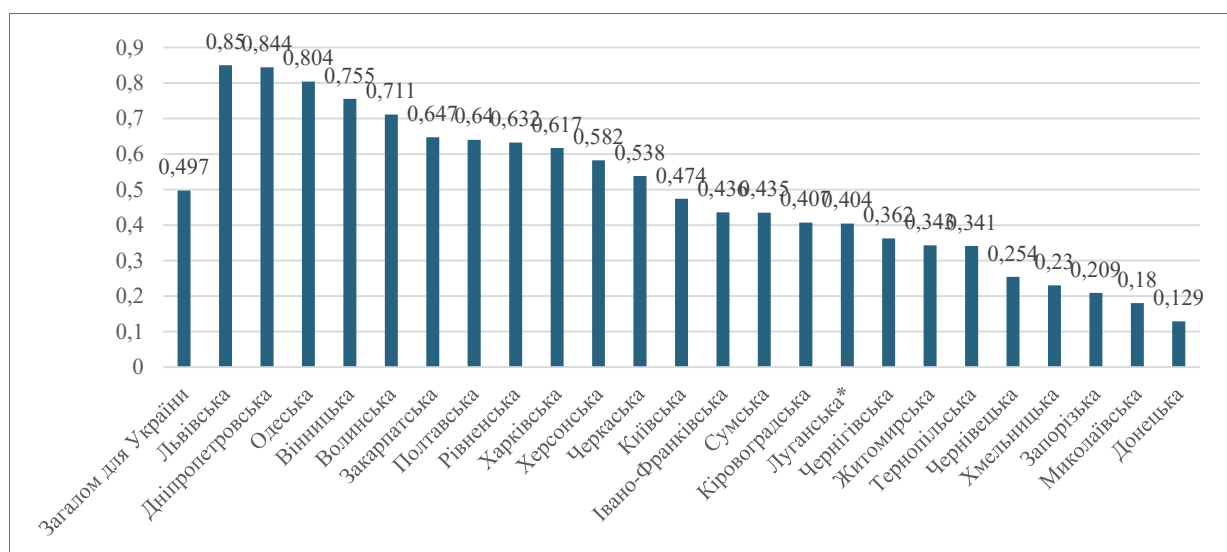


Рис. 1. Індекс цифрової трансформації регіонів України у 2024 році

Джерело: побудовано автором за даними [13]

на основі інвалідності, отримання електронного пенсійного посвідчення тощо [15].

Забезпечуючи організацію управління у сфері соціального захисту, цифрові державні платформи є ключовим елементом моделі «digital welfare state». Концепція «digital welfare state» полягає в перетворенні традиційної соціальної системи на цифрову екосистему, в якій усі етапи соціального захисту, в тому числі моніторинг і здійснення виплат, реалізуються із використанням цифрових технологій. Серед яскравих прикладів «digital welfare state» можна навести Данію як лідера цифровізації із високо цифровізованим державним сектором і населенням з високим рівнем цифрової грамотності та довіри до державного сектору. Також Данія має розвинену систему соціального захисту, для якої характерний високий рівень державних витрат (рис. 2). Саме тому приклад Данії може надати корисні інсайти щодо впровадження інновацій і цифрових технологій у публічному адмініструванні сфери соціального захисту в Україні як в контексті можливостей, так і з огляду на потенційні ризики.

Протягом останніх 25 років уряд Данії розгорнув технології для полегшення державного управління та надання послуг у широкому діапазоні сфер від систем розгляду справ і самообслуговування громадян до догляду за дітьми, державних шкіл та медичних працівників. Данія має добре розвинену цифрову інфраструктуру: високе покриття мереж і широкосмуговий зв'язок, цифрову поштову скриньку для комунікації між громадянами й органами влади, а також широко впроваджене рішення eID (NemID).

Дослідження данських стратегій цифровізації із середини 1990-х років до 2015 року показують, що вони представляють два типи наративів. Перший набір політик розглядав цифровізацію як суспільний проект, заснований на солідарності, громадянських

правах, місцевій участі й освіті. Згодом фокус поступово змістився на цифровізацію як засіб створення більш економічно ефективного державного адміністрування, в якому громадяни все більше покладаються на електронне спілкування та цифрове самообслуговування.

Нещодавно системи штучного інтелекту в Данії були включені в політичне бачення як засіб подальшого розвитку та розширення цифровізації державного сектору. Датське агентство цифровізації підкреслило, що ШІ використовуватиметься лише там, де він «забезпечить цінність для громадян» та за умов етичної відповідальності, таким чином укладаючи свою стратегію в рамки дискурсу ЄС про етичний ШІ. Проекти ШІ стали частиною національної стратегії Данії щодо штучного інтелекту, яка містить 24 ініціативи в державному та приватному секторах. У цій стратегії, зокрема, пропонується, щоб Данія дотримувалася загальної етичної і людиноцентричної рамки для ШІ, а державний сектор використовував цю технологію для надання послуг світового рівня.

Що стосується громадян, то стратегія виокремлює більш індивідуальне обслуговування (наприклад, розпізнавання голосу для екстрених викликів), інтелектуальних помічників, які допомагають читати та слухати, а також кращу підтримку в центрах обслуговування громадян у муніципалітетах. У стратегії зазначається, що ШІ піднімає «етичні питання» щодо балансу між перевагами нових технологій і дотриманням основних прав людини, належного процесу та соціальних цінностей Данії.

Водночас, проекти з підписом «AI Signature» усе ще перебувають на ранніх стадіях, проте вже демонструють певну напругу, пов'язану з широким впровадженням автоматизованих систем у держсекторі. В епоху інтенсивної обробки даних ризик розширен-

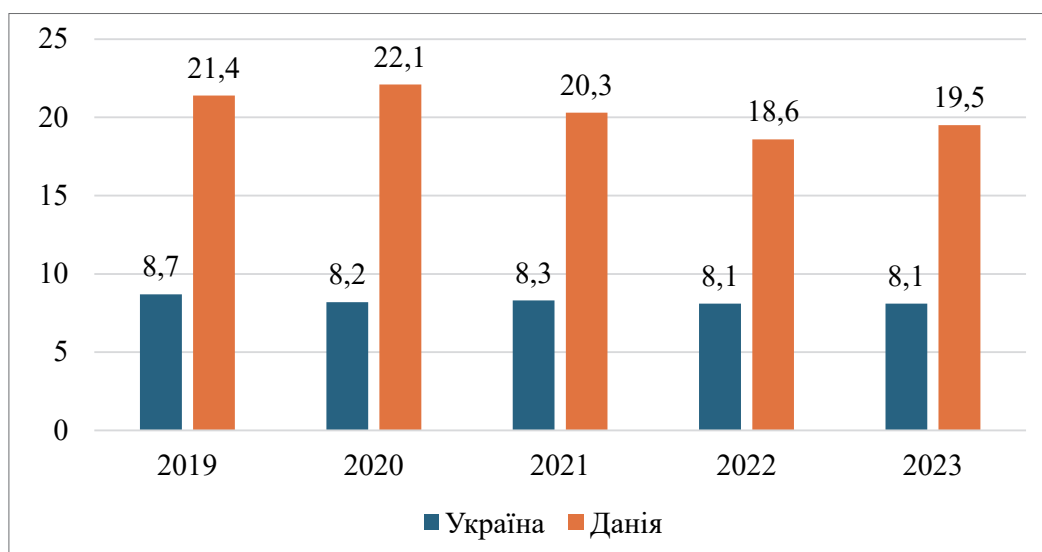


Рис. 2. Витрати на соціальний захист в Данії та Україні, % від валового внутрішнього продукту (ВВП)

Джерело: побудовано автором за даними [9; 16]

ня інформаційної асиметрії та асиметрії влади між особою і державою стає вагомим чинником, який може ще більше підживлюватися оптимістичними наративами про те, чого може досягти управління, кероване даними. Розвиток у напрямку «digital welfare state» та все більша увага до автоматизованих рішень як частини надання державних послуг і контролю над соціальними виплатами ефективно розгортає той самий тип аналітики даних, який технологічні гіганти розгортають у комерційних цілях, щоб орієнтуватися та впливати на поведінку своїх користувачів. Подібним чином це може призвести до максимізації даних, профілювання особи, інвазивних засобів стеження та прогнозування громадян і, зрештою, позбавлення прав залежно від того, як державний сектор розробляє та розгортає свій проєкт цифрового добробуту. Оскільки держава має повноваження та засоби для прямого втручання в життя своїх громадян, її застосування аналітики даних може призвести до спостереження в державному секторі, якщо тільки немає чіткої політичної мети не йти цим шляхом [17].

Порівнюючи досвід Данії та України у сфері цифровізації публічного адміністрування, можна зауважити декілька важливих аспектів.

По-перше, довіра до держави в Данії, зокрема, у сфері цифровізації соціальних послуг, є досить високою, як і рівень цифрової грамотності населення. Ці показники для України є помітно нижчими, проте прогрес, досягнутий у межах проєктів «єДопомога» та «Дія» є значним, адже мільйони громадян активно користуються мобільними додатками для отримання соціальних виплат, реєстрації бізнесу та інших послуг.

По-друге, країни використовують дещо відмінні моделі надання послуг. Хоча обидві країни застосовують принцип «one-stop shop», у Данії він реалізований через кілька спеціалізованих веб-порталів (єдину цифрову поштову скриньку, eID (NemID) та інтегровані портали), а в Україні через веб портал «Дія». Ключові відмінності в підходах двох держав полягають у більшому акценті на міжгалузевій аналітиці та прогнозуванні потреб у Данії і швидкості запуску сервісів та масштабованості мобільних рішень в Україні.

По-третє, залишається суттєвий розрив у рівні розвитку інфраструктури та технологій у досліджу-

ваних державах, а також у закріпленні етичних рамок використання таких технологій як ШІ, та у законодавчому регулюванні. Як було зауважено, етична стратегія ШІ закріплена в національній політиці Данії, тоді як в Україні подібні законодавчі ініціативи знаходяться на етапі розвитку. Зрештою, такий стан речей віддзеркалюється в підвищенні ефективності на фактичних результатах, адже для Данії середній час обробки запиту становить декілька днів, а охоплення соціальних послуг понад 95%. Натомість в Україні платформи «Дія» і «єДопомога» дозволили зменшити час розгляду заяв із кількох тижнів до 3–5 днів, охопивши понад 7 млн. громадян, і значно покращили доступність послуг навіть у віддалених громадах.

Висновки та перспективи подальших досліджень. Цифровізація публічного адміністрування є не лише засобом підвищення ефективності та якості надання послуг в сфері соціального захисту. Вона дозволяє розбудовувати більш людиноцентричний підхід, підвищуючи залученість населення у їх формуванні, доступність для громадян, зокрема, вразливих груп, та інклюзивність. З огляду на проведений у статті аналіз, можна запропонувати такі рекомендації для України:

- підвищувати довіру громадян до держави шляхом підвищення прозорості процесів та ефективної комунікації;
- забезпечувати інклюзивність та індивідуальний підхід у комунікації із громадянами;
- доцільно проводити ширше інформування населення про наявні соціальні послуги та способи їх отримання;
- етичні стандарти ШІ мають бути закріплені у національних стратегіях;
- ризики надмірного втручання з боку держави мають бути попереджені в результаті надання гарантії прозорості алгоритмів, закріплення права на пояснення рішень і механізмів оскарження, обмеження обсягу збору даних та захист персональної інформації.

Подальші напрями досліджень можуть стосуватися вивчення досвіду інших країн, зокрема, територіально та культурно близьких до України (Польща, Чехія тощо), у сфері цифровізації публічного адміністрування сфери надання послуг соціального захисту.

Література

1. Проект Плану відновлення України: матеріали робочої групи «Соціальний захист». Кабінет Міністрів України, 2022. 32 с. URL: <https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/social-protection.pdf> (дата звернення: 06.05.2025).
2. Lowe C., Rigolini J., Solbes Castro L. Pathways toward digitalization in Social Protection and Labor (SPL) service delivery: Social protection & jobs discussion paper No. 2307. World Bank, 2023. 55 p. URL: <https://documents1.worldbank.org/curated/en/099100523151038686/pdf/P173530036a7f30f60899c06a6172040bf3.pdf> (дата звернення: 06.05.2025).
3. Малиновський В. Я. Стратегічні аспекти цифрової трансформації соціальної сфери. *Соціально-економічні проблеми сучасного періоду України*. 2021. № 1. С. 27–31. URL: <https://doi.org/10.36818/2071-4653-2021-1-4> (дата звернення: 06.05.2025).
4. Idzi F. M., Gomes R. C. Digital governance: government strategies that impact public services. *Global Public Policy and Governance*. 2022. Vol. 2, No. 4. P. 427–452. URL: <https://doi.org/10.1007/s43508-022-00055-w> (дата звернення: 06.05.2025).
5. Bonavolontà V., D'Angelo M. Digital transition and public administration in Italy: the experience of the Italian National Social Security Institution — INPS. *Ubezpieczenia Społeczne. Teoria i praktyka*. 2021. No. 4. P. 87–101. URL: <http://dx.doi.org/10.5604/01.3001.0015.5236> (дата звернення: 06.05.2025).
6. Implementation of digital technologies in public administration / V. U. Khodakivska et al. *Revista de la universidad del Zulia*. 2023. Vol. 14, No. 39. P. 295–312. URL: <http://dx.doi.org/10.46925/rdluz.39.16> (дата звернення: 06.05.2025).
7. Khodadadi A., Abbasspour A. Modeling digital governance in virtual organizations in the public sector: A case study of the Social Security Insurance Organization. *Political Sociology of Iran*. 2022. Vol. 5, No. 12. P. 3231–3246. URL: <https://doi.org/10.30510/psi.2022.339758.3407> (дата звернення: 06.05.2025).
8. Scupola A., Mergel I. Co-production in digital transformation of public administration and public value creation: The case of Denmark. *Government Information Quarterly*. 2022. Vol. 39, No. 1. Article 101650. URL: <https://doi.org/10.1016/j.giq.2021.101650> (дата звернення: 06.05.2025).
9. Цифрові рішення та інноваційні підходи в сфері соціального забезпечення / С. Ю. Соколюк та ін. *Збірник наукових праць Уманського національного університету*. 2024. № 105 (2). С. 63–73. URL: <https://doi.org/10.32782/2415-8240-2024-105-2-63-73> (дата звернення: 06.05.2025).
10. Innovative technologies for the public administration transformation / V. Dovhan et al. *Studies of Applied Economics*. 2021. Vol. 39, No. 5. URL: <https://doi.org/10.25115/eea.v39i5.4945> (дата звернення: 06.05.2025).
11. Линдюк С. Інновації у публічному управлінні для забезпечення соціальної безпеки. *Науковий вісник: Державне управління*. 2024. № 2 (16). С. 114–136. URL: [https://doi.org/10.33269/2618-0065-2024-2\(16\)-114-136](https://doi.org/10.33269/2618-0065-2024-2(16)-114-136) (дата звернення: 06.05.2025).
12. Чечель А., Микита А. Стратегічні цифрові технології у публічному секторі України. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 9. С. 176–185. URL: <https://doi.org/10.31470/2786-6246-2024-9-176-185> (дата звернення: 06.05.2025).
13. Індекс цифрової трансформації регіонів України: підсумки 2024 року. Міністерство цифрової трансформації України, 2024. 28 с. URL: <https://thedigital.gov.ua/storage/uploads/files/page/community/reports/ІНДЕКС%202024%202%201.pdf> (дата звернення: 06.05.2025).
14. Digital, inclusive and accessible support to the digitalisation of public services in Ukraine (Diia Support Project). *United Nations Development Programme Ukraine*. URL: <https://www.undp.org/uk/ukraine/projects/digital-inclusive-accessible-support-digitalisation-public-services-ukraine-dia-support-project> (дата звернення: 06.05.2025).
15. Грант для ветеранів та членів їхніх сімей. *Дія*. URL: https://diia.gov.ua/services/grant-dlya-veteraniv-ta-chleniv-yihnih-simej?utm_source=chatgpt.com (дата звернення: 06.05.2025).
16. Government expenditure by function (COFOG). *Eurostat*. URL: https://ec.europa.eu/eurostat/databrowser/view/gov_10a_exp/default/table?lang=en (дата звернення: 06.05.2025).
17. Jørgensen R. F. Data and rights in the digital welfare state: the case of Denmark. *Information, Communication & Society*. 2023. Vol. 26, No. 1. P. 123–138. URL: <https://doi.org/10.1080/1369118X.2021.1934069> (дата звернення: 06.05.2025).

References

1. Kabinet Ministriv Ukrainy. (2022). *Proekt Planu vidnovlennia Ukrainy: Materialy robochoi hrupy "Sotsialnyi zakhyst"* [Project of Ukraine's Recovery Plan: Materials of the working group "Social Protection"]. URL: <https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/social-protection.pdf> [in Ukraine].
2. Lowe, C., Rigolini, J., Solbes Castro, L. (2023). *Pathways toward digitalization in Social Protection and Labor (SPL) service delivery (Social Protection & Jobs Discussion Paper No. 2307)*. World Bank. URL: <https://documents1.worldbank.org/curated/en/099100523151038686/pdf/P173530036a7f30f60899c06a6172040bf3.pdf>.
3. Malynovskyi, V. Ya. (2021). Stratehichni aspekty tsyfrovoyi transformatsii sotsialnoi sfery [Strategic aspects of digital transformation in the social sphere]. *Sotsialno-ekonomichni problemy suchasnoho periodu Ukrainy*. No. 1. Pp. 27–31. URL: <https://doi.org/10.36818/2071-4653-2021-1-4> [in Ukraine].

4. Idzi, F. M., Gomes, R. C. (2022). Digital governance: government strategies that impact public services. *Global Public Policy and Governance*, No. 2(4), Pp. 427–452. URL: <https://doi.org/10.1007/s43508-022-00055-w>.
5. Bonavolontà, V., D'Angelo, M. (2021). Digital transition and public administration in Italy: the experience of the Italian National Social Security Institution — INPS. *Ubezpieczenia Społeczne. Teoria i praktyka*, No. 4, Pp. 87–101. URL: <http://dx.doi.org/10.5604/01.3001.0015.5236>.
6. Khodakivska, V. U., Prystupa, L., Ivanyshyna, O., Panura, I., & Tuchak, T. (2023). Implementation of digital technologies in Public Administration. *Revista de la Universidad del Zulia*, Vol. 14, No. 39, Pp. 295–312. URL: <http://dx.doi.org/10.46925/rdluz.39.16>.
7. Khodadadi, A., Abbasspour, A. (2022). Modeling digital governance in virtual organizations in the public sector: A case study of the Social Security Insurance Organization. *Political Sociology of Iran*, Vol. 5, No. 12, Pp. 3231–3246. URL: <https://doi.org/10.30510/psi.2022.339758.3407>.
8. Scupola, A., Mergel, I. (2022). Co-production in digital transformation of public administration and public value creation: The case of Denmark. *Government Information Quarterly*, Vol. 39, No. 1, Pp. 101650. URL: <https://doi.org/10.1016/j.giq.2021.101650>.
9. Sokoliuk, S. Yu., Prokopchuk, O. T., Zharun, O. V., Korotieiev, M. A., Maksymenko, S. M. (2024). Tsyfrovi rishennia ta innovatsiini pidkhody v sferi sotsialnoho zabezpechennia [Digital solutions and innovative approaches in social security]. *Collection of scientific papers of Uman National University*, No. 105(2). Pp. 63–73. URL: <https://doi.org/10.32782/2415-8240-2024-105-2-63-73> [in Ukraine].
10. Dovhan, V., Hrushchynska, N., Kudrina, O., Bozhkova, V., Zaporozhets, T., Makarenko, M. (2021). Innovative technologies for the public administration transformation. *Studies of Applied Economics*, Vol. 39, No. 5. URL: <https://doi.org/10.25115/eea.v39i5.4945>.
11. Lindyuk, S. (2024). Innovatsii u publichnomu upravlinni dla zabezpechennia sotsialnoi bezpeky [Innovations in public administration for ensuring social security]. *Naukovyi visnyk: Derzhavne upravlinnia*, No. 2(16), Pp. 114–136. URL: [https://doi.org/10.33269/2618-0065-2024-2\(16\)-114-136](https://doi.org/10.33269/2618-0065-2024-2(16)-114-136) [in Ukraine].
12. Chechel, A., Mykyta, A. (2024). Stratehichni tsyfrovi tekhnolohii u publichnomu sektori Ukrainy [Strategic digital technologies in Ukraine's public sector]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia*, No. 9, Pp. 176–185. URL: <https://doi.org/10.31470/2786-6246-2024-9-176-185> [in Ukraine].
13. Ministerstvo tsyfrovoy transformatsii Ukrainy. (2024). *Indeks tsyfrovoy transformatsii rehioniv Ukrainy. Indeks 2024* [Index of digital transformation of Ukrainian regions. Index 2024]. URL: <https://thedigital.gov.ua/storage/uploads/files/page/community/reports/ИНДЕКС%202024%20%201.pdf>Problecon [in Ukraine].
14. United Nations Development Programme Ukraine. (2024). *Digital, inclusive and accessible support to the digitalisation of public services in Ukraine (Diia Support Project)*. URL: <https://www.undp.org/uk/ukraine/projects/digital-inclusive-accessible-support-digitalisation-public-services-ukraine-dia-support-project>
15. Ministry of Digital Transformation of Ukraine. (2025). *Grant dla veteraniv ta chleniv yikhnikh simei* [Grant for veterans and their family members]. Diia. URL: https://diia.gov.ua/services/grant-dlya-veteraniv-ta-chleniv-yihnih-simej?utm_source=chatgpt.com
16. Eurostat. (n.d.). *Government expenditure by function (COFOG)*. URL: https://ec.europa.eu/eurostat/databrowser/view/gov_10a_exp/default/table?lang=en
17. Jørgensen, R. F. (2023). Data and rights in the digital welfare state: the case of Denmark. *Information, Communication & Society*, Vol. 26, No. 1. Pp. 123–138. URL: <https://doi.org/10.1080/1369118X.2021.1934069>.

Стаття надійшла до редакції 11.05.2025

Луковський Роман Ігорович

*аспірант кафедри адміністративного та фінансового менеджменту
Національного університету «Львівська політехніка»*

Lukovsky Roman

*Postgraduate Student of the Department of Administrative and Financial Management
Lviv Polytechnic National University*

ORCID: 0009-0009-3269-7467

Парійчук Вікторія Анатоліївна

*асистент кафедри адміністративного та фінансового менеджменту
Національний університет «Львівська політехніка»*

Pariichuk Viktoriia

*Assistant of the Department of Administrative and Financial Management
Lviv Polytechnic National University*

ORCID: 0000-0003-3892-6362

DOI: 10.25313/2617-572X-2025-5-11027

ПРОЦЕСИ ДІДЖИТАЛІЗАЦІЇ ПІД ЧАС ЗАПРОВАДЖЕННЯ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ЯК ВАЖЛИВИЙ ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ПУБЛІЧНОГО УПРАВЛІННЯ

DIGITALIZATION PROCESSES DURING THE IMPLEMENTATION OF THE LEGAL REGIME OF MARTYR STATE AS AN IMPORTANT TOOL FOR ENSURING EFFECTIVE PUBLIC ADMINISTRATION

Анотація. Вступ. З виникненням перших цифрових пристроїв наприкінці ХХ століття, запустився незворотний процес діджиталізації, а з появою інтернету та смартфонів вона набула масового характеру. Штучний інтелект, Big Data, інтернет, хмарні сервіси постійно розвиваються й отримують дедалі більше сфер застосування, в тому числі в сфері сучасного публічного управління. Новому етапу розвитку діджиталізації сучасного публічного управління посприяла коронавірусна пандемія. Швидкий перехід на віддалений формат роботи дозволив органам публічного управління продовжити ефективно працювати. А з початком повномасштабного вторгнення Росії хмарні сервіси допомогли зберегти критично важливі дані для органів публічного управління України.

З метою дотримання рівноваги при реалізації стратегії розвитку держави потребує впливу управлінського персоналу шляхом прийняття виважених науково-обґрунтованих управлінських рішень. Прийняття таких рішень можливе лише на основі фактичних, актуальних інформаційних даних про реальний стан діяльності органів публічної влади. Побудувати ефективну модель сучасних управлінських процесів неможливо без використання цифрових технологій.

Реалізація основних напрямків розвитку держави згідно із вимогами міжнародних угод та договорів і намічених цілей розвитку держави можливе через активне впровадження діджиталізації в систему публічного управління. Отже, роль діджиталізації в публічному управлінні є безперечно значною. Формування цифрової інфраструктури – шлях до виконання намічених цілей держави та реалізації ефективних управлінських процесів.

Мета. Метою написання статті є дослідження сучасного стану діджиталізації як важливого інструменту формування сучасного публічного управління в умовах воєнного стану.

Матеріали і методи. Матеріалами дослідження є: нормативно-правові акти України, монографії та наукові статті, присвячені питанням сучасних наукових підходів щодо модернізації публічного управління в умовах цифрових тран-

сформаций суспільства, використанню світового досвіду гіджиталізації як стратегічного напрямку оптимізації публічного управління, а також напрямкам розвитку гіджиталізації для формування ефективного публічного управління.

Методи дослідження: описовий, порівняльний, аналіз та синтез, метод системного аналізу, функціонально-цільовий, абстрактно-логічний.

Результати. Розглянуто гіджиталізацію як складову мережевого суспільства та предмет сучасного наукового дискурсу; вивчено теоретичні засади формування та розвитку гіджиталізації як інструменту сучасного публічного управління; досліджено особливості гіджиталізації публічного управління як складника цифрової трансформації України, що використовується в умовах воєнного стану; висвітлено проблеми цифрової трансформації, які виникли після повномасштабного вторгнення Росії на територію України в системі вітчизняного публічного управління; визначено перспективні напрямки розвитку гіджиталізації для формування ефективного публічного управління в умовах дії правового режиму воєнного стану.

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на законодавче визначення впровадження гіджиталізації, цифровізації у органах публічної влади.

Ключові слова: гіджиталізація, цифровізація, управління, державна установа, публічна влада, публічне управління, воєнний стан.

Summary. Introduction. With the emergence of the first digital devices at the end of the 20th century, an irreversible process of digitalization was launched, and with the advent of the Internet and smartphones, it became widespread. Artificial intelligence, Big Data, the Internet, and cloud services are constantly developing and gaining more and more areas of application, including in the field of modern public administration. The coronavirus pandemic contributed to a new stage in the development of digitalization of modern public administration. The rapid transition to a remote work format allowed public administration bodies to continue to work effectively. And with the beginning of the full-scale Russian invasion, cloud services helped to preserve critically important data for public administration bodies in Ukraine.

In order to maintain balance in the implementation of the state development strategy, the influence of management personnel is required by making balanced, scientifically based management decisions. Such decisions can only be made on the basis of factual, up-to-date information data on the real state of activities of public authorities. It is impossible to build an effective model of modern management processes without the use of digital technologies.

The implementation of the main directions of state development in accordance with the requirements of international agreements and treaties and the intended goals of state development is possible through the active implementation of digitalization in the public administration system. Therefore, the role of digitalization in public administration is undoubtedly significant. The formation of digital infrastructure is the way to fulfill the intended goals of the state and implement effective management processes.

Purpose. The purpose of writing the article is to study the current state of digitalization as an important tool for the formation of modern public administration under martial law.

Materials and methods. The research materials are: regulatory legal acts of Ukraine, monographs and scientific articles devoted to the issues of modern scientific approaches to the modernization of public administration in the conditions of digital transformations of society, the use of world experience in digitalization as a strategic direction for optimizing public administration, as well as directions for the development of digitalization for the formation of effective public administration.

Research methods: descriptive, comparative, analysis and synthesis, system analysis method, functional-target, abstract-logical.

Results. Digitalization is considered as a component of the network society and the subject of modern scientific discourse; the theoretical principles of the formation and development of digitalization as a tool of modern public administration are studied; the features of the digitalization of public administration as a component of the digital transformation of Ukraine, used in martial law, are investigated; the problems of digital transformation that arose after the full-scale invasion of Russia into the territory of Ukraine in the system of domestic public administration are highlighted; promising directions of digitalization development for the formation of effective public administration under the legal regime of martial law are identified.

Prospects. In further scientific research, it is proposed to focus attention on the legislative definition of the implementation of digitalization, digitalization in public authorities.

Key words: digitalization, digitalization, administration, state institution, public authority, public administration, martial law.

Постановка проблеми. Науково-технічний прогрес та стрімкий розвиток інформаційних технологій нещадно впливають на сучасне суспільство. Діджиталізація, як явище, що відображає інтеграцію інформаційних технологій в усі сфери життя, стає фундаментальним аспектом сучасної епохи.

Новітні інформаційно-комунікаційні технології (ІКТ) докорінно змінюють усі соціальні відносини — формується нове, інформаційне, а тепер уже цифро-

ве суспільство. Це зменшує відстані та створює безпрецедентні можливості для регіонального розвитку.

Однією з найважливіших передумов ефективного реформування державних установ та органів влади в контексті цифрової трансформації є електронне урядування, яке трансформується в цифрову форму та метою якого є підвищення ефективності роботи уряду з громадянами та бізнесом і зменшення загальних витрат часу та коштів.

Використання діджиталізації, зокрема, в державному управлінні, може надати значний поштовх для цифрової трансформації та розвитку конкурентоспроможної економіки в Україні. Отже, існує потреба детально вивчити специфіку діджиталізації державного управління в Україні в ході її цифрової трансформації та розробити пропозиції щодо напрямків її впровадження.

Аналіз останніх досліджень і публікацій.

Упродовж останніх років проблематика діджиталізації публічного управління активно дискутується американськими та європейськими вченими, зокрема, особливості практичного впровадження концепції «Ера цифрового врядування» розкриті в працях А. Вільямса та Х. Хей [1]; П. Данлеві [2], Х. Маргетс, С. Бастоу та Дж. Тінклер [3], Л. Де Нардіс [4]. У науковій літературі проблеми впровадження та розвитку цифрових технологій досліджувались у роботах таких вчених, як: А. Асанова [5], В. Бабаєв [6], М. Демкова [7], Н. Дяченко [8], А. Серенко [9] та інші. Але у вітчизняних наукових працях тема діджиталізації публічного управління й досі залишається не розкритою, на відміну від проблематики вже впровадженої в Україні концепції «електронного урядування» на базі технологій діджиталізації публічного управління.

Метою статті є дослідження сучасного стану діджиталізації як важливого інструменту формування сучасного публічного управління в надскладних умовах функціонування нашого суспільства.

Матеріали і методи. Матеріалами дослідження є: нормативно-правові акти України, монографії та наукові статті, присвячені питанням сучасних наукових підходів щодо модернізації публічного управління в умовах цифрових трансформацій суспільства, використанню світового досвіду діджиталізації як стратегічного напрямку оптимізації публічного управління, а також напрямкам розвитку діджиталізації для формування ефективного публічного управління.

Методи дослідження: описовий, порівняльний, аналіз та синтез, метод системного аналізу, функціонально-цільовий, абстрактно-логічний.

Виклад основного матеріалу. У контексті адаптації до нових реалій господарюючі субєкти в усьому світі усвідомлюють зміни та можливості, які може принести впровадження цифрових технологій. Такими базовими технологіями четвертої промислової революції є Інтернет речей, цифрові екосистеми, аналітика великих даних та цифрові платформи [10], а отже, діджиталізація. Розглянувши різні точки зору на цей процес, можна отримати більш повне розуміння його сутності. Аналіз наукової літератури показує, що деякі автори наголошують на технологічному аспекті діджиталізації та визначають її як процес перетворення аналогової інформації в цифрову форму за допомогою різних цифрових технологій. Інші автори зосереджуються на організаційних

змінах та стратегічному плануванні і розглядають діджиталізацію не лише як технологічний аспект, а й як складний процес, що впливає на організаційну культуру, бізнес-моделі та взаємодію з клієнтами.

Новітні ІКТ докорінно змінюють усі соціальні відносини — формується нове, інформаційне, а тепер уже цифрове суспільство. Це зменшує відстані та створює безпрецедентні можливості для регіонального розвитку. Однією з найважливіших передумов ефективного реформування державних установ та органів влади в контексті цифрової трансформації є електронне урядування, яке трансформується в цифрову форму, метою якого є підвищення ефективності роботи уряду з громадянами та бізнесом і зменшення загальних витрат часу та коштів [11].

Слово «діджиталізація» міцно увійшло до нашого словника у 2019 році та навіть було обрано словом року [12]. Однак точне визначення цього терміну досі є предметом дискусій не лише у вітчизняній науковій сфері, а й за кордоном. Це слово походить від англійського «digital», що означає «цифровий», «пальцевий». У різних джерелах використовується кілька визначень терміну: «цифровізація», «діджиталізація» та «цифрова трансформація», а також є прикметники — «цифровий» та «діджитальний».

У контексті національних підходів термін «діджиталізація» зазвичай стосується процесів цифровізації, тобто зазвичай оцифрування даних.

Розвиток цифрових технологій у сучасному суспільстві стає об'єктивно неминучим процесом, що впливає на всі сфери життя держави. Це стосується, зокрема, надання державних послуг населенню шляхом використання інформаційно-комунікаційних технологій та Інтернету. Використання цифрових інструментів у наданні державних послуг сприяє всебічному розширенню можливостей громадян брати участь у процесі державотворення та державного управління. Основою для впровадження процесів діджиталізації є нормативно-правове забезпечення надання цифрових послуг органами державної влади та муніципалітетами. Адекватність та всеохоплюючий характер правової бази, а також її відповідність нормам і стандартам міжнародного права характеризують здатність національної державної служби ефективно здійснювати державну владу, функції регулювання, координації та контролю над своїм населенням.

Діджиталізація державних послуг тісно пов'язана з цифровими трансформаціями, спрямованими на розширення елементів електронної демократії, зокрема впровадження електронного голосування, автоматизацію надання адміністративних послуг, використання систем електронних судів та впровадження елементів електронного урядування загалом [13].

В умовах стрімкого розвитку цифрового суспільства ІКТ стали основою реформування діяльності державних установ, а їх активне використання є запорукою ефективного та повноцінного державного управління.

В Україні підготовлено десятки законопроектів та прийнято низку законів, що стосуються впровадження ІКТ та цифровізації державного управління. Це підкреслює нагальну потребу впровадження реформ та трансформацій на основі «цифрового» підходу. Наразі в Україні створені умови для формування та розвитку цифрового суспільства, що є головним пріоритетом для перспектив розвитку країни. Впровадження технологічних інновацій у діяльність державних органів спрямоване на виконання завдань та цілей державних інституцій, сприяння ефективності їх застосування, вирішення викликів часу та побудову сучасної системи у сфері державного управління.

Ефективність державних структур у сучасних умовах розвитку інформаційного суспільства неможлива без впровадження цифрових технологій. Заслужують на увагу незаперечні переваги електронного урядування як форми державного управління, що базується на використанні ІКТ та Інтернету.

Впровадження елементів електронного адміністрування через інформаційну систему «Електронний уряд» у 2003 році та низка нормативно-правових актів досі не реалізовані повністю. Після прийняття Концепції розвитку електронного адміністрування в Україні (2010, 2017) суттєвих змін не відбулося. Також не відчутні були і зміни після розробки проекту «Цифрова адженда України — 2020» [14] та попри існування спеціалізованих органів — Державного агентства з питань електронного урядування України та Національного центру підтримки електронного адміністрування. Слід зазначити, що вищезазначені документи мали загалом декларативний характер.

Обравши європейський шлях розвитку, Україна поставила собі за мету покращити бізнес-клімат, створити публічно доступні адміністративні процедури для бізнесу з використанням електронних інструментів та застосувати принципи належного управління, що неможливо без використання ІКТ. Не випадково, що для побудови ефективної, прозорої, відкритої та гнучкої структури державної служби Державна стратегія сталого розвитку «Україна-2020» (2015) та Державна стратегія регіонального розвитку на період до 2020 року (2014) передбачали завдання, пов'язані із застосуванням новітніх ІКТ у своїй діяльності.

Наявність нових викликів, що виникли для України останніми роками, відсутність реалізації нових можливостей для розвитку територіальних громад та регіонів у напрямку кращої якості життя людей, відсутність змін у зміцненні партнерських відносин між регіонами, зменшенні міжрегіональних та внутрішньо-регіональних диспропорцій у показниках економічного розвитку та якості життя людей сприяли прийняттю Кабінетом Міністрів України Державної стратегії регіонального розвитку на 2021–2027 роки [15].

Перелік викликів доповнюється складною епідеміологічною ситуацією, пов'язаною з поширенням гострого респіраторного захворювання COVID-19, що також призвело до недостатньої підготовки установ до кризових ситуацій на державному рівні.

До проблемних питань, які потребують вирішення в рамках цієї стратегії, належать:

- слабка інтеграція регіональних просторів у загальноукраїнський простір;
- низька конкурентоспроможність регіонів, одним із факторів впливу на яку є низький рівень цифровізації регіонів та низька цифрова обізнаність;
- недостатній потенціал центральних та місцевих органів виконавчої влади, органів місцевого самоврядування та інститутів регіонального розвитку для ефективного впровадження реформ, надання якісних послуг населенню та вирішення проблем соціально-економічного розвитку територій.

Наразі Україні потрібно розробити та впровадити нову стратегію розвитку країни, оскільки проект стратегії сталого розвитку України до 2030 року не реалізовано. Вартими уваги є матеріали Кабінету Міністрів України «Вектори економічного розвитку 2030», які виносяться на обговорення та в яких думка щодо розвитку цифрової економіки викладена в окремому розділі (Таблиця 1) [16].

Отже, інформаційно-комунікаційні процеси цифрової оптимізації сучасного державного управління систематизовані за такими напрямками: цифрова інфраструктура, цифрові навички та цифрові компетенції, цифровізація державного управління та послуг, цифрова трансформація економіки, інтеграція в цифровий простір Європейського Союзу.

Одним із найважливіших напрямків розвитку цифрової економіки є цифровізація державного сектору. Модернізація державного управління досягається і буде досягатися шляхом цифровізації державного сектору, а ефективність таких цифрових трансформацій залежить, перш за все, від кваліфікації персоналу та, в даному випадку, від цифрових знань та навичок.

Для пришвидшення процесів діджиталізації у громадських просторах на місцевому, регіональному та державному рівнях необхідно активізувати процеси впровадження ІКТ у їхню діяльність, використовуючи різні моделі державно-приватного партнерства. Залучення приватного капіталу до процесів модернізації державного управління, як це практикується за кордоном, безумовно, принесло позитивні результати, але в Україні розвиток таких партнерств все ще перебуває на початковій стадії [17].

Цифрова трансформація є основою сталого розвитку України як провідної європейської країни. Цифровізація відкриває новий світ з новими можливостями та сферами, що мають значний вплив на зміни в країні з метою покращення всіх життєво важливих сфер для громадян країни. Однак,

Таблиця 1

Розвиток цифрової економіки

Бачення розвитку	Відповіді на поточні виклики	Кардинальна зміна функціонування
Створення якісної, доступної та захищеної цифрової інфраструктури	– покриття мобільним інтернетом; – візуалізація та хмарні послуги; – оцифровані дані та реєстри; – кібербезпека.	– покриття мобільним інтернетом; – хмарні обчислення; – реєстри та інтеперабельність; – кібербезпека
Підвищення якості цифрових навичок громадян та розвиток цифрових компетенцій в окремих секторах	– цифрові навички громадян; – цифрові компетенції фахівців освіти і науки; – цифрові компетенції чиновників; – Цифрові компетенції фахівців охорони здоров'я.	– цифрові навички громадян; – цифрові компетенції фахівців освіти і науки; – цифрові компетенції чиновників; – Цифрові компетенції фахівців охорони здоров'я.
Цифрова трансформація державного сектору	– синхронізація даних державних органів; – прозорість бюджетів; – статистика; – державні електронні сервіси; – електронна демократія.	– статистика; – державні електронні сервіси; – електронна демократія.
Цифрова трансформація соціального сектору	– освітня цифрова платформа; – цифровізація освіти; – E-Health; – електронна система невідкладної допомоги; – електронні соціальні послуги.	– цифровізація освіти; – E-Health; – електронна система невідкладної допомоги; – електронні соціальні послуги.

Джерело: узагальнено авторами на основі [16]

започаткування процесів адаптації до нових реалій, окрім значних переваг, несе з собою низку проблем, ризиків та викликів, які також потребують подальшого дослідження.

Необхідно розглянути ключові виклики у сфері цифрової трансформації в системі вітчизняного публічного управління, які виникли з початком повномасштабного вторгнення Росії на територію України:

1) державні послуги (електронні та ті, що надаються ЦНАПами та/або безпосередньо органами, що їх надають) — значна кількість громадян знаходиться далеко від місця проживання, а це означає, що вони не можуть отримати всі необхідні послуги (принцип екстериторіальності ще не поширюється на всі послуги, і не всі послуги доступні в електронному вигляді);

2) тривале призупинення надання певних послуг підприємствами, що надають ці послуги;

3) неорганізованість у визначенні документів, необхідних для замовлення послуг;

4) недостатній системний розвиток державних послуг (відсутність життєвого циклу послуг, необхідність подальшого інституційного розвитку, впорядкування адміністративних зборів за надання послуг, децентралізація окремих груп послуг на місцевий рівень, розвиток методичного забезпечення тощо), труднощі у наданні послуг українцям, які тимчасово перебувають за кордоном для захисту від військових дій;

5) підвищений попит на державні послуги через переміщення, втрату документів, необхідність отримання державних соціальних виплат, пенсій тощо;

6) публічні реєстри та електронна взаємодія — у зв'язку з війною постало питання фізичного захисту державних інформаційних систем, їхньої відмовостійкості, можливості зберігання даних та переміщення державних інформаційних систем за кордон, що призвело до блокування доступу до цих реєстрів на певний період; недостовірність даних у реєстрах, відсутність єдиного наскрізного ідентифікатора, низька якість центральних довідників та стандартів, недостатня готовність державних інформаційних систем до електронної взаємодії;

7) центри надання адміністративних послуг — знищення ЦНАПів у районах, які були або тимчасово окуповані; відсутність доступу до реєстрів та інформаційних систем або тривале відновлення доступу до цих систем для забезпечення надання послуг громадянам; не всі громади створили ЦНАПи, відсутність можливості надавати електронні послуги в населених пунктах без доступу до Інтернету (цифровий розрив); складність надання послуг через відсутність уніфікованого програмного забезпечення, що забезпечує можливість роботи з різними державними інформаційними системами; відсутність можливості для громадян отримувати послуги там, де їм зручно; відсутність електронної взаємодії між учасниками процесу обслуговування (Трембіта, СЕВ ОБВ);

8) цифрові документи — через війну виникла потреба використовувати, на додаток до або замість фізичних документів, які були втрачені або до яких громадяни тимчасово не мають доступу, цифрові зображення документів, які може пред'явити (надати) людина на смартфоні через мобільний додаток Дія;

9) необхідність впровадження цифрових та антикорупційних інструментів в адміністративні процедури відшкодування шкоди, завданої внаслідок збройної агресії Російської Федерації;

10) брак фінансування для всіх напрямків цифровізації;

11) щонайменше 726 операторів фіксованого електронного зв'язку зазнали втрат у результаті військових дій. Після деокупації населених пунктів руйнування мереж становить до 100%. Якість передачі даних через фіксований доступ до Інтернету знизилася в середньому на 23% по всій країні (станом на 1 січня 2024 року) [18].

12) 12,2% населених пунктів не мають доступу до мобільного зв'язку, а 3,1% мають частковий доступ. 3534 базові станції мобільних операторів не працюють, що становить майже 11% від загальної кількості. Якість передачі даних через мережі мобільного доступу до Інтернету знизилася в середньому на 26% по всій країні (оцінка станом на 1 січня 2024 року) [9].

13) створення можливостей для іноземців вести бізнес в Україні без необхідності фізичної присутності на території України;

14) низький рівень захисту інформаційних ресурсів органів державної влади, місцевого самоврядування та ОКР.

Варто розглянути ключові обмеження / рамки у сфері цифрової трансформації в системі вітчизняного публічного управління, які виникли з початком

повномасштабного вторгнення Росії на територію України (Рис. 1).

В Україні вже існують численні обмеження на використання цифрових технологій, наприклад, у сферах державних закупівель, систем електронного документообігу та надання адміністративних послуг. Без певних передумов держава стане жертвою старих, застарілих моделей управління. Діджиталізація в публічному управлінні відкриває нові можливості для ефективного управління кризами. Це сприяє більшій прозорості, доступності послуг та оновленню даних. Діджиталізація дозволяє державним установам набагато краще реагувати на виклики сучасного світу.

Наразі існує значна кількість перспективних напрямків розвитку діджиталізації для формування ефективного публічного управління в Україні (Рис. 2).

Діджиталізація робить процеси ефективнішими та результативнішими, дозволяючи швидко та гнучко реагувати на кризові ситуації. Це дозволяє владі швидше реагувати на зміну ситуації, адаптувати свою політику та приймати важливі рішення, що особливо важливо під час війни. З іншого боку, діджиталізація допомагає підвищити прозорість діяльності уряду та зробити їхні послуги доступнішими для громадян. Це може зменшити соціальну напруженість та недовіру до влади в часи кризи та дати змогу громадянам активніше брати участь у процесі вирішення проблем.

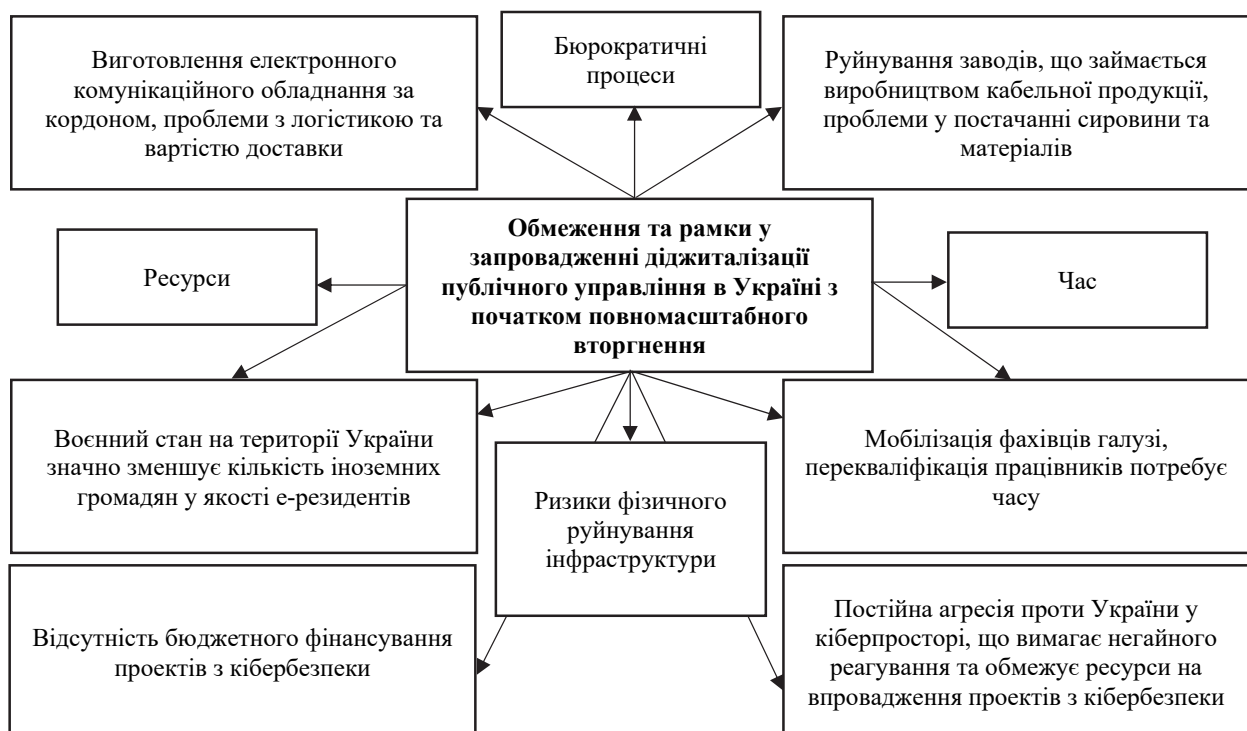


Рис. 1. Основні обмеження та рамки у сфері діджиталізації в системі вітчизняного публічного управління, які виникли з початком повномасштабного вторгнення Росії на територію України

Джерело: розроблено авторами

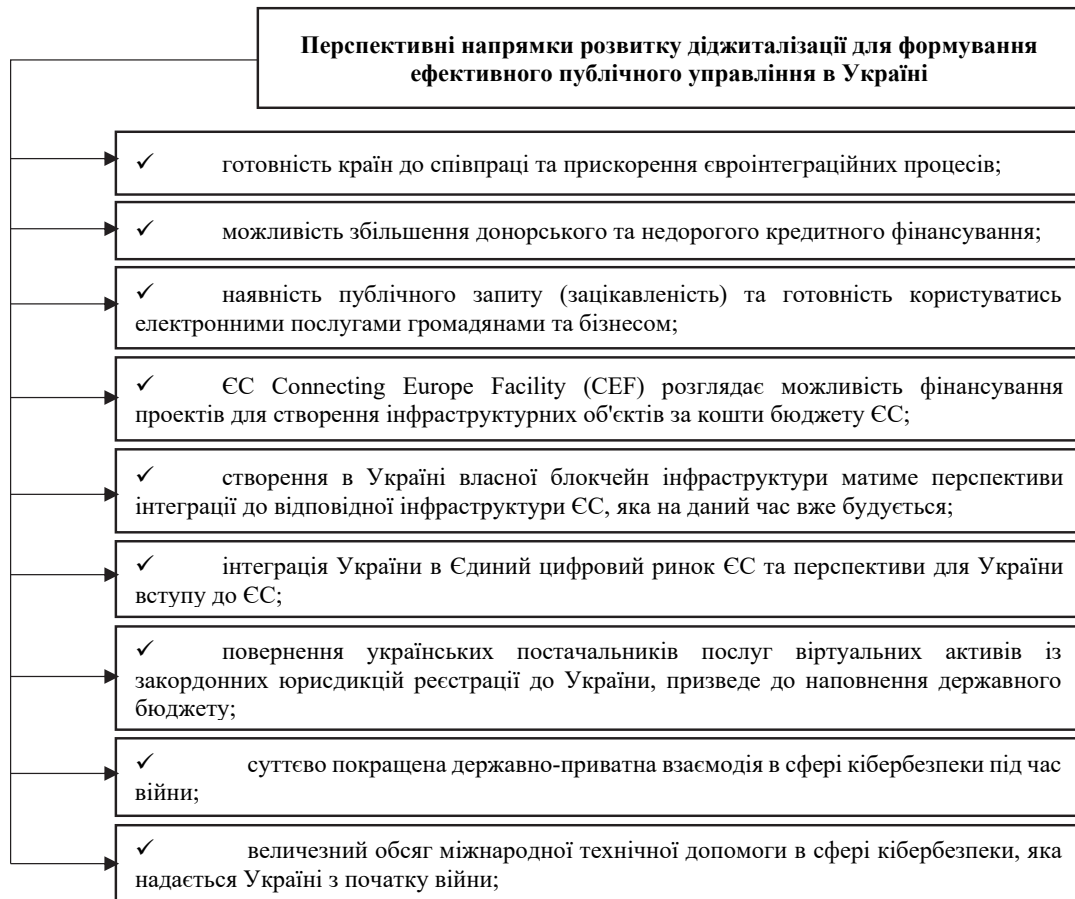


Рис. 2. Перспективні напрямки розвитку діджиталізації для формування ефективного публічного управління в Україні

Джерело: розроблено авторами

Висновки і перспективи подальших досліджень. Отже, можна зробити висновок, що діджиталізація української влади значно підвищує її стійкість до криз. Це дозволяє швидше та ефективніше реагувати на кризи, забезпечує більшу прозорість та доступність, а також дає громадянам можливість відігравати активнішу роль у вирішенні проблем. Тим не менш, важливо стежити за потенційними ризиками кібербезпеки, пов'язаними з діджиталізацією, та вживати необхідних заходів для їх усунення. Діджиталізацію в органах державної влади слід розвивати далі для покращення процесів прийняття рішень, розширення взаємодії з громадами та забезпечення кібербезпеки.

Тому органам влади слід активно співпрацювати з експертами з кібербезпеки для розробки та впровадження надійних стратегій і технологій захисту.

Важливо розробити комплексні навчальні програми для державних установ з питань використання цифрових технологій та кібербезпеки.

Також за підсумками дослідження пропонується зосередити увагу на процесах співпраці органів влади з фахівцями та експертами з цифровізації і кібербезпеки. Активно переймати досвід країн ЄС у запровадженні діджиталізації у публічному управлінні та займатися пошуком фінансових ресурсів, донорів для розвитку діджиталізації у органах публічної влади.

Це дасть змогу пришвидшити запровадження діджиталізації у публічному управлінні та ефективніше реагувати на виклики сучасності у сфері цифровізації, особливо в умовах воєнного стану, коли діджиталізація стає важливим фактором у стабільному функціонуванні та взаємодії органів влади з громадянами.

Література

1. Williams A., Hay H. Digital-era policy making. *Governance in the Digital Economy*. 2000.
2. Dunleavy P. New Public Management is Dead — Long Live Digital-Era Governance. *Journal of Public Administration Research and Theory*. 2005. September.
3. Dunleavy P., Margetts H., Bastow S., Tinkler J. Digital Era Governance: IT Corporations, The State and E-Government. Oxford: Oxford University Press, 2006. 302 p.
4. DeNardis L. The global war for Internet governance. Yale University Press, 2014.
5. Асанова А. Електронний уряд як дійовий механізм взаємодії і форма співпраці держави та громадян в інформаційному суспільстві. URL: http://www.nbu.gov.ua/e-journals/dutp/20061/txts/TEKNOLOGIYA/06aa_avis.pdf (дата звернення: 10.05.2025).
6. Бабаєв В.М. Текст лекцій з дисципліни «Електронне урядування» (для студентів 5 курсу спеціальності 8.03060101 «Менеджмент організацій і адміністрування» денної форми навчання) / В.М. Бабаєв, М.М. Новікова, С.О. Гайдученко; Харк. нац. ун-т міськ. госп-ва ім. О.М. Бекетова. Х. : ХНУМГ, 2014. 127 с.
7. Баранов О.В. Електронне урядування в Україні: аналіз та рекомендації: [результати дослідження] / [О.А. Баранов, І.Б. Жилияєв, М.С. Демкова та ін.]; за ред. І.Г. Малиукової. К. : ООО «Поліграф-Плюс», 2007. 254 с.
8. Дяченко Н. Прогнозні оцінки динаміки впровадження електронного урядування в Україні. *Державне управління та місцеве самоврядування*. 2013. С. 31–36.
9. Серенюк А. Надання адміністративних послуг а електронній формі в органах місцевого самоврядування: результати дослідження 2016 року. URL: www.kbuapa.kharkov.ua/ebook/apdu/2017-1/.../01.pdf (дата звернення: 10.05.2025).
10. Bolgarova N., Bolhov V., Akhnovska I., Kozlovskiy S., Lavrov R., Petrunenko I. Civilizational Cycles and Economic Development in the Context of Technological Transitions and Global Pandemics. *Montenegrin Journal of Economics*. 2022. Vol. 18, № 4. P. 191–202. <http://dx.doi.org/10.14254/1800-5845/2022.18-4.16>.
11. Сурай А.В. Деякі питання цифровізації публічного управління. *Публічне управління в умовах воєнного часу та надзвичайних ситуаціях: сучасний стан, проблеми, перспективи розвитку. матеріали V міжнар. наук.-практ. конф.*, м. Переяслав, 30 листопада 2022 р. Переяслав : Університет Григорія Сковороди в Переяславі. 2023. С. 319–322.
12. Слово року-2019. Словник сучасної української мови та сленгу «Мислово». URL: <http://myslovo.com/> (дата звернення: 10.05.2025).
13. Е-урядування — ключ до реформ в Україні. 2019. URL: <https://www.kmu.gov.ua/ua/news/e-uryaduvannyaklyuch-do-reform-v-ukrayini> (дата звернення: 10.05.2025).
14. Цифрова адженда України — 2020 («Цифровий порядок денний» — 2020): Концептуальні засади (версія 1.0). URL: <https://uccr.org.ua/uploads/files/58e78ee3c3922.pdf> (дата звернення: 10.05.2025).
15. Державна Стратегія регіонального розвитку на 2021–2027 роки : Постанова КМУ від 05 серпня 2020 р. № 695. URL: <https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text> (дата звернення: 10.05.2025).
16. Вектори економічного розвитку 2030: матеріали для обговорення. *Кабінет Міністрів України*. URL: <https://nes2030.org.ua/docs/doc-vector.pdf> (дата звернення: 10.05.2025).
17. Савченко О.С. Систематизація наукових підходів до поняття «цифровізація у публічному управлінні». *Держава та регіони. Серія «Публічне управління та адміністрування»*. 2022. № 2(76). С. 72–76.
18. Офіційний вебсайт Міністерства цифрової трансформації України. URL: <https://thedigital.gov.ua/> (дата звернення: 10.05.2025).

References

1. Williams, A., & Hay, H. (2000). *Digital-era policy making*. Governance in the Digital Economy.
2. Dunleavy, P. (2005, September). New public management is dead — Long live digital-era governance. *Journal of Public Administration Research and Theory*.
3. Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). *Digital Era Governance: IT Corporations, The State and E-Government*. Oxford: Oxford University Press.
4. DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.
5. Asanova, A. (2006). Elektronnyi uriad yak diievyi mekhanizm vzaemodii i forma spivpratsi derzhavy ta hromadian v informatsiinomu suspilstvi [E-Government as an effective mechanism of interaction and cooperation between the state and citizens in the information society]. Retrieved from <http://www.nbu.gov.ua/e-journals/dutp/20061/txts/TEKNOLOGIYA/06aa%20avis.pdf>
6. Babaiev, V.M., Novikova, M.M., & Haiduchenko, S. O. (2014). *Lecture text on the discipline "E-Government"* (for 5th-year students majoring in 8.03060101 "Management of Organizations and Administration", full-time study). Kharkiv: O.M. Beketov National University of Urban Economy.
7. Baranov, O.V., Zhyliaiev, I.B., Demkova, M.S., et al. (2007). *E-Government in Ukraine: Analysis and Recommendations* (I.H. Maliukova, Ed.). Kyiv: Polihraf-Plius.
8. Diachenko, N. (2013). Forecast evaluation of e-government implementation dynamics in Ukraine. *Public Administration and Local Self-Government*, 31–36.

9. Serenok, A. (2017). Nadannia administratyvnykh posluh u elektronni formi v orhanakh mistsevoho samovriaduvannia: rezultaty doslidzhennia 2016 roku [Provision of administrative services in electronic form in local self-government bodies: Results of the 2016 research]. Retrieved from www.kbuapa.kharkov.ua/ebook/apdu/2017-1/.../01.pdf
10. Bolgarova, N., Bolhov, V., Akhnovska, I., Kozlovskiy, S., Lavrov, R., & Petrunenko, I. (2022). Civilizational cycles and economic development in the context of technological transitions and global pandemics. *Montenegrin Journal of Economics*, 18(4), 191–202. <https://doi.org/10.14254/1800-5845/2022.18-4.16>
11. Surai, A. V. (2023). Some issues of digitalization of public administration. In *Public Administration in Wartime and Emergencies: Current State, Challenges, Development Prospects* (pp. 319–322). Proceedings of the 5th International Scientific-Practical Conference, Pereiaslav, November 30, 2022. Pereiaslav: Hryhorii Skovoroda University.
12. Myslovo. (2019). Slovo roku-2019 [Word of the year — 2019]. *Dictionary of Contemporary Ukrainian Language and Slang*. Retrieved from <http://myslovo.com/>
13. Cabinet of Ministers of Ukraine. (2019). *E-Governance as the key to reforms in Ukraine*. Retrieved from <https://www.kmu.gov.ua/ua/news/e-uryaduvannyaklyuch-do-reform-v-ukrayini>
14. Digital Agenda of Ukraine — 2020 (Version 1.0). (n.d.). *Conceptual Principles*. Retrieved from <https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf>
15. Cabinet of Ministers of Ukraine. (2020). *State Regional Development Strategy for 2021–2027* (Resolution No. 695, August 5, 2020). Retrieved from <https://zakon.rada.gov.ua/laws/show/695-2020-п#Text>
16. Cabinet of Ministers of Ukraine. (n.d.). *Vectors of Economic Development 2030: Discussion Materials*. Retrieved from <https://nes2030.org.ua/docs/doc-vector.pdf>
17. Savchenko, O. S. (2022). Systematization of scientific approaches to the concept of “digitalization in public administration”. *State and Regions. Series “Public Administration and Administration”*, (2)76, 72–76.
18. Ministry of Digital Transformation of Ukraine. (n.d.). *Official Website*. Retrieved from <https://thedigital.gov.ua/>

Стаття надійшла до редакції 26.05.2025

Стеців Ірина Семенівна

*доктор наук з державного управління, доцент,
доцент кафедри адміністративного та фінансового менеджменту
Національний університет «Львівська політехніка»*

Stetsiv Iryna

*Doctor of Science in Public Administration, Associate Professor,
Associate Professor at the Department of Administrative and Financial Management
Lviv Polytechnic National University
ORCID: 0000-0003-4982-1355*

Козопас Андрій Володимирович

*аспірант кафедри адміністративного та фінансового менеджменту
Національного університету «Львівська політехніка»*

Kozopas Andrii

*PhD student at the Department of Administrative and Financial Management
Lviv Polytechnic National University*

DOI: 10.25313/2617-572X-2025-5-11050

ІНСТИТУЦІЙНІ МЕХАНІЗМИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІННОВАЦІЙНОГО ПІДПРИЄМНИЦТВА В УМОВАХ ТРАНСФОРМАЦІЙНОЇ ЕКОНОМІКИ УКРАЇНИ

INSTITUTIONAL MECHANISMS OF STATE REGULATION OF INNOVATIVE ENTREPRENEURSHIP IN THE CONTEXT OF UKRAINE'S TRANSFORMATIONAL ECONOMY

Анотація. Вступ. У сучасних умовах трансформаційної економіки України, що супроводжується викликами повномасштабної війни, руйнуванням виробничої інфраструктури, дисбалансом у державному управлінні та необхідністю пришвидшеного економічного відновлення, інноваційне підприємництво постає як ключовий чинник національної конкурентоспроможності та технологічної модернізації. Разом із цим посилюється потреба у формуванні ефективних інституційних механізмів державного регулювання, які б забезпечували належні умови для стимулювання та підтримки інноваційної активності бізнесу, зокрема в сегменті малих та середніх підприємств. Наявні дослідження демонструють фрагментарність підходів до регуляторної політики у цій сфері, що зумовлює необхідність поглибленого теоретико-методологічного обґрунтування моделей інституційної модернізації.

Мета. Метою статті є обґрунтування структури та напрямів вдосконалення інституційних механізмів державного регулювання інноваційного підприємництва в Україні в умовах трансформаційної економіки та післявоєнного відновлення.

Матеріали та методи. Матеріалами дослідження є нормативно-правові акти, стратегічні документи України, статистичні матеріали Державної служби статистики, міжнародні рейтинги інноваційного розвитку, а також наукові праці українських дослідників. Методологічний інструментарій включає методи аналізу та синтезу (для виявлення сутності інституційного механізму), елементи SWOT-аналізу (для виявлення сильних і слабких сторін реалізації інституційних механізмів в Україні), систематизації (для класифікації форм та суб'єктів регулювання), логічне узагальнення (для формування авторської моделі), а також структурно-функціональний і індуктивно-дедуктивний підходи (для побудови схеми удосконалення).

Результати. У результаті проведеного аналізу виявлено, що чинна інституційна система державного регулювання інноваційного підприємництва в Україні є недостатньо ефективною через відсутність єдиного стратегічного центру, неузгодженість між центральними та регіональними ініціативами, обмежений доступ до фінансування, а також слабку інтеграцію науки, бізнесу й держави. Запропоновано модель інституційної модернізації, яка охоплює напрями стратегічної координації, цифровізації інфраструктури підтримки, розвитку регіональних центрів інновацій, посилення кадрової спроможності органів влади та створення системи результативного моніторингу. Схематично відображено комплексний, багаторівневий підхід до інституційної трансформації з урахуванням вимог повоєнної відбудови.

Перспективи. Запропонований у статті підхід формує підґрунтя для подальших прикладних досліджень щодо інституціоналізації партнерств держави, бізнесу та науки, розробки цифрових платформ управління інноваціями, а також впровадження регіональних політик підтримки інноваційних кластерів. Перспективним напрямом є апробація розробленої моделі на рівні пілотних проєктів у регіонах, що мають високий інноваційний потенціал або критично постраждали внаслідок воєнних дій.

Ключові слова: інституційний механізм, державне регулювання, інноваційне підприємництво, трансформаційна економіка, інноваційна політика, публічне управління, післявоєнне відновлення, інфраструктура підтримки інновацій, регіональний інноваційний розвиток.

Summary. Introduction. In the current context of Ukraine's transformational economy – marked by the challenges of full-scale war, destruction of production infrastructure, imbalances in public governance, and the urgent need for accelerated economic recovery – innovative entrepreneurship has emerged as a key factor of national competitiveness and technological modernization. This situation strengthens the need for the development of effective institutional mechanisms of state regulation that would ensure appropriate conditions for stimulating and supporting innovation activity in business, particularly within the small and medium-sized enterprise (SME) sector. Existing studies demonstrate the fragmentation of approaches to regulatory policy in this area, which necessitates a deeper theoretical and methodological substantiation of institutional modernization models.

Purpose. The purpose of this article is to justify the structure and directions for improving the institutional mechanisms of state regulation of innovative entrepreneurship in Ukraine under conditions of a transformational economy and post-war recovery.

Materials and Methods. The research materials include legal and regulatory acts, strategic documents of Ukraine, statistical data from the State Statistics Service, international innovation development rankings, and scholarly works by Ukrainian researchers. The methodological framework incorporates methods of analysis and synthesis (to identify the essence of the institutional mechanism), elements of SWOT analysis (to reveal the strengths and weaknesses of implementing institutional mechanisms in Ukraine), systematization (to classify regulatory forms and actors), logical generalization (to develop the author's model), as well as structural-functional and inductive-deductive approaches (to construct a modernization scheme).

Results. The analysis revealed that the current institutional system of state regulation of innovative entrepreneurship in Ukraine is insufficiently effective due to the absence of a unified strategic center, inconsistency between central and regional initiatives, limited access to financing, and weak integration among science, business, and the state. A model of institutional modernization is proposed, covering directions for strategic coordination, digitalization of support infrastructure, development of regional innovation centers, strengthening the institutional capacity of government bodies, and the establishment of a results-based monitoring system. A schematic representation demonstrates a comprehensive, multi-level approach to institutional transformation, considering the imperatives of post-crisis reconstruction.

Discussion. The approach proposed in the article lays the foundation for further applied research on institutionalizing state-business-science partnerships, developing digital platforms for innovation governance, and implementing regional policies to support innovation clusters. A promising direction involves pilot testing the proposed model in regions with high innovation potential or those critically affected by the war.

Key words: institutional mechanism, state regulation, innovative entrepreneurship, transformational economy, innovation policy, public governance, post-war recovery, innovation support infrastructure, regional innovation development.

Постановка проблеми. У сучасних умовах трансформаційної економіки України, яка перебуває під впливом глобальних технологічних змін, війни, процесів євроінтеграції та структурної перебудови внутрішнього ринку, інноваційне підприємництво набуває ключового значення як драйвер економічного зростання, підвищення конкурентоспроможності та зміцнення національної безпеки.

Ефективне державне регулювання розвитку інноваційного підприємництва стає необхідною умовою для створення сприятливого інституційного середовища, в якому наука, бізнес і влада функціонують у синергії. Попри наявність програмних документів, стратегій інноваційного розвитку, запровадження інструментів державної підтримки (стартап-фондів, податкових стимулів, інноваційних хабів), в Україні досі не сформовано цілісної системи інституційних механізмів, здатної ефективно регулювати процеси інноваційної підприємницької активності на різних рівнях державного управління. Спостерігається

низький рівень координації між органами виконавчої влади, відсутність системної політики залучення приватного капіталу до інновацій, слабка інтеграція регіональних ініціатив у національні стратегії. Бракує прозорої моделі взаємодії держави з ключовими учасниками інноваційної екосистеми.

Проблема полягає в недостатній результативності чинних інституційних механізмів, що регламентують підтримку інноваційного підприємництва, а також у відсутності адаптивного інституційного середовища, яке відповідало б викликам воєнного і післявоєнного періоду. Невирішеними залишаються питання формування ефективної мережі державних і недержавних інституцій розвитку, забезпечення стійких каналів комунікації між ними, запровадження механізмів результативного моніторингу та оцінювання політик у сфері інновацій. Вимагають дослідження сучасні моделі інституційного регулювання, що дозволяють поєднати стратегічне планування держави з гнучкістю інноваційного середовища. Вищенаведене свід-

чить про необхідність комплексного переосмислення ролі держави в інноваційному розвитку, впровадження дієвих механізмів інституційного супроводу підприємництва з високою часткою нововведень, а також потребою у науково обґрунтованих підходах до трансформації регуляторної політики в умовах кризової економіки воєнного та повоєнного часу.

Аналіз останніх досліджень і публікацій. Питанням державного регулювання інноваційного підприємництва приділяється значна увага у працях українських дослідників. Зокрема, у статті Н. В. Філіпової розкрито підходи до формування механізму державного управління інноваційною діяльністю, наголошено на проблемах фрагментарності інституційного середовища та запропоновано напрями удосконалення нормативного регулювання у сфері інноваційної політики [1]. Дослідження І. М. Москалець акцентує увагу на складових механізму реалізації державної політики інноваційного розвитку економіки України, обґрунтовує концепцію комплексного регуляторного впливу з урахуванням міжрівневої взаємодії [2]. Є. Ю. Забашта проаналізувала інституційні чинники, що впливають на ефективність розвитку інноваційного підприємництва, та запропонувала структурну модель механізму його підтримки [3]. К. В. Безверхий розглянув роль недержавних суб'єктів у системі інституційного регулювання інновацій, наголосивши на важливості розширення повноважень ІТ-бізнесу та малого підприємництва [4]. Низка науковців зосередили увагу на трансформації підходів до державного регулювання інноваційної діяльності, враховуючи міжнародний досвід і європейські та підходи проблемах нормативно-правового забезпечення інноваційної діяльності промислових підприємств, а також на слабких сторонах інституційної моделі, що існує на сьогодні [5, 6].

Водночас, наявні дослідження здебільшого зосереджуються на окремих аспектах проблеми — інституційно-правовому забезпеченні, організаційних підходах чи регіональній політиці. Відсутній системний аналіз інституційної моделі як цілісного механізму державного регулювання інноваційного підприємництва в умовах воєнної економіки та посткризової трансформації. Вищенаведене зумовлює необхідність подальших досліджень, спрямованих на інтеграцію елементів публічної політики, цифрової трансформації, регіонального розвитку та державної підтримки з урахуванням сучасних викликів і стратегічних цілей України.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування структури та напрямів вдосконалення інституційних механізмів державного регулювання інноваційного підприємництва в Україні в умовах трансформаційної економіки та післявоєнного відновлення.

Матеріали та методи дослідження. Матеріалами для проведення дослідження стали нормативно-правові акти України, що регламенту-

ють державну політику у сфері інноваційної діяльності, підприємництва та публічного управління, а також стратегічні документи, зокрема Національна економічна стратегія-2030, Державна стратегія регіонального розвитку, Закон України «Про інноваційну діяльність», законопроекти щодо інноваційних парків і кластерів. До аналітичної бази дослідження увійшли статистичні дані Державної служби статистики України, щорічні звіти Global Innovation Index, аналітичні огляди міжнародних організацій (OECD, World Bank, WIPO), звіти Українського інституту інтелектуальної власності та інші джерела, що дозволили оцінити динаміку інституційного забезпечення інноваційного підприємництва.

У дослідженні використано сукупність загальнонаукових і спеціальних методів, зокрема методи аналізу і синтезу (для визначення змісту інституційних механізмів та їх структурної побудови), метод систематизації (для класифікації суб'єктів і форм державного регулювання), логічне узагальнення (для формування авторського бачення вдосконалення регуляторної моделі), елементи SWOT-аналізу (для виявлення сильних і слабких сторін реалізації інституційних механізмів в Україні), структурно-функціональний підхід (для виявлення взаємозв'язків між органами влади різного рівня), а також індуктивно-дедуктивний підхід (для переходу від емпіричних фактів до узагальнень і рекомендацій).

Обґрунтування теоретичних висновків і прикладних пропозицій здійснювалося з урахуванням сучасних трансформаційних процесів в українській економіці, зокрема необхідності відновлення інституційної спроможності держави в умовах війни, актуалізації потреби у технологічному розвитку підприємницького сектору та посилення координаційної ролі держави в побудові національної інноваційної екосистеми. Отримані результати стали основою для формування узагальненої моделі інституційного оновлення державної політики підтримки інноваційного підприємництва в Україні.

Виклад основного матеріалу. У сучасних умовах економічної нестабільності, спричиненої широкомасштабними збройними конфліктами, порушенням ланцюгів постачання, деструкцією інфраструктури та суттєвим переформатуванням соціально-економічних пріоритетів, інноваційне підприємство набуває особливої ваги як джерело адаптивного розвитку, технологічного оновлення та відновлення національного економічного потенціалу. У Глобальному індексі інновацій 2024 року Україна посідає 60-те місце серед 133 економік, представлених у рейтингу GII, 4-те місце серед 38 країн групи з рівнем доходу нижче середнього, 34-те місце серед 39 економік Європи [7].

Наведена нижче діаграма показує зв'язок між рівнем доходу (ВВП на душу населення) та інноваційною ефективністю (оцінка GII). Лінія тренду дає уявлення про очікувану інноваційну ефективність

відповідно до рівня доходу. Економіки, що знаходяться вище лінії тренду, показують кращі результати, ніж очікувалося, а ті, що знаходяться нижче, показують результати нижче очікуваних. Відносно ВВП Україна показує результати, що перевищують очікування для її рівня розвитку.

Поряд із цим слід відмітити, що показники інноваційної результативності в Україні зокрема у частині патентів за походженням, обсягів високотехнологічного виробництва та його експорту протягом останніх років значно знизилась. Зокрема кількість патентів за походженням дорівнювала 794 патентам у 2022 році, що на 39,02% менше, ніж у попередньому році — та еквівалентно рангу індикатора 34. Також показник експорту високотехнологічних товарів дорівнював 1,06 млрд. доларів США у 2022 році, що на 27,4% менше, ніж у попередньому році — та еквівалентно рангу індикатора 68 (рис. 2).

Основними інноваційними сильними сторонами України є корисні моделі за походженням/млрд. доларів США за паритетом покупної сили (ПКС)

ВВП (1 місце), частка жінок, які працюють з вищою освітою, % (2 місце) та витрати на програмне забезпечення, % ВВП (4 місце) (табл. 1).

Результати проведеного дослідження сильних та слабких сторін свідчать, що ефективне державне регулювання стає не просто інструментом підтримки інноваційної активності, а критично важливою умовою мобілізації ресурсів, інтеграції зусиль суб'єктів розвитку та забезпечення стійкості підприємницького середовища.

Інституційні механізми державного регулювання інноваційного підприємництва — це комплекс формалізованих норм, організаційно-функціональних структур, процедур та управлінських інструментів, спрямованих на формування, реалізацію та оцінювання державної політики щодо розвитку підприємств з високою інноваційною активністю. Їхня сутність полягає у забезпеченні координованої взаємодії держави, бізнесу, науково-освітнього середовища та громадянського суспільства з метою створення сприятливого інституційного простору для генерування

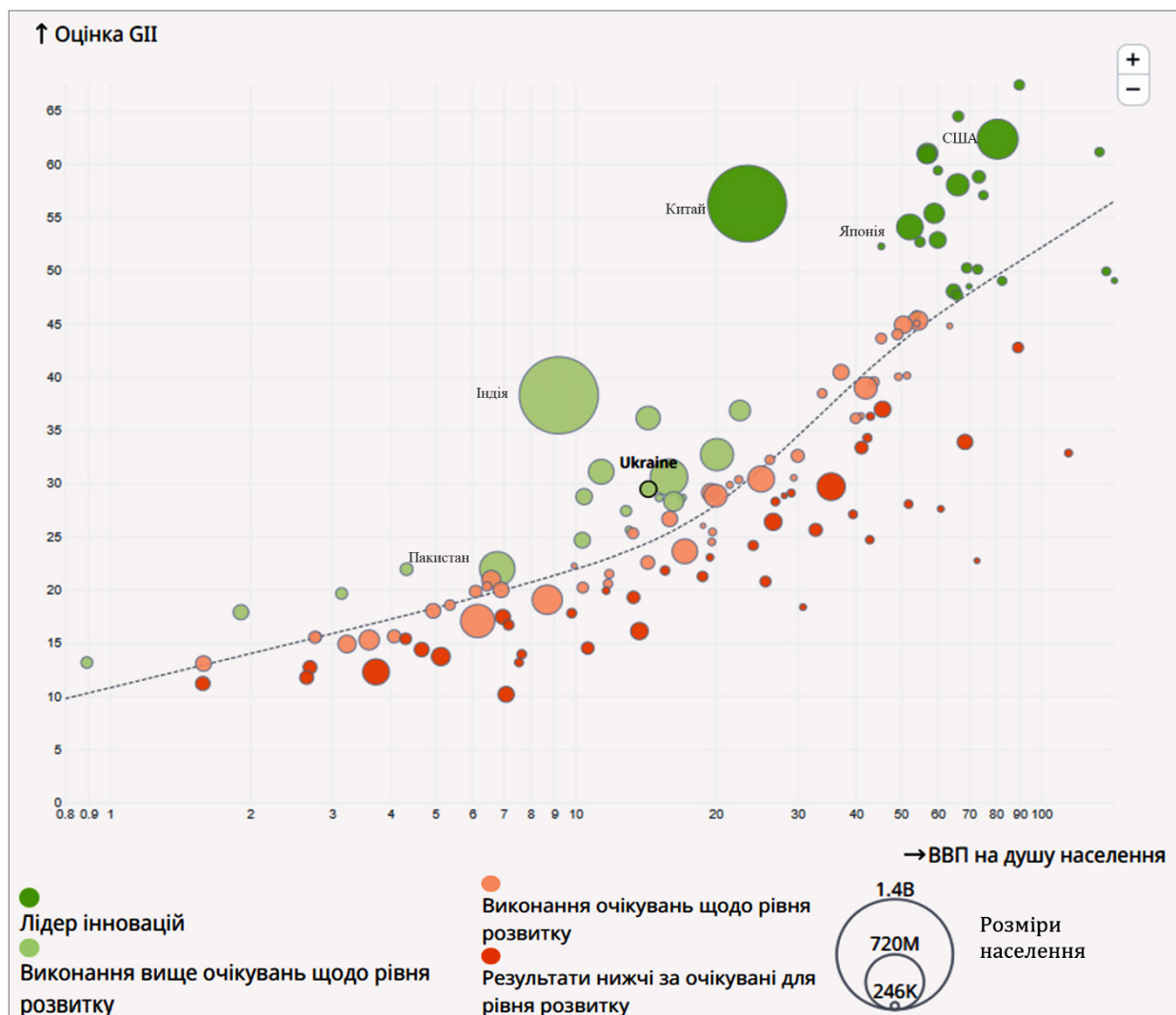


Рис. 1.

Джерело: сформовано за даними [7]

Таблиця 1

Сильні та слабкі сторони інновацій в Україні за показниками ГПІ 2024

	Ранг	Код	Назва індикатора
Сильні сторони	1	6.1.3	Корисні моделі за походженням/млрд. доларів США за ПКС ВВП
	2	5.1.5	Жінки, що працюють з вищою освітою, %
	4	6.2.3	Витрати на програмне забезпечення, % ВВП
	5	6.3.4	Експорт послуг ІКТ, % від загального обсягу торгівлі
	10	2.1.2	Державне фінансування/учень, середня школа, % ВВП/населення
	11	7.3.3	Створення мобільних додатків/млрд. доларів США за ПКС ВВП
	16	2.1.1	Витрати на освіту, % ВВП
	18 років	2.1.5	Співвідношення учнів до вчителів, середня школа
	20	7.1.4	Промислові зразки за походженням/млрд. доларів США за ПКС ВВП
	29	5.2.1	Спільні публікації державних досліджень та промисловості, %
Слабкі сторони	130	6.2.1	Зростання продуктивності праці, %
	125	3.2.3	Валове нагромадження капіталу, % ВВП
	123	1.1.1	Операційна стабільність для бізнесу*
	120	5.2.4	Угоди про спільні підприємства/стратегічні альянси/млрд. доларів США за ПКС ВВП
	115	3.3.1	ВВП/одинаця споживання енергії
	95	4.2.3	Одержувачі венчурного капіталу, угоди/млрд. доларів США за ПКС ВВП
	80	4.2.1	Ринкова капіталізація, % ВВП
	57	4.1.3	Кредити від мікрофінансових установ, % ВВП
	49	6.2.2	Оцінка єдиного, % ВВП
	41	2.3.3	Глобальні корпоративні інвестори в дослідження та розробки, трійка провідних, млн. доларів США

Джерело: сформовано за даними [7]

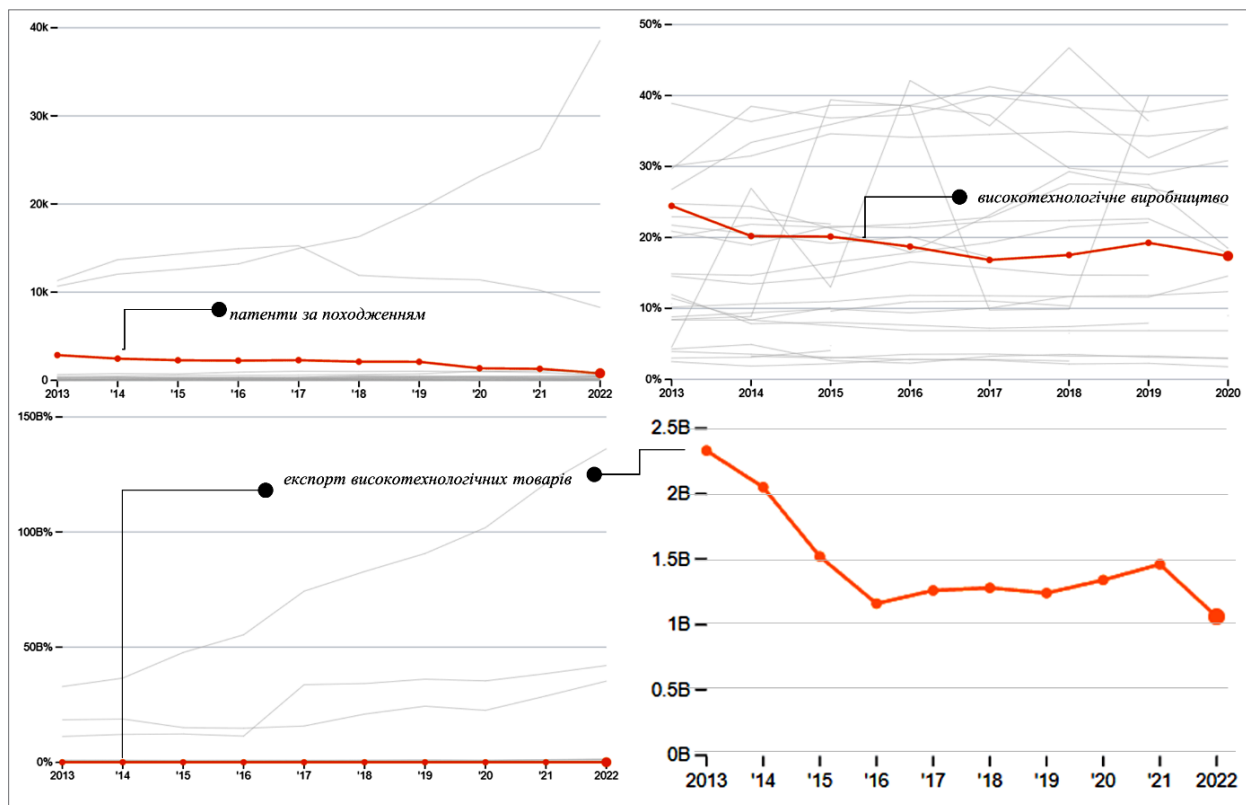


Рис. 2. Інноваційні результати в Україні 2014–2022 роки

Джерело: сформовано за даними [7]

та впровадження інновацій. В умовах глибоких трансформацій та відновлення після руйнувань, інституційні механізми повинні бути не лише стабілізуючими, а й адаптивними, динамічними та здатними до швидкого реагування на зміни в економічному та соціальному середовищі. Їх ефективність значною мірою визначає здатність держави забезпечити перехід до інноваційно-орієнтованої економіки та реалізувати стратегічні цілі національного відновлення.

Повномасштабна війна, розв'язана Росією проти України, кардинально змінила умови функціонування національної економіки, зумовивши потребу в перегляді державних пріоритетів, зокрема щодо підтримки інноваційної підприємницької діяльності. Знищення промислових активів, масове переміщення бізнесу, порушення логістичних ланцюгів та обмеження доступу до фінансування поставили інноваційне підприємництво в надзвичайно уразливе становище. У таких умовах роль держави як

регулятора та модератора інноваційного середовища суттєво зросла.

Чинне законодавство України визначає загальні принципи інноваційної діяльності, форми підтримки суб'єктів інноваційного підприємництва, інституційні повноваження державних органів та механізми їх реалізації. Основу правового поля становлять Закон України «Про інноваційну діяльність», Закон України «Про наукову і науково-технічну діяльність», Закон України «Про розвиток інноваційної інфраструктури», Податковий кодекс України, Концепція розвитку цифрової економіки та суспільства України, Стратегія інноваційного розвитку України на 2020–2030 роки, Закон України «Про державну підтримку інвестиційних проєктів зі значними інвестиціями» [8].

На сьогодні нормативно-правове забезпечення державної підтримки інноваційної діяльності залишається структурно сформованим, однак не повною

Таблиця 2

Аналіз нормативно-правове забезпечення державної підтримки інноваційної діяльності

Сильні сторони	Слабкі сторони
Наявність базових законів, що визначають правові засади інноваційної діяльності	Розпорошеність правового регулювання: відсутність єдиної рамкової політики
Створення державних інституцій підтримки (УФС, ДІФКУ)	Формальний характер діяльності більшості установ, низька ефективність їх роботи
Запровадження фінансових інструментів (гранти, кредити, пільги)	Недостатній обсяг фінансування, складний доступ до програм для МСП
Підтримка стартапів та цифрових інновацій в рамках державної цифрової політики	Відсутність сталої мережі інноваційних структур на регіональному рівні
Можливість імплементації іноземного досвіду через міжнародні проєкти	Слабка інтеграція науки та бізнесу, низький рівень комерціалізації НДДКР
Декларована підтримка державно-приватного партнерства	Відсутність чітких механізмів публічно-приватної кооперації в інноваційній сфері

Джерело: сформовано за даними [8]

Таблиця 3

Порівняння функцій ключових інституцій державної підтримки інноваційного підприємництва в Україні

Інституція	Основні функції у сфері інноваційного підприємництва
Міністерство економіки України	Розробка політики підтримки підприємництва, адміністрування інноваційних програм, державно-приватне партнерство
МОН України	Підтримка наукових досліджень, інтеграція науки та інновацій, управління університетськими стартапами
Фонд розвитку інновацій (УФС)	Грантова підтримка стартапів, акселераційні програми, просування інновацій на ранніх стадіях
Державна інноваційна фінансово-кредитна установа	Кредитування інноваційних підприємств, лізинг високотехнологічного обладнання, консультаційна підтримка
Офіс розвитку підприємництва та експорту	Сприяння інноваційній експортній діяльності, консалтинг, залучення міжнародних партнерів
Агенції регіонального розвитку (АРР)	Місцеві проєкти з підтримки інновацій, розбудова регіональних кластерів, залучення місцевого бізнесу
Центри інноваційної інфраструктури (хаби, інкубатори, парки)	Надання офісного простору, менторських програм, комунікаційної підтримки, зв'язків із інвесторами

Джерело: сформовано за даними [8]

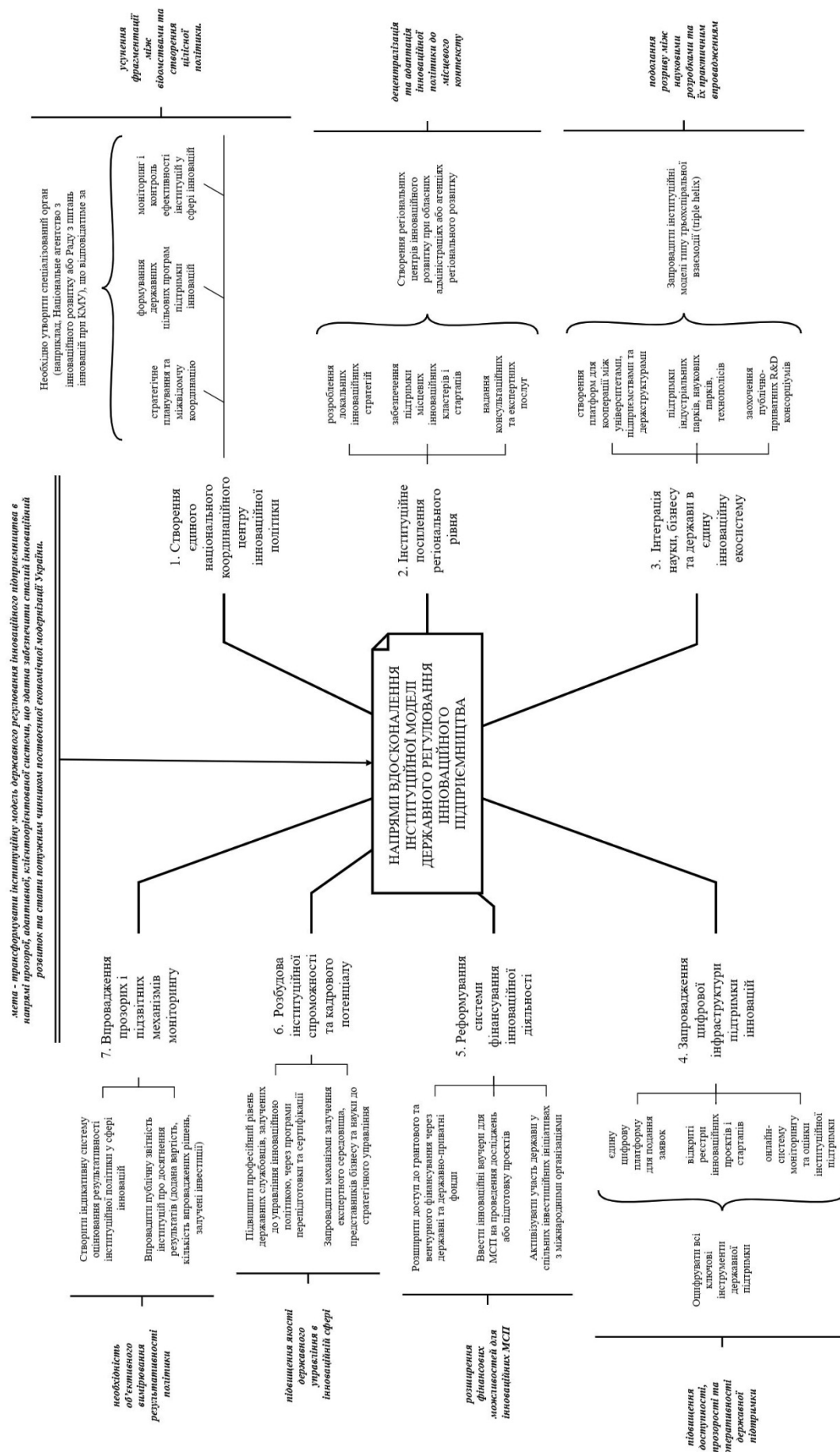


Рис. 3. Архітектура інституційних рішень у сфері державного регулювання інноваційного підприємництва

мірою адаптованим до викликів воєнного стану. Проведений аналіз свідчить про наявність слабких і сильних сторін, що відображено у таблиці 2.

Інституційна структура державної підтримки інноваційного підприємництва в Україні представлена низкою органів, зокрема Кабінет Міністрів України, Міністерство економіки України, Міністерство освіти і науки України, Фонд розвитку інновацій (у перспективі — Український Фонд стартапів), Державна інноваційна фінансово-кредитна установа (ДФКУ), Офіс розвитку підприємництва та експорту, а також Агенції регіонального розвитку та Інноваційні структури недержавного сектору: бізнес-інкубатори, наукові парки, стартап-хаби, IT-кластери, які все частіше діють у партнерстві з державними програмами (через механізми державно-приватного партнерства). Порівняння функцій ключових інституцій державної підтримки інноваційного підприємництва представлено у таблиці 3.

Попри збереження базових елементів нормативно-інституційної системи підтримки інноваційного підприємництва, наявні підходи потребують глибокої модернізації, з урахуванням викликів воєнного періоду. Йдеться насамперед про інтеграцію інновацій у пріоритети відбудови, посилення міжвідомчої координації, розширення цифрової платформи підтримки, а також перехід до гнучких і адаптивних інструментів стимулювання підприємництва в умовах кризи. З метою візуалізації напрямів вдосконалення інституційної моделі державного регулювання інноваційного підприємництва запропоновано модель архітектури інституційних рішень у сфері державного регулювання інноваційного підприємництва (рис. 3).

Наведена модель відображає цілісне бачення багаторівневої трансформації механізмів управління інноваційною сферою в Україні та ілюструє, як національний стратегічний рівень, регіональні ініціативи, науково-бізнесова взаємодія, цифрові інструменти, фінансові важелі, кадрова спроможність та прозора оцінка ефективності можуть бути поєднані в єдину, узгоджену модель регуляторного впливу.

Кожен із визначених напрямів є не ізольованим блоком, а взаємопов'язаним елементом управлінської системи, що забезпечує як формування загальнонаціональної інноваційної політики, так і її реалізацію на галузевому й територіальному рівнях. Сутність запропонованого підходу полягає в подоланні фрагментарності управлінських рішень шляхом впровадження єдиного координаційного центру, який відповідатиме за стратегічне планування, програмну цілеспрямованість та контроль досягнення результатів у сфері інновацій. Одночасно пропонується активне посилення ролі регіонів через створення центрів підтримки інноваційного розвитку, здатних реагувати на локальні економічні особливості.

Особливе місце у схемі займає інтеграція науки, бізнесу і держави, яка передбачає інституціалізацію

партнерств і формування сталих каналів трансферу технологій. Запропонована модель також акцентує на необхідності цифровізації всієї інфраструктури державної підтримки, що дозволить зробити процеси доступними, відкритими та контрольованими в реальному часі. Одночасно передбачається реформування системи фінансування інноваційної діяльності, розширення інструментів доступу до грантів, венчурного капіталу й інноваційних ваучерів.

Важливим доповненням до інституційної реформи є розвиток людського капіталу в системі публічного управління: підвищення кваліфікації держслужбовців, залучення експертного середовища, формування команд з аналітичною, проектною та технологічною компетентністю. Завершальним елементом моделі виступає впровадження системи моніторингу, орієнтованої на досягнення конкретних результатів, що забезпечить публічну підзвітність усіх учасників інноваційного процесу.

Запропонована модель репрезентує цілісну, гнучку й адаптивну модель державного регулювання інноваційного підприємництва, яка відповідає сучасним викликам трансформаційної економіки, а також потребам післявоєнної відбудови країни на засадах технологічного прориву та стійкого розвитку.

Висновки та перспективи подальших досліджень. Інституційні механізми державного регулювання відіграють ключову роль у формуванні сприятливого середовища для розвитку інноваційного підприємництва в умовах трансформаційної економіки України. Наявна система є фрагментованою, недостатньо ефективною, характеризується слабкою координацією між органами влади різних рівнів та обмеженим функціональним наповненням. Встановлено, що державна інноваційна політика в Україні реалізується через численні, але малоефективні інституції, серед яких відсутній єдиний стратегічний центр управління, що ускладнює вироблення цілісного бачення підтримки інноваційного бізнесу, зокрема малого та середнього. Чинна нормативно-правова база, хоча й охоплює базові засади підтримки інноваційної діяльності, потребує системного оновлення, гармонізації з європейськими підходами та реального наповнення фінансово-організаційними механізмами впровадження.

У ході дослідження виявлено ключові бар'єри: інституційна розпорошеність, дублювання функцій органів управління, недостатня інтеграція науки, бізнесу та держави, обмежений доступ до фінансування інновацій, низька цифровізація державних сервісів підтримки підприємництва.

Запропоновано багаторівневу модель інституційної модернізації, яка включає: стратегічну координацію, цифрову трансформацію інфраструктури підтримки, розвиток регіональних центрів інновацій, формування ефективної системи моніторингу результатів та посилення кадрової спроможності органів державної влади. Сформована модель від-

повідляє викликам поствоєнної відбудови України та створює передумови для забезпечення стійкого інноваційного зростання, зростання технологічної самодостатності країни та зміцнення конкурентних позицій українських підприємств на глобальному ринку.

Отримані результати можуть бути інституціоналізовані шляхом апробації моделі на пілотних регіонах, що мають високий інноваційний потенціал або значно постраждали внаслідок війни, із подальшим масштабуванням успішних практик через систему державного стратегічного управління.

Література

1. Філіпова Н. В. Механізм державного регулювання інноваційної діяльності. *Чернігівський державний інститут економіки і управління*. URL: <https://dspace.kntu.kr.ua/bitstreams/98f23097-3cc3-4e4d-b933-336f7768910d/download> (дата звернення: 06.05.2025).
2. Москалець І. М. Механізм реалізації державної політики інноваційного розвитку економіки України: дис. ... канд. екон. наук. Житомир, 2024. URL: https://ztu.edu.ua/site/files/1/docs/.../dis_%D0%9C%D0%BE%D1%81%D0%BA%D0%B0%D0%BB%D0%B5%D1%86%D1%8C.pdf (дата звернення: 06.05.2025).
3. Забашта Є. Ю. Формування механізму розвитку інноваційного підприємництва: дис. ... канд. екон. наук. Київ : КНУТД, 2021. URL: https://er.knutd.edu.ua/bitstream/123456789/17856/1/20210624_302.pdf (дата звернення: 06.05.2025).
4. Котельбан С. Механізм державного регулювання інноваційного розвитку економіки: теоретична основа дослідження. *Сталий розвиток економіки*. 2018. 3(40). С. 44–51. URL: <https://economdevelopment.in.ua/index.php/journal/article/view/133> (дата звернення: 06.05.2025).
5. Демчук С. В. Державне регулювання інноваційної діяльності підприємств: міжнародний досвід. *Економіка і регіон*. 2022. 2(85). С. 15–20. [https://doi.org/10.26906/EiR.2022.2\(85\).2626](https://doi.org/10.26906/EiR.2022.2(85).2626).
6. Левицький В. Нормативно-правове забезпечення інноваційної та інвестиційної діяльності промислових підприємств України. *Соціально-економічні проблеми і держава*. 2022. Вип. 2 (27). С. 25–34. URL: <http://sepd.tntu.edu.ua/images/stories/pdf/2022/22lvoppu.pdf> (дата звернення: 06.05.2025).
7. Ukraine ranking in the Global Innovation Index 2024. Global Innovation Index. *Innovation Ecosystems & Data Explorer*. URL: <https://www.wipo.int/gii-ranking/en/ukraine> (дата звернення: 06.05.2025).
8. Законодавство України: Офіційний вебпортал парламенту України. <https://zakon.rada.gov.ua> (дата звернення: 06.05.2025).

References

1. Filipova, N. V. (n.d.). *Mekhanizm derzhavnoho rehuliuvannia innovatsiinoi diialnosti* [Mechanism of state regulation of innovation activity]. Chernihiv State Institute of Economics and Management. Retrieved from <https://dspace.kntu.kr.ua/bitstreams/98f23097-3cc3-4e4d-b933-336f7768910d/download>
2. Moskalyets, I. M. (2024). *Mekhanizm realizatsii derzhavnoi polityky innovatsiinoho rozvytku ekonomiky Ukrainy* [Mechanism of implementation of state policy of innovation-driven economic development of Ukraine] (PhD dissertation). Zhytomyr. Retrieved from https://ztu.edu.ua/site/files/1/docs/.../dis_%D0%9C%D0%BE%D1%81%D0%BA%D0%B0%D0%BB%D0%B5%D1%86%D1%8C.pdf
3. Zabashta, Y. Yu. (2021). *Formuvannia mekhanizmu rozvytku innovatsiinoho pidpriemnytstva* [Formation of a mechanism for the development of innovative entrepreneurship] (PhD dissertation). Kyiv: KNUTD. Retrieved from https://er.knutd.edu.ua/bitstream/123456789/17856/1/20210624_302.pdf
4. Kotelban, S. (2018). *Mekhanizm derzhavnoho rehuliuvannia innovatsiinoho rozvytku ekonomiky: teoretychna osnova doslidzhennia* [Mechanism of state regulation of innovation-driven economic development: theoretical basis of the study]. *Stalyi rozvytok ekonomiky — Sustainable Development of Economy*, 3(40), 44–51. Retrieved from <https://economdevelopment.in.ua/index.php/journal/article/view/133>
5. Demchuk, S. V. (2022). *Derzhavne rehuliuvannia innovatsiinoi diialnosti pidpriemstv: mizhnarodnyi dosvid* [State regulation of innovative activity of enterprises: international experience]. *Ekonomika i rehion — Economics and Region*, 2(85), 15–20. [https://doi.org/10.26906/EiR.2022.2\(85\).2626](https://doi.org/10.26906/EiR.2022.2(85).2626)
6. Levytskyi, V., Radynskyi, S., & Diachun, O. (2022). *Normatyvno-pravove zabezpechennia innovatsiinoi ta inwestytsiinoi diialnosti promyslovykh pidpriemstv Ukrainy* [Legal support for innovation and investment activity of industrial enterprises in Ukraine]. *Sotsialno-ekonomichni problemy i derzhava — Socio-Economic Problems and the State*, 2(27), 25–34. Retrieved from <http://sepd.tntu.edu.ua/images/stories/pdf/2022/22lvoppu.pdf>
7. Global Innovation Index. (2024). *Ukraine ranking in the Global Innovation Index 2024: Innovation ecosystems & data explorer*. World Intellectual Property Organization. Retrieved from <https://www.wipo.int/gii-ranking/en/ukraine>
8. Verkhovna Rada of Ukraine. (n.d.). *Zakonodavstvo Ukrainy* [Legislation of Ukraine]. Official web portal of the Parliament of Ukraine. Retrieved from <https://zakon.rada.gov.ua>

НАУКОВЕ ФАХОВЕ ВИДАННЯ

Електронне наукове видання

«ПУБЛІЧНЕ АДМІНІСТРУВАННЯ ТА НАЦІОНАЛЬНА БЕЗПЕКА»

Electronic scientific publication

«PUBLIC ADMINISTRATION AND NATIONAL SECURITY»

№ 5 (58)

Головний редактор — *Романенко Є. О.*

Київ 2025

Видано у авторській редакції

Підписано до публікації 31.05.2025

Адреса редакції:
04070, м. Київ, Андріївський узвіз, буд. 11, оф. 68
Контактний телефон: +38(044) 222 58 89
Контактний телефон: +38(067) 401 84 35
E-mail: editor@inter-nauka.com