ПУБЛІЧНІ ІНТЕРЕСИ ЯК ОСНОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: СЕКТОРАЛЬНА СПЕЦИФІКА, ТРАНСФОРМАЦІЯ ПОЛІТИКО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

Колективна монографія

IZDEVNIECĪBA
BALTIJA
PUBLISHING
2026

УДК 34(082)
На308

Рецензенти:

Карабін Тетяна — доктор юридичних наук, професор, завідувач кафедри адміністративного, фінансового та інформаційного права Ужгородського національного університету;

Денисова Аліна — доктор юридичних наук, професор, завідувач кафедри адміністративного права та адміністративного процесу Одеського державного університету внутрішніх справ

Публічні інтереси як основа національної безпеки України: На308 секторальна специфіка, трансформація політико-правового забезпечення : колективна монографія. Рига, Латвія : Baltija Publishing, 2026. 880 с.

ISBN 978-9934-26-679-9

DOI https://doi.org/10.30525/978-9934-26-679-9

У монографії «Публічні інтереси як основа національної безпеки України: секторальна специфіка, трансформація політико-правового забезпечення» здійснено комплексне дослідження публічних інтересів як фундаментального елемента формування та реалізації державної політики у сфері національної безпеки України. Особливу увагу приділено теоретико-методологічним засадам розуміння публічного інтересу в умовах сучасних глобалізаційних процесів, цифрової трансформації та воєнних викликів. Розкрито взаємозв'язок між забезпеченням прав і свобод людини, стабільністю державних інституцій та ефективністю механізмів захисту національних інтересів у контексті сучасних безпекових загроз.

У праці проаналізовано секторальну специфіку реалізації публічних інтересів у ключових сферах суспільного життя, зокрема у сфері інформаційної безпеки, економічної політики, енергетичної безпеки, охорони здоров'я, освіти, кіберпростору та екологічної політики. Значну увагу приділено трансформації публічного управління в умовах воєнного стану та необхідності адаптації національного законодавства до сучасних викликів і європейських стандартів. Досліджено проблематику балансу між приватними та публічними інтересами, а також роль держави в забезпеченні стійкості суспільства в кризових умовах.

УДК 34(082)

© Колектив авторів, 2026
© ГО «Центр безпекових, правових та політичних досліджень», 2026

ISBN 978-9934-26-679-9

PUBLIC INTERESTS AS THE BASIS OF UKRAINE'S NATIONAL SECURITY: SECTORAL SPECIFICITY, TRANSFORMATION OF POLITICAL AND LEGAL SUPPORT

A collective monograph

IZDEVNIECĪBA
BALTIJA
PUBLISHING
2026

UDC 34(082)
Ha308

Reviewers:

Karabin Tetiana — Doctor of Law, Professor, Head of the Department of Administrative, Financial and Information Law of Uzhgorod National University;

Denysova Alina — Doctor of Law, Professor, Head of the Department of Administrative Law and Administrative Process of Odessa State University of Internal Affairs

Ha308 **Public** Interests as the Basis of Ukraine's National Security: Sectoral Specificity, Transformation of Political and Legal Support : a collective monograph. Riga, Latvia : Baltija Publishing, 2026. 880 p.

ISBN 978-9934-26-679-9
DOI https://doi.org/10.30525/978-9934-26-679-9

The monograph "Public Interests as the Basis of Ukraine's National Security: Sectoral Specificity, Transformation of Political and Legal Support" provides a comprehensive study of public interests as a fundamental element of the formation and implementation of state policy in the field of national security of Ukraine. Particular attention is paid to the theoretical and methodological principles of understanding public interest in the context of modern globalization processes, digital transformation and military challenges. The relationship between ensuring human rights and freedoms, the stability of state institutions and the effectiveness of mechanisms for protecting national interests in the context of modern security threats is revealed.

The work analyzes the sectoral specifics of the implementation of public interests in key areas of public life, in particular in the field of information security, economic policy, energy security, healthcare, education, cyberspace and environmental policy. Considerable attention is paid to the transformation of public administration in martial law and the need to adapt national legislation to modern challenges and European standards. The issue of the balance between private and public interests is studied, as well as the role of the state in ensuring the stability of society in crisis conditions.

UDC 34(082)

© Team of authors, 2026
© Center for security, legal and political studies, 2026

ISBN 978-9934-26-679-9

ЗМІСТ

Галупова Л. І.
Правова природа та класифікація технологій подвійного призначення . . . 1

Дуліна О. В.
Інфраструктурна безпека як складова забезпечення публічних інтересів у системі національної безпеки України . . . 40

Завгородня Ю. В.
Емпіричний аналіз кейсу кібератаки: механізм, наслідки та політико-правова кваліфікація . . . 92

Іванський А. Й.
Поняття, ознаки та особливості правового регулювання фінансових санкцій у мирний період та в умовах воєнного стану . . . 132

Кирилюк А. В.
Роль міжнародних стандартів щодо захисту ПІВ і задоволення суспільних інтересів у сфері фармації . . . 199

Ківалов С. В.
Забезпечення продовольчої безпеки України в умовах національного кризового адміністрування та глобальної нестабільності . . . 244

Копитова О. С.
Теоретико-правові засади застосування штучного інтелекту в правосудді: забезпечення балансу публічного і приватного інтересу . . . 287

Мазуренко С. В.
Гуманітарна та соціальна функції права інтелектуальної власності: теоретико-правові засади їх розмежування в системі права . . . 337

Намясенко О. К.
Безпекові виклики штучного інтелекту: правові аспекти 384

Петрик Д. П.
Особлива безпека як чинник національної безпеки 422

Пехник А. В.
Когнітивна безпека та медіатехнології в системі
захисту публічних інтересів України 455

Сапарова А. О.
Конституційно-правовий вимір цифрових прав людини 494

Слободянюк М. А.
Публічно-приватна співпраця у сфері кібербезпеки:
баланс інтересів держави, бізнесу та суспільства 538

Хорішко Л. С.
Strategic communications of the EU and Ukraine in implementing
public interests in the environmental sphere 602

Чернявська Б. В., Губачова Д. В.
Стійкість критичної інфраструктури у вимірі публічного
інтересу: правова конвергенція України та Європейського
Союзу за директивою (ЄС) 2022/2557 (CER) 640

Шатіло В. А.
Проблеми і перспективи розвитку унітаризму:
вітчизняний та зарубіжний досвід 706

Ястребова В. А.
Теоретико-ідеологічні засади політичної легітимації
російського окупаційного режиму 756

Ilnytska N. F.
Essence and elements of the mechanism of administrative
and legal regulation of the creation of legal entities 795

Karpa M., Kitsak T.
Architectonics of competence relations in public service 822

Krupenya I.
The Russian-Ukrainian war: a test for the international
legal order and global diplomacy 845

CONTENTS

Halupova L. I.
Legal nature and classification of dual-use technologies . . . 1

Dulina O. V.
Infrastructure security as a component of safeguarding public interests within the national security system of Ukraine . . . 40

Zavhorodnia Y. V.
Empirical analysis of the cyberattack case: mechanism, consequences and political and legal qualification . . . 92

Ivanskyy A. Y.
Concept, signs, and features of legal regulation of financial sanctions in peacetime and under martial law . . . 132

Kyryliuk A. V.
The role of international standards in protecting consumers and serving the public interest in the pharmaceutical sector . . . 199

Kivalov S. V.
Ensuring food security in ukraine in the conditions of national crisis management and global instability . . . 244

Kopytova O. S.
Theoretical and legal foundations for the use of artificial intelligence in the administration of justice: ensuring the balance between public and private interests . . . 287

Mazurenko S. V.
Humanitarian and social functions of intellectual property law: theoretical and legal foundations of their distinction within the legal system . . . 337

Namiasenko O. K.
Security challenges of artificial intelligence: legal aspects . . . 384

Petryk D. P.
Personal safety as a psychophysical factor of national security . . . 422

Pekhnyk A. V.
Cognitive security and media technologies in the system of protection of public interests of Ukraine 455

Saparova A. O.
Constitutional and legal dimension of digital human rights 494

Slobodianiuk M. A.
Public-private cooperation in cybersecurity: balance of interests of the state, business, and society 538

Khorishko L. S.
Strategic communications of the EU and Ukraine in implementing public interests in the environmental sphere 602

Chernyavska B. V., Hubacheva D. V.
Critical infrastructure resilience in the dimension of public interest: legal convergence of Ukraine and the European Union under directive (EU) 2022/2557 (CER) 640

Shatilo V. A.
Problems and prospects of the development of unitarism: domestic and foreign experience 706

Iastrebova V. A.
Theoretical and ideological foundations of the political legitimization of the russian occupation regime 756

Ilnytska N. F.
Essence and elements of the mechanism of administrative and legal regulation of the creation of legal entities 795

Karpa M., Kitsak T.
Architectonics of competence relations in public service 822

Krupenya I.
The Russian-Ukrainian war: a test for the international legal order and global diplomacy 845

ПРАВОВА ПРИРОДА ТА КЛАСИФІКАЦІЯ ТЕХНОЛОГІЙ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

LEGAL NATURE AND CLASSIFICATION OF DUAL-USE TECHNOLOGIES

Halupova L. I.,
Candidate of Law,
Associate Professor of the Department
of Intellectual Property Law and Patent Justice,
National University "Odesa Law Academy",
Odesa, Ukraine

Abstract. This section provides a comprehensive theoretical and legal analysis of the legal nature and classification of dual-use technologies in the context of contemporary challenges related to security, innovation, and the protection of intellectual property rights. It substantiates that dual-use technologies, due to their potential application in both civilian and military spheres, require a special legal regime that ensures a balance between the interests of national security, technological development, and the protection of private rights. Particular attention is paid to the ambiguity of the legal status of such technologies, which arises from their multifunctional nature and the intersection of different regulatory domains, including intellectual property law, export control, and security law.

The study proposes a doctrinal approach to defining dual-use technologies as complex legal objects that combine features of intellectual property objects and regulated goods within international and national control regimes. It also develops a classification of dual-use technologies based on functional purpose, degree of risk, and scope

of legal regulation. It is concluded that the effective regulation of dual-use technologies requires the formation of a coherent legal framework that integrates public and private law mechanisms and ensures proportionality between the interests of innovation and security.

Keywords: dual-use technologies, legal nature, classification, intellectual property, export control, national security, innovation, public interest, private interest, legal regulation.

1. Теоретико-правові підходи до розуміння технологій подвійного призначення

Генеза категорії технології подвійного призначення (dual-use) у міжнародному праві пов'язана з поступовим перетворенням технологій із «нейтрального» інструмента економічного розвитку на автономний фактор міжнародної безпеки, який потребує спеціального режиму правового стримування. Поняття технологій подвійного призначення виникло не як продукт класичної кодифікації, а як результат еволюції переважно «м'яких» міжнародних режимів експортного контролю, що формувалися у відповідь на дві взаємопов'язані тенденції: по-перше, на дифузію військово значущих інновацій у цивільні сектори (електроніка, матеріалознавство, аерокосмічна сфера, хімія та біотехнології), по-друге, на глобалізацію ланцюгів постачання і транснаціоналізацію знань, коли критичною стає не лише фізична поставка обладнання, а й передача документації, програмного коду, навчання, «технічної допомоги» та доступу до хмарних середовищ. У цій логіці технології подвійного призначення позначає не «подвійність» речі як такої, а правову оцінку її потенціалу: здатності цивільного продукту або знання бути інтегрованими у військову чи спеціальну техніку. Саме тому рання інституціоналізація контролю відбувалася через міждержавні координаційні механізми та контрольні списки, де «подвійне використання» функціонувало як критерій включення

до переліків і як підстава для дозвільної моделі експорту, а не як універсальна дефініція в конвенційному сенсі; у сучасній доктрині це розуміють як характерну рису експортного контролю: він спирається на комбінацію спискового підходу та оціночних категорій ризику, які держава конкретизує у внутрішньому праві. Українські дослідники справедливо підкреслюють, що міжнародні механізми контролю за трансфером товарів і технологій подвійного призначення історично розвивалися як «режимні» домовленості, вплив яких проявляється через національні регуляторні інструменти та практику їх застосування, зокрема через системи ліцензування і комплаєнсу (у вітчизняній літературі це детально аналізується на матеріалі ключових режимів і їхнього регуляторного «відлуння» в національних моделях) [2].

Після завершення біполярної конфронтації відбулася «перезбірка» експортно-контрольної архітектури: фокус з суто блокового стримування змістився на запобігання розповсюдженню чутливих технологій у ширшому колі ризиків, включно з регіональною нестабільністю, тероризмом та появою недержавних суб'єктів як адресатів контролю. Як наслідок, особливої ваги набуло те, що Рада Безпеки ООН, ухваливши Резолюцію 1540 (2004) на підставі Глави VII Статуту ООН, сформулювала для держав імперативний обов'язок встановлювати й забезпечувати ефективний контроль, зокрема експортний та прикордонний, щодо матеріалів і технологій, пов'язаних із ядерною, хімічною та біологічною зброєю та засобами її доставки, включаючи «пов'язані матеріали» й практично значимий для правозастосування пласт технологій подвійного призначеня [17]. У доктрині та практико-орієнтованих рекомендаціях підкреслюється, що Резолюція 1540 не замінює режимів спискового контролю, але виконує роль правового «якоря»: забезпечує універсальні межі, в яких держави деталізують переліки, процедури ліцензування, криміналізацію та

адміністративний нагляд (звідси — поява численних рекомендацій щодо імплементації Резолюції 1540 як стандарту належного експортного контролю) [6].

Європейська інтеграційна правова система, в свою чергу, інституціоналізувала категорію «технологію подвійного призначення» як елемент єдиного наднаціонального режиму контролю: нині визначальною віхою є Регламент (ЄС) 2021/821, який прямо фіксує, що «технології подвійного призначення» охоплюють не лише матеріальні об'єкти, а й програмне забезпечення та технологію, які можуть бути використані як у цивільних, так і у військових цілях, а також встановлює комплексний контроль експорту, брокерства, технічної допомоги, транзиту і передачі відповідних позицій [22]. Важливо, що європейська модель демонструє еволюцію від переважно спискового підходу до більш виразної ризик-орієнтації (зокрема у зв'язку з технологіями кіберспостереження та іншими «нематеріальними» трансферами), що концептуально підсилює тезу: технології подвійного призначення — це не статична «властивість речі», а правова кваліфікація в динамічному середовищі загроз та інновацій. Для українського дослідницького простору цінним є те, що у вітчизняних роботах простежується саме ця логіка: формування європейської моделі експортного контролю пояснюється як поєднання національних режимів і наднаціональних механізмів, які з часом набули уніфікованого характеру, а отже задають орієнтир для гармонізації підходів України з правом ЄС у сфері технологій подвійного призначення [3, с. 180].

У підсумку, генеза категорії технологій подвійного призначення в міжнародному праві відображає поступовий перехід від «епізодичного» політико-координаційного контролю технологій до багаторівневого правового режиму, де універсальні безпекові зобов'язання (передусім у площині нерозповсюдження) поєднуються з регіональними інтеграційними механізмами та національними

інструментами ліцензування і комплаєнсу; саме на цій основі в сучасній доктрині обґрунтовується потреба розглядати технології подвійного призначення як особливий об'єкт правового регулювання, у якому приватноправова логіка обігу знань та інновацій постійно взаємодіє з публічно-правовою логікою запобігання ризикам і забезпечення безпеки [2].

Наукова дискусія довкола поняття «технологія подвійного призначення» є значно більш суперечливою, ніж це видається з побіжного погляду на нормативні тексти. Попри значний інтерес до цієї теми, загальновизнаного визначення технологій подвійного призначення не склалось. Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» містить визначення товарів подвійного призначення — це окремі види виробів, обладнання, матеріалів, програмного забезпечення і технологій, спеціально не призначені для військового використання, а також послуги (технічна допомога), пов'язані з ними, які, крім цивільного призначення, можуть бути використані у військових або терористичних цілях чи для розроблення, виробництва, використання товарів військового призначення, зброї масового знищення, засобів доставки зазначеної зброї чи ядерних вибухових пристроїв, у тому числі окремі види ядерних матеріалів, хімічних речовин, бактеріологічних, біологічних та токсичних препаратів, перелік яких визначається Кабінетом Міністрів України [4].

Таким чином, можемо побачити, що українське законодавство оперує узагальненим поняттям «товари подвійного використання», яке є родовою категорією і охоплює декілька принципово різних за правовою природою об'єктів. Зі змісту статті 1 Закону України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» від 20 лютого 2003 року № 549-IV випливає, що до «товарів»

законодавець відносить одночасно: вироби та обладнання (матеріальні речі), матеріали (речовини), програмне забезпечення (нематеріальний об'єкт), технології (нематеріальний об'єкт), а також послуги технічної допомоги. Це є класичною законодавчою помилкою родо-видового змішання: «товар» у цивілістиці позначає матеріальний об'єкт цивільного обороту, тоді як технологія і програмне забезпечення є нематеріальними об'єктами, що за своєю правовою природою є результатами інтелектуальної, творчої діяльності і підпадають під режим права інтелектуальної власності. Визначення Європейської Комісії також оперує поняттям "dual-use items", що перекладається як «об'єкти подвійного призначення» відносячи до них водночас і товари, і програмне забезпечення, і технологію як таку, що свідчить про універсальну проблему правових систем — підпорядкування принципово різних за природою об'єктів єдиній адміністративній категорії заради зручності регуляторного контролю [29].

З точки зору права інтелектуальної власності ця конструкція є неприйнятною, оскільки вона ігнорує фундаментальний поділ об'єктів цивільного права на речі та результати інтелектуальної діяльності — поділ, що має принципові наслідки для режиму охорони, передачі та захисту прав. Тому для цілей дослідження необхідно провести чітке розмежування між трьома рівнями ієрархії понять.

Перший рівень — «товари подвійного призначення» у вузькому розумінні — охоплює виключно матеріальні об'єкти: обладнання, прилади, хімічні речовини, матеріали, компоненти. Вони є речами у цивільно-правовому розумінні, їхній обіг регулюється нормами про право власності, і право інтелектуальної власності стосується їх лише опосередковано — через охорону втіленого в них технічного рішення (винахід, промисловий зразок).

Другий рівень — «програмне забезпечення подвійного призначення» — є самостійною категорією, що посідає проміжне

місце: програмне забезпечення є нематеріальним об'єктом, охороняється переважно авторським правом як літературний твір, але може також патентуватися в частині програмно реалізованих винаходів, і водночас є найбільш рухливим об'єктом з точки зору контролю за передачею.

Третій рівень — «технології подвійного призначення» у власному, вузькому значенні — є тим об'єктом, який становить предмет дослідження з позицій права інтелектуальної власності: це нематеріальні результати інтелектуальної, творчої діяльності, що втілюють технічне рішення (винахід, корисна модель), виробничий процес, ноу-хау, технічну документацію або параметри навченої моделі ШІ.

Традиційне розмежування технологій подвійного призначення, що коріниться в епоху холодної війни і базується на протиставленні цивільного і військового секторів, є дедалі менш адекватним в умовах сучасного взаємопов'язаного технологічного ландшафту; академічна дефініція має розширити поняття технології за межі фізичних предметів — включивши до нього нематеріальні активи: програмне забезпечення, алгоритми і дані, визнаючи зростаюче значення цих елементів у сучасній геополітичній конкуренції [20].

З урахуванням викладеного пропонуємо таке авторське визначення: технології подвійного призначення — це результати інтелектуальної, творчої діяльності, що набувають об'єктивної форми вираження як технічні рішення, ноу-хау, програмне забезпечення, технічної документації та ін., яким іманентно притаманна функціональна бівалентність — конструктивно закладена, а не ситуативна здатність до рівноцінного застосування як у цивільній, так і у військовій, оборонній або іншій сфері, що становить підвищений ризик для міжнародного миру, безпеки або прав людини, — при цьому правовий статус таких результатів визначається не їхніми технічними характеристиками як такими, а сукупністю контекстуальних факторів передачі (профіль кінцевого

користувача, кінцеве призначення, геополітичні параметри транзакції), а самі результати підпорядковуються гібридному правовому режиму, що поєднує охоронні інструменти права інтелектуальної власності з публічно-правовим превентивним контролем над їх обігом і передачею.

Для детального правового аналізу даних об'єктів необхідно розглянути їх специфічні ознаки. Так, перша ознака — нематеріальність і відокремленість від матеріального носія. На відміну від «товарів» подвійного призначення, що є речами, технологія є нематеріальним об'єктом, що існує незалежно від будь-якого конкретного матеріального втілення. Один і той самий синтез хімічної речовини може бути описаний у патенті, зафіксований у технічній документації, збережений у пам'яті дослідника і переданий усно — і в усіх цих формах він залишається тією самою технологією. Ця ознака визначає принципову неможливість повного контролю над технологією через фізичний митний бар'єр і зумовлює необхідність механізмів контролю за нематеріальною передачею (intangible transfer of technology, ITT).

Друга ознака — іманентна функціональна бівалентність, яку необхідно відмежовувати від простої можливості зловживання. Визначення того, де продукт «вписується» у ринок, є менш питанням вихідної технології і більше питанням того, як він позиціонується і для кого він призначений; подвійність є не фізичною властивістю об'єкту, а функцією його архітектурних можливостей у конкретному ринковому і безпековому полі [14]. Правово релевантна бівалентність передбачає, що обидва застосування є технічно рівноцінними і не вимагають суттєвого перепроектування об'єкту: алгоритм розпізнавання образів, що однаково добре виконує функцію медичної діагностики і ідентифікації цілей, є бівалентним у цьому розумінні; кухонний ніж, що теоретично може бути використаний як зброя, бівалентним у правовому розумінні не є.

Третя ознака — контекстуальна невизначеність правового статусу, що є унікальною властивістю, не характерною для жодного іншого об'єкту права інтелектуальної власності. Патент на цивільний винахід залишається цивільним патентом незалежно від того, хто є покупцем ліцензії; авторське право на програму не змінює свого режиму від того, для яких цілей вона використовується. Технологія подвійного призначення, натомість, набуває різного правового статусу залежно від транзакції: та сама технологія є «цивільною» при передачі університету-партнеру і стає «контрольованою» при передачі суб'єкту з країни, що перебуває під санкціями. Регулювання намірів навряд чи здатне запобігти тому, щоб дослідження, що є доброчесним за задумом, пізніше використовувалося для ворожих цілей; саме тому правовий режим не може зупинятись на моменті створення об'єкту і неминуче охоплює весь ланцюг його передачі [1].

Четверта ознака — множинність форм правової охорони при відсутності оптимального єдиного інструменту. Технологія подвійного призначення може охоронятися патентним правом (технічне рішення), авторським правом (програмний код), правом на комерційну таємницю (ноу-хау, виробничі процеси) або режимом секретного патенту (при державному засекреченні). Жоден із цих інструментів не є достатнім окремо: патент вимагає публічного розкриття, що суперечить безпековим вимогам; авторське право охороняє форму, але не функцію; комерційна таємниця є чутливою і не забезпечує захисту від зворотного інженерування; секретний винахід (корисна модель) блокує комерціалізацію. Відтак суб'єкти у сфері оборонно-промислового комплексу змушені формувати гібридні портфельні стратегії охорони прав інтелектуальної власності.

П'ята ознака — структурна колізія між охоронним режимом права інтелектуальної власності і публічно-правовим контрольним

режимом. Право інтелектуальної власності надає правовласнику виключне право розпоряджатися результатом своєї творчої діяльності, включаючи право ліцензування будь-яким третім особам. Режим контролю за подвійним призначенням обмежує це право, вимагаючи державного дозволу на ліцензування іноземним контрагентам і забороняючи певні передачі незалежно від волі правовласника. Уряди регулюють товари подвійного призначення з метою запобігання їх неправомірному використанню у військових цілях або в актах тероризму; регуляторні рамки зменшують ризик потрапляння цих товарів до несанкціонованих рук, захищаючи національну безпеку і глобальну стабільність, — і саме ця публічна мета легітимує обмеження приватних прав інтелектуальної власності [15]. Ця ознака є вирішальною для правового конструювання: вона означає, що дослідження технологій подвійного призначення як об'єктів права інтелектуальної власності неможливе без одночасного аналізу публічно-правових обмежень, що деформують класичний режим виключних прав.

Шоста ознака — динамічна нестабільність класифікаційного статусу в часі. На відміну від об'єктів права інтелектуальної власності, чий правовий режим є відносно стабільним протягом строку охорони, технологія подвійного призначення може змінювати свій класифікаційний статус у зв'язку зі змінами технологічного ландшафту, геополітичної ситуації або оновленням контрольних переліків. Поняття подвійного призначення не є статичним, а динамічно формується еволюцією геополітичного процесу і технологічного прогресу; те, що вважається подвійного призначення, може змінюватись з часом і в різних геополітичних конфігураціях [20]. Це означає, що технологія, яка сьогодні є вільно ліцензованою, завтра може потрапити під режим контролю — і навпаки, що має прямі наслідки для чинності ліцензійних угод і патентних стратегій.

Таким чином, пропоноване авторське визначення і система ознак дозволяють чітко визначити предмет дослідження: ним є саме

нематеріальні результати інтелектуальної творчої діяльності, що характеризуються іманентною функціональною бівалентністю, — а не «товари» у широкому нормативному розумінні Закону України № 549-IV.

У науково-правовому дискурсі співвідношення понять військові технології, цивільні технології, стратегічні товари та чутливі технології розкриває різні функціональні, цільові та безпекові виміри технологічних об'єктів й визначає, на які саме групи правового регулювання вони підпадають.

Під військовими технологіями розуміють ті розробки та технічні рішення, які створюються насамперед для забезпечення обороноздатності та ведення воєнних дій, включно з озброєнням, бойовими системами, тактичними засобами чи спеціальними компонентами (безпілотні комплекси, системи наведення, оборонні інтегровані платформи тощо). Саме такі технології традиційно підлягають жорсткому експортному та внутрішньому контролю держави через їх прямий зв'язок з національною безпекою та обороною; у праві України це, зокрема, регулюється Законом України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання», де визначення товарів військового призначення та механізми їх контролю закріплені як окремі категорії контролю [4].

На противагу цьому цивільні технології — це технічні рішення, розробки, програмне забезпечення та обладнання, що створюються з метою задоволення потреб господарської діяльності, інфраструктури, науки чи побуту, не маючи первинного застосування у військовій сфері. Проте сучасний розвиток науки й техніки призводить до того, що межа між цивільними й військовими технологіями стає розмитою: технології, що спочатку мали виключно цивільне призначення, здатні бути модернізованими або адаптованими для використання у військових цілях, що саме і створює

поле для концепції технологій подвійного призначення. Такі приклади містяться у профільній літературі: безпілотні літальні апарати (UAV), навігаційні системи, складні матеріали та програмне забезпечення, що застосовуються в обох сферах [14].

У контексті міжнародних режимів експортного контролю виділяють також категорію стратегічних товарів, яка включає не лише чисто військові засоби, але й товари і технології, що мають потенційно системне значення для обороноздатності, національної безпеки чи життєзабезпечення держави. У правовій доктрині стратегічні товари розглядаються як ширша категорія, до якої належать: зброя, боєприпаси, військова техніка, але також певні технології подвійного призначення, критичні матеріали, програмне забезпечення та технічні дані, котрі можуть бути використані для створення або підтримки військових спроможностей або для критичної інфраструктури. Таким чином, стратегічні товари охоплюють як військові, так і технології подвійного призначення і є предметом централізованого національного та міжнародного контролю у торгівлі та передачі технологій [24].

Важливою для розмежування є також категорія чутливих технологій (sensitive technologies), яка в науково-правовому і практичному застосуванні найчастіше належить до підгрупи стратегічних технологій, але з додатковою характеристикою підвищеного ризику. Чутливими вважаються ті технології або компоненти, розкриття, передача або непряме використання яких може суттєво підсилити можливості військових систем або обійти національні / міжнародні механізми контролю, навіть якщо вони технічно не є зброєю. Це може включати криптографію високого рівня, мікроелектроніку, деякі класи програмних продуктів, а також складні алгоритми та знання, які прямо не є озброєнням, але суттєво впливають на оборонні чи безпекові спроможності. У практичних посібниках із експортного контролю такі чутливі технології часто змішуються

з технологіями подвійного призначення, але головна відмінність полягає в ризиковому потенціалі їх застосування, що обумовлює необхідність більш суворих механізмів контролю.

З погляду правового аналізу, ці поняття не є ізольованими: вони формують ієрархічну систему класифікації технологічних об'єктів, де військові технології складають найвищий рівень безпекового контролю, цивільні — базовий рівень цивільного застосування, стратегічні товари включають систему контрольованих об'єктів із визначеним потенціалом загрози, а чутливі технології — підгрупу всередині стратегічних і технологій подвійного призначення, що потребують підвищеної уваги і специфічних правових механізмів регламентації. Такий підхід дозволяє більш диференційовано оцінювати як національно-правові режими контролю передачі технологій (експорт, трансфер, ліцензування), так і міжнародні зобов'язання щодо нерозповсюдження, ефективно балансуючи між свободою технічної інновації та потребами забезпечення безпеки.

У науково-правовому аналізі критерії віднесення технологій до категорії подвійного призначення виступають не лише технічними ознаками, а правовими параметрами, які дозволяють відрізнити об'єкти, щодо яких законодавець чи міжнародний режим має право застосовувати спеціальні режими контролю. У сучасних моделях регулювання (зокрема, режим ЄС щодо dual-use цього поняття вживає як основу для класифікації товарів, програмного забезпечення і технології, що можуть бути використані для цивільних і військових застосувань) ключовими стають три підходи: функціональний, цільовий та ризик-орієнтований [9].

Функціональний підхід передбачає аналіз функції технології чи товару — тобто того, які саме операції чи дії може здійснювати об'єкт у своїх базових режимах. За таким критерієм до товарів подвійного призначення належать технології з технічними характеристиками, що усвідомлено спроектовані або імплементовані

для застосування як у мирних, так і у військових цілях. Наприклад, радіолокаційні системи, високотехнологічні матеріали або програмні блоки навігації мають первинно цивільну функцію, але їх функціональний потенціал може бути використаний і в оборонних системах. Саме функціональна універсальність є ключем до формалізації технологій подвійного призначення як предмету експортного контролю: це не тільки наявність цивільних функцій, а й їх здатність бути перенаціленими на оборонні застосування [10].

Цільовий підхід фокусує увагу не лише на технічних можливостях об'єкта, а на цілях і намірах потенційного користувача чи контексті застосування. Тут юридичне значення має саме заплановане використання: якщо технологія використовується для створення озброєнь, підтримки військових операцій або розробки засобів військового характеру, вона може бути класифікована як подвійного призначення навіть за відсутності очевидної технічної універсальності. Такий підхід тісно переплітається з механізмами експортних ліцензій і контролю кінцевого використання (end-use control), що передбачають оцінювання претендента на експорт за намірами, ринковою метою й кінцевим споживачем. Це особливо важливо у міжнародних режимах, де сам факт експорту «нейтрального» товару може створювати ризики для безпеки залежно від кінцевої мети отримувача [9].

Третім важливим критерієм є ризик-орієнтований підхід — він виходить з оцінки потенційного ризику для безпеки, незалежно від функціонального чи цільового використання в конкретному випадку. За цим підходом технологія визнається подвійного призначення, якщо її потенційний вплив на безпеку перевищує визначений поріг ризику, навіть якщо фактичні функції чи цільове застосування ще не мають прямого зв'язку з військовою сферою. Регламент ЄС щодо контролю такого експорту використовує подібну логіку оцінювання ризику для позицій, що не завжди перелічені у традиційних списках, але при цьому можуть бути

використані для розповсюдження озброєнь або порушення міжнародних зобов'язань.

У комплексі ці підходи дозволяють формалізувати критерії класифікації технологій, які мають бути включені до національних чи міжнародних переліків, що підлягають контролю:

— через оцінювання функцій — вирішується, чи здатний об'єкт виконувати операції військового характеру;

— через аналіз цілей — встановлюється, як саме об'єкт буде використаний кінцевим споживачем;

— через ризикову оцінку — визначається, чи його передача створює значущі ризики для безпеки.

Така синтетична модель є гнучкішою за прості перелікові підходи, оскільки вона дозволяє враховувати технологічні зміни, інтегрованість у глобальні ланцюги та небезпеки, що виникають у контексті новітніх технологій (наприклад, штучного інтелекту, телекомунікацій, навігаційних систем та інших ІТ-інструментів), що все частіше піднімається в сучасних наукових дискусіях про технології подвійного призначення (зокрема у рамках дискусій щодо регулювання новітніх технологічних платформ) [11].

Проблема правової невизначеності і динамічності переліків технологій подвійного призначення — це одна з центральних проблем сучасних режимів експортного контролю, що має як теоретико-правове, так і прикладне значення для національного та міжнародного права. Сутність цієї проблеми полягає в тому, що самі переліки технологій, що підлягають контролю, не є статичними або апріорно визначеними, а постійно змінюються під впливом технологічного прогресу, геополітичних ризиків та різних інтересів держав-учасниць міжнародних режимів контролю, що, у свою чергу, породжує правову невизначеність для правозастосувачів і приватних суб'єктів господарювання.

По-перше, більшість сучасних міжнародних та регіональних механізмів експортного контролю, наприклад режим Wassenaar

Arrangement (Вассенаарські домовленості) [29], базуються на переліковому підході, де перелік товарів і технологій подвійного призначення фіксується у вигляді довгих списків категорій і позицій, що підлягають контролю. Проблема в тому, що перелік не здатен одночасно охопити всі новітні технології або бути імперативно точним щодо майбутніх інновацій, оскільки технологічна реальність розвивається швидше, ніж механізми його редагування. Це означає, що деякі продукти чи технології можуть технічно відповідати критеріям технологій подвійного призначення, але юридично не бути включеними до списку, оскільки список ще не встиг оновитися. Така невідповідність створює правову невизначеність у правовому статусі окремих об'єктів і ставить суб'єктів господарювання у ситуацію, коли немає чітких орієнтирів стосовно того, чи підпадає їх продукція під контроль [30].

По-друге, динамічність переліків стимулюється не тільки технологічним прогресом, але й геополітичними факторами. Наприклад, у контексті останніх змін, таких як оновлення Annex I Регламенту ЄС щодо контролю технологій подвійного призначення, переліки доповнюються новими позиціями для реагування на конкретні загрози або геополітичні виклики; відповідно, вони можуть змінюватися щороку або навіть частіше. Це підтверджується оновленнями переліків ЄС у 2025 році, коли були внесені нові позиції для контролю технологій (що відображає прагнення адаптуватися до актуальних ризиків) [8].

По-третє, така постійна неузгодженість і динаміка призводять до кількох правових наслідків:

— прозорість нормативного регулювання знижується, що ускладнює прогнозування правового статусу нових технологій;

— нормативна визначеність підривається, оскільки законодавство не завжди може забезпечити чіткі критерії віднесення технологій до контролюваних категорій;

— міжнародна кооперація зменшується, якщо регіони (наприклад, ЄС та окремі держави) різняться в оцінці того, які технології підпадають під контроль, що створює фрагментацію правового середовища [23].

Наукові дослідження також показують, що така невизначеність має системний характер, оскільки термін «технології подвійного призначення» сам по собі є широким, а поля можливого застосування технологій зростають у різних секторах — від біотехнологій і штучного інтелекту до квантових обчислень, що ще більше ускладнює фіксацію таких товарів у переліках [19].

У міжнародному праві нормативне закріплення поняття технологій подвійного призначення відбувається передусім через режими експортного контролю, які формують стандарти, критерії віднесення й механізми правового регулювання передачі таких технологій. Найважливішим з них є Вассенаарські домовленості — багатосторонній режим контролю експортів звичайних озброєнь та товарів і технологій подвійного призначення, створений у 1996 р. як наступник холодновоєнної системи CoCom для просування прозорості, відповідальності й стабільності у міжнародній торгівлі такими об'єктами. Сам Вассенаарські домовленості щодо контролю за експортом звичайних озброєнь та товарів і технологій подвійного призначення не є міжнародним договором із обов'язковою юридичною силою, а виступає погодженою групою держав-постачальників, які узгоджують контрольні списки — списки контрольованих товарів і технологій та принципи їх застосування — і обмінюються інформацією про експортні ліцензії та відмови у видачі ліцензій, щоб уникати «дестабілізуючих накопичень» озброєнь та чутливих технологій у третіх державах. Такий режим координує національні політики, де кожна держава в межах своїх національних правових систем застосовує власний контроль, але базується на спільних списках і принципах, узгоджених в Домовленостях [31].

Вассенаарські домовленості фактично є нормотворчим джерелом для сучасних режимів контролю технологій подвійного призначення, оскільки саме через них сформовано Перелік товарів і технологій подвійного призначення — базовий перелік товарів і технологій, які можуть бути як цивільними, так і військовими за призначенням, структурований за категоріями (матеріали, електроніка, комп'ютери, телекомунікації тощо). Ці списки оновлюються щороку на засіданнях членів Вассенаарських домовленостей, і хоча вони не мають прямої міжнародно-правової обов'язковості, вони широко впливають на національні правові режими експортного контролю та відповідні переліки, включаючи ЄС та Україну.

У цьому контексті режими експортного контролю виступають як нормативні «ядра» міжнародної системи нерозповсюдження: вони поєднують елементи м'якого права (координаційні принципи, рекомендації, контрольний список) з обов'язковим імплементаційним національним правом. Важливо підкреслити, що такі режими не врегульовують технології само по собі, а встановлюють умови, за яких держави повинні запроваджувати національні процедури контролю над їх експортом і трансфером, зокрема через ліцензування, моніторинг кінцевого використання тощо. Саме тому сучасні наукові праці підкреслюють, що Вассенаарські домовленості і подібні процедури стали нормативним орієнтиром і каталізатором розвитку національних режимів контролю технологій подвійного призначення, а не обов'язковими нормативними джерелами в класичному міжнародно-правовому розумінні [2].

Ще одним важливим чинником нормативної рамки міжнародного контролю є співвідношення таких режимів із Світовою організацією торгівлі (СОТ), яка, з одного боку, загалом підтримує принципи свободи торгівлі та недискримінації, а з іншого — визнає, що держава може запроваджувати обмеження в ім'я безпеки (наприклад, для запобігання поширенню озброєнь чи чутливих технологій),

якщо це відповідає загальним правилам. Відомо, що в рамках СОТ дилеми між експортним контролем і свободою торгівлі вирішуються через механізми забезпечення того, що заходи безпеки, застосовані державою-членом, не є маскуванням протекціонізму, а справді спрямовані на досягнення законної безпекової мети. Такий баланс між безпекою й торгівлею тісно пов'язаний із тим, як саме держава імплементує міжнародні списки та принципи режимів експортного контролю, що призводить до необхідності узгодження національного права з міжнародними стандартами, водночас зберігаючи відповідність зобов'язанням СОТ щодо недискримінації [18].

У сукупності, ці елементи — Вассенаарські домовленості як джерело контрольних списків і принципів, режими експортного контролю як глобальні механізми координації, а також взаємодія з принципами свободи торгівлі та безпеки в межах СОТ — визначають сьогоднішнє нормативне закріплення поняття технологій подвійного призначення в міжнародному праві, яке не є одномоментним акцептом одного міжнародного договору, а побудовано на кооперації держав-постачальників, узгодженні стандартів і їх імплементації в національні правові системи.

2. Класифікація технологій подвійного призначення

Класифікація технологій подвійного призначення є не технічним, а принципово правовим завданням, оскільки вона вирішує питання про те, який нормативний режим застосовується до конкретного об'єкту, і тому будь-яка класифікаційна схема повинна відповідати не лише потребам систематизації знань, але і вимогам правової визначеності, передбачуваності та адміністративної здійсненності. Відсутність єдиної усталеної класифікації у доктрині і практиці є прямим наслідком принципової багатовимірності цих технологій як правового феномену — жоден єдиний критерій не є достатнім для їхньої повної характеристики, і кожен існуючий

підхід до класифікації відображає певну регуляторну логіку, обираючи один вимір як привілейований. Авторська позиція полягає в тому, що наукова класифікація технологій подвійного призначення як об'єктів права інтелектуальної власності повинна бути багаторівневою — тобто кожна технологія характеризується одночасно за кількома незалежними вимірами, що у своїй сукупності формують повний правовий профіль об'єкту.

Першим і найбільш операціоналізованим критерієм класифікації є галузево-предметний, що відповідає архітектурі чинних міжнародних режимів контролю. Список контрольованих предметів Вассенаарських домовленостей поділяється на дві частини: «Список предметів подвійного призначення та технологій» і «Список озброєнь», причому перший традиційно охоплює десять предметних категорій — від спеціальних матеріалів і пов'язаного обладнання до аерокосмічних і силових установок [26]. Ці десять категорій відображають галузевий зріз контрольованих технологій у том вигляді, в якому його бачить найбільш авторитетний багатосторонній режим конвенційного контролю. Поряд з ними діють режими, що охоплюють специфічні технологічні домени з принципово вищим рівнем деструктивного потенціалу: ядерні технології підпадають під режим Групи ядерних постачальників (NSG), ракетні — під MTCR, хімічні та біологічні — під Австралійську групу. З часів першого і єдиного застосування ядерної зброї у 1945 році науковці, аналітики і урядовці прагнуть визначити заходи стримування подальшого розповсюдження ядерних технологій; у кінці 1960-х розпочались аналогічні зусилля щодо біологічних наук, і сьогодні ті самі питання постають щодо інформаційних технологій, чий потенціал може поставити кіберзброю поряд з ядерною і біологічною у клубі технологій, здатних завдати масштабну шкоду [27]. Однак галузевий критерій є недостатнім сам по собі, оскільки він фіксує лише традиційні, кодифіковані в міжнародних режимах

домени і не відповідає на питання про правовий режим кросгалузевих технологій загального призначення.

Другим критерієм є класифікація за ступенем специфічності для деструктивних застосувань, яку в доктрині часто позначають як "military specificity" і яка відображає не галузеву приналежність, а глибину конструктивної орієнтованості технології на летальне застосування. З аналітичного погляду необхідно розрізняти декілька атрибутів розрізненності цивільного і військового застосувань: фізичні властивості — наскільки легко ідентифікувати технологію як таку, що стосується виключно військових цілей, виходячи з її зовнішніх характеристик; процес розробки — чи є цивільне і військове використання відокремленими чи об'єднаними на етапі розробки; доктрина і розгортання — чи визначає прийнята доктрина використання того чи іншого застосування технології. Виходячи з цього критерію, технології подвійного призначення утворюють три підкатегорії. До першої належать технології з низькою специфічністю — ті, чиї цивільне і військове застосування є рівноцінними і зовні нерозрізненними (алгоритми машинного навчання, базові хімічні синтези, телекомунікаційне обладнання загального призначення); правовий режим таких технологій є найменш обтяжливим, однак їхнє регулювання є найбільш складним. До другої належать технології з середньою специфічністю — ті, що мають чітко виражені цивільні застосування, але потребують відносно незначного перепрофілювання для деструктивного використання (прецизійне верстатне обладнання, певні матеріали з підвищеними фізичними властивостями, системи позиціонування та навігації). До третьої — технології з високою специфічністю, що є за своїм конструктивним задумом орієнтованими переважно на військове або деструктивне застосування і мають лише похідні цивільні аналоги (центрифуги для збагачення урану, спеціальні ракетні паливні суміші, засоби ураження біологічних агентів).

Третім і з точки зору права інтелектуальної власності є найбільш релевантним критерієм є класифікація за формою втілення, яка безпосередньо визначає, який саме правовий інструмент охорони застосовується і яким є режим контролю за передачею. Принципово важливим є те, що Вассенаарські домовленості поширюють контроль на «технологію» як на знання, що застосовується до розробки, виробництва або використання контрольованих предметів, незалежно від форми їх втілення, і прямо охоплюють як матеріальні предмети, так і програмне забезпечення та нематеріальні знання. Технологія залишається під контролем навіть тоді, коли вона застосовується до будь-якого неконтрольованого предмету, а контроль не поширюється лише на ту «технологію», яка є мінімально необхідною для встановлення, функціонування, технічного обслуговування або ремонту тих предметів, що не підлягають контролю [13]. Виходячи з критерію форми втілення, технології подвійного призначення як об'єкти права інтелектуальної власності поділяються на чотири підкатегорії. Першу становлять технічні рішення, охоронювані патентним правом на винахід чи корисну модель, — це конструктивно оформлені, кодифіковані у формулі винаходу рішення, чий правовий режим найкраще вписується в класичну патентну систему, але водночас є найбільш вразливим до конфлікту між вимогою публічного розкриття і вимогою безпекового засекречення. Другу підкатегорію становить програмне забезпечення подвійного призначення, що охороняється переважно авторським правом як літературний твір, однак специфіка об'єкту полягає в тому, що небезпечний потенціал міститься не у формі коду, а в реалізованій ним функціональності, яка авторсько-правовою охороною не захищається. Третю підкатегорію становить ноу-хау і технічна документація — нематеріальні носії виробничого знання, що охороняються переважно режимом комерційної таємниці і є найбільш вразливими до неконтрольованого витоку через нематеріальну

передачу. Четверту, принципово нову підкатегорію становлять параметри навчених моделей штучного інтелекту — математичні структури у вигляді вагових матриць нейромережі, що не підпадають у чистому вигляді під жоден із класичних об'єктів права інтелектуальної власності і є найбільш проблематичним об'єктом контролю з точки зору як ідентифікації, так і правової охорони.

Четвертим критерієм є класифікація за вектором технологічного трансферу, що дозволяє розрізняти технології залежно від напрямку їхнього первинного розвитку і подальшої дифузії. В доктрині усталилось розрізнення між так званими "spin-off" технологіями, що виникли у військовій сфері і поширились у цивільну (класичним прикладом є Інтернет, GPS, мікрохвильові печі), та "spin-on" або "spin-in" технологіями, що виникли у комерційній сфері і були адаптовані для військового використання. Оборонна промисловість тривалий час функціонувала як критичний двигун технологічних інновацій і нерідко «відгалужувала» (spin off) розроблені нею технології у комерційну сферу; сьогодні ситуація дедалі більше змінюється на протилежну — армії все більше залежать від технологій, первісно розроблених для комерційних ринків і потім вбудованих (spin into) в оборонний сектор [15]. Ця зміна вектору трансферу має принципове значення для права інтелектуальної власності: spin-off технологія, як правило, розроблялась з державним фінансуванням і підпадає під режим службових розробок у сфері ОПК, тоді як spin-in технологія є комерційною і охороняється в рамках звичайного цивільного режиму права інтелектуальної власності, однак при її придбанні державою або при спробі надати до неї доступ іноземним контрагентам вона стикається з обмеженнями режиму контролю за подвійним призначенням. Особливо важливою є третя категорія — технології загального призначення (General Purpose Technologies, GPT), що розвиваються паралельно в обох секторах без чіткого первинного

вектору: нові технологічні домени — наноматеріали, когнітивні науки, інформаційні технології, штучний інтелект, аналітика даних і машинне навчання — суттєво просунули людський соціальний і економічний добробут, але водночас породили потенціал для їхнього використання в зловмисних цілях; до цього слід додати безпілотні літальні апарати, адитивне виробництво, квантові обчислення і нейротехнології [12].

П'ятим критерієм є класифікація за темпоральним виміром — розрізнення між «зрілими» (mature) і «виникаючими» (emerging) технологіями подвійного призначення, що відображає принципово різні регуляторні виклики. Зрілі технології мають усталений профіль ризику, кодифіковані у контрольних переліках і є предметом відпрацьованих процедур ліцензування; їх правовий режим є відносно передбачуваним. Виникаючі технології є за своєю природою нестабільними в класифікаційному відношенні: їхні можливості нелінійно зростають, нові застосування виникають швидше за регуляторну реакцію, і вони нерідко є кросплатформними і кросдисциплінарними, що унеможливлює їхнє віднесення до будь-якої однієї галузевої категорії. Оновлення переліку контрольованих предметів ЄС у 2025 році приводить його у відповідність до рішень, прийнятих у рамках Вассенаарських домовленостей, MTCR, Австралійської групи і NSG у 2024 році, і забезпечує ефективніший контроль на рівні ЄС над новими технологіями, що відповідає цілям безпеки в торгівлі предметами подвійного призначення; зокрема, оновлення передбачає запровадження нових позицій, пов'язаних із квантовими технологіями [16]. Конвергенція виникаючих технологій є особливо виклично: перспектива ШІ-синтетичної біології суттєво збільшує біоризики і породжує новий набір проблем подвійного призначення — хоча біоризик підпадає під усталений режим управління, навіть експериментальне, але легітимне використання вченими може призводити до несподіваних розробок [5]. Це означає,

що виникаючі технології вимагають не просто включення до нових рядків існуючих переліків, а принципово іншого регуляторного підходу, що ґрунтується на оцінці ризику, а не на апріорній специфікації.

Шостим критерієм є класифікація за суб'єктним профілем розробника і режимом фінансування, що є принципово важливим саме з точки зору права інтелектуальної власності, оскільки від нього залежить питання про первинне виникнення прав і про режим їх обмеження державою. Тут розрізняють технології, розроблені в рамках державного оборонного замовлення з повним державним фінансуванням, де права на результати належать державі або обтяжені її ліцензією; технології, розроблені в рамках змішаного фінансування, де виконавець зберігає право власності з обов'язковою урядовою ліцензією і можливістю право примусового втручання держави у використання патенту; технології, розроблені приватним суб'єктом за власні кошти, де права інтелектуальної власності виникають у повному обсязі без державних обтяжень, однак передача таких технологій підпадає під режим контролю при спробі ліцензування іноземним контрагентам; і нарешті технології, що виникли в академічному і науковому середовищі і є предметом принципового конфлікту між свободою наукового обміну та вимогами безпекового контролю за нематеріальною передачею.

Сьомим критерієм, що є специфічним для завдань саме цього дослідження, є класифікація за відповідністю об'єкту класичним категоріям права інтелектуальної власності, що дозволяє структурувати подальший правовий аналіз. За цим критерієм виокремлюються: технології, що повністю охоплюються класичними об'єктами права інтелектуальної власності (патентоздатні технічні рішення, охоронювані авторським правом програми, ноу-хау та комерційна таємниця); технології, що частково охоплюються класичними об'єктами (алгоритми ШІ, де патентується технологія як винахід,

але не математична суть; програмно-апаратні комплекси, де окремі компоненти охоронюються різними інструментами); і технології, що принципово не охоплюються наявними категоріями права інтелектуальної власності в їх усталеному розумінні — насамперед вагові параметри навчених нейромереж і технічні знання, що існують виключно у вигляді некодифікованого досвіду носіїв. Конвергенція ШІ і синтетичної біології — два найдинамічніших технологічних домени — прискорює розробку нових технологій у медицині, сільському господарстві, але водночас створює нові ризики подвійного використання і прогалини в управлінні, які ставлять під сумнів адекватність будь-яких класифікаційних схем, побудованих на статичних переліках [28].

Синтез цих семи класифікаційних критеріїв дозволяє стверджувати, що технологія подвійного призначення не є однорідною правовою категорією, що дозволяє застосувати до неї єдиний правовий режим, а є простором правових режимів, що розрізняються залежно від поєднання класифікаційних ознак. Технологія, що одночасно є ядерною за галузевою приналежністю, має високу специфічність деструктивного застосування, втілена у формі ноу-хау, розроблена з державним фінансуванням і є зрілою в темпоральному відношенні, — це принципово інший правовий об'єкт, ніж технологія ШІ, що є технологією загального призначення, має низьку специфічність, втілена у формі вагових параметрів нейромережі, розроблена приватним суб'єктом і є виникаючою у темпоральному відношенні. Саме це розуміння є методологічним підґрунтям для подальшого дослідження специфіки правового режиму технологій подвійного призначення як об'єктів права інтелектуальної власності.

Суб'єктний склад правовідносин щодо технологій подвійного призначення є питанням, що безпосередньо визначає практичну здійсненність будь-якого класифікаційного режиму і є вихідною

точкою для розуміння правового режиму охорони: адже обсяг прав, обмежень і обов'язків суттєво різниться залежно від того, хто є первинним носієм прав на конкретну технологію. Аналіз суб'єктного складу з позицій права інтелектуальної власності дозволяє виокремити п'ять якісно різних суб'єктних груп, кожна з яких перебуває у специфічних правовідносинах із державою, режимом контролю за подвійним призначенням і системою охорони результатів інтелектуальної діяльності.

Першим суб'єктом є держава як безпосередній суб'єкт права інтелектуальної власності на технології подвійного призначення. Поширеним припущенням є те, що оборонні відомства самостійно винаходять усе, чим користуються; це могло бути ближче до правди в епоху холодної війни, коли уряди мали власні закриті дослідницькі лабораторії, однак ця модель трансформувалась: сьогодні більшість інновацій, що потрапляють у військові системи, виникає в приватному секторі [25]. Проте держава зберігає первинне право власності на технології, розроблені в рамках повністю державно фінансованих оборонних програм, реалізованих власними установами або через спеціальну конструкцію вилучення у підрядника. Відповідно до положень Департаменту енергетики США, держава набуває статус правовласника на всі винаходи, заплановані або вперше практично реалізовані в рамках виконання контрактів з великими комерційними компаніями, іноземними організаціями та іншими суб'єктами, що не є бенефіціарами закону про патентні права підрядників; лише у відповідних ситуаціях відомство може відмовитись від своїх патентних прав для заохочення участі промисловості, сприяння комерційному використанню та конкуренції [21]. Правовий статус держави як правовласника є принципово суперечливим: з одного боку, держава виступає суб'єктом забезпечення публічного інтересу у сфері безпеки, що легітимує обмеження прав приватних осіб; з іншого — вона є суб'єктом, що забезпечує реалізацію

системи охорони прав інтелектуальної власності. Ця подвійність породжує конфлікт інтересів, що є особливо очевидним у питанні примусового ліцензування: держава може одночасно бути власником патенту на технологію подвійного призначення і регулятором, що вирішує, кому дозволити доступ до цієї технології.

Другим суб'єктом є оборонні підрядники та компанії оборонно-промислового комплексу — суб'єкти, що перебувають у найбільш складних і багаторівневих правовідносинах щодо прав інтелектуальної власності на технології подвійного призначення. Уряд США не набуває автоматично права власності на запатентовані винаходи, розроблені з фінансуванням Міністерства оборони; Закон Бай-Доула, розширений Рональдом Рейганом у 1983 році спеціально для федеральних підрядників, дозволяє підрядникам зберігати патентні права, а уряд натомість отримує невиключну ліцензію на використання винаходу в урядових цілях [30]. Ця конструкція є принципово важливою для розуміння суб'єктного складу: підрядник залишається власником прав інтелектуальної власності, однак його право розпоряджатися є системно обтяженим урядовою ліцензією і потенційним правом march-in (механізм державного втручання). Підрядники, як правило, мають право зберігати право інтелектуальної власності на винаходи, розроблені в рамках урядових контрактів, але зобов'язані надати уряду ліцензію на використання цих патентів; щодо авторських прав — уряд може отримати права на відтворення, розповсюдження і демонстрацію творів, розроблених за контрактом; щодо комерційних таємниць — захист пропрієтарної інформації може бути оскаржений вимогою уряду на доступ [1]. Принципово важливим практичним питанням є «правило фінансування» (funding rule): обсяг прав уряду прямо залежить від пропорції урядового фінансування в розробці конкретного компонента технології. Відповідно до відомої практики "list it or lose it" підрядники зобов'язані у встановленій формі

ідентифікувати об'єкт права інтелектуальної власності, розроблену за приватні кошти до укладання договору або окремо від договору, якщо вони бажають зберегти обмежені права щодо неї; наприклад, підрядник, що розробив програмне забезпечення на основі штучного інтелекту за власні кошти, повинен вказати обмежені права держави на нього в переліку об'єктів, інакше ризикує тим, що уряд автоматично отримає необмежені права. Таким чином, оборонний підрядник є суб'єктом, у якого право інтелектуальної власності є формально збереженим, але функціонально обтяженим системою державних обмежень, що охоплює спектр від «обмежених прав» (limited rights) через «права для урядових цілей» (government purpose rights) до «необмежених прав» (unlimited rights) залежно від структури фінансування кожного конкретного технологічного компонента. У добу передового програмного забезпечення і штучного інтелекту уряд дедалі більше покладається на придбання комерційних технологій подвійного призначення для забезпечення стратегічної, оперативної і тактичної переваги збройних сил, і саме тому політика права інтелектуальної власності стала серйозною перешкодою для оборонних інновацій: програмні компанії, що прагнуть підтримати Міністерство оборони, ризикують втратити самі активи, що забезпечують їхній бізнес [15].

Третьою групою суб'єктів є університети та академічні дослідники — суб'єкти, що перебувають у принципово специфічному становищі через конфлікт між академічною свободою і вимогами контролю за нематеріальною передачею технологій. Контроль за передачею програмного забезпечення і технологій є одним із найскладніших завдань для органів, що впроваджують режими контролю за предметами подвійного призначення та зброєю, і ці проблеми особливо гостро виявляються у сфері застосування контролю в дослідницьких інститутах і академічному середовищі [11]. Правовий статус університету як суб'єкта прав інтелектуальної власності

на технології подвійного призначення є принципово неоднорідним. Закон Бай-Доула охоплює лише патентоздатні винаходи, що виникають із федерально фінансованих досліджень; непатентоздатні винаходи, твори, що підпадають під авторське право, комерційні таємниці і нематеріальна власність, зокрема дані, — всі вони можуть мати значну цінність як для університетів, так і для інших сторін, однак не підпадають під регулювання Бай-Доула [7]. Це означає, що університет є суб'єктом прав інтелектуальної власності на технологію подвійного призначення лише в тому обсязі, в якому ця технологія є патентоздатним винаходом, розробленим з федеральним фінансуванням, — що є вкрай вузькою категорією порівняно з усім масивом академічних знань, що складають технологію подвійного призначення в широкому розумінні. Особливо гострою є проблема суб'єктності індивідуального академічного дослідника. Верховний суд США у справі Stanford v. Roche вирішив, що патентне законодавство США завжди надавало перевагу правам індивідуальних винахідників і продовжить це робити, і що університетам для набуття права інтелектуальної власності на винаходи своїх дослідників необхідна письмова згода від останніх; це рішення є важливою перемогою для прав викладачів, оскільки воно підтверджує, що академічні дослідники є чимось значно більшим, ніж просто працівниками своїх установ [13]. Таким чином, індивідуальний академічний дослідник зберігає первинне право на результати своєї інтелектуальної діяльності, якщо тільки він не здійснив письмову уступку університету; однак навіть при збереженні цього права він є суб'єктом системи контролю за нематеріальною передачею технологій, що принципово обмежує його академічну свободу. Вассенаарські домовленості обмежують «нематеріальну передачу технологій» — тобто передачу знань про використання включених до списку предметів, — і це означає, що повсякденні академічні комунікації, включаючи наукові публікації, конференційні виступи

та навчання студентів і аспірантів з третіх країн, потенційно підпадають під контрольний режим.

Четвертою групою суб'єктів є компанії-розробники нових технологій, що не є традиційними оборонними підрядниками, однак чиї розробки дедалі більше потрапляють у сферу контролю за подвійним призначенням. Ця група є принципово новою в суб'єктному складі правовідносин у даній сфері і являє собою найбільш динамічний і найменш юридично захищений сегмент.

П'ятою групою є іноземні суб'єкти — кінцеві користувачі технологій подвійного призначення, — чий правовий статус є принципово обмеженим і залежним від рішень суб'єктів передачі і регуляторних органів країни-постачальника. У сфері права інтелектуальної власності іноземний суб'єкт є ліцензіатом або набувачем прав на використання технології, і саме в цій транзакції виникає класичний конфлікт між правом ліцензіара розпоряджатися своєю інтелектуальною власністю і публічно-правовою вимогою одержати дозвіл регулятора. Принципово важливим є те, що "deemed export" — презумпція того, що розкриття контрольованої технології іноземному громадянину навіть на території США є «експортом», — фактично трансформує будь-які відносини ліцензіара з іноземним ліцензіатом у об'єкт потенційного контролю: порушення режиму контролю може статися у власній лабораторії або офісі без того, щоб будь-що перетнуло фізичний кордон; наймання іноземних громадян і управління їхнім доступом до контрольованих технологій є основним викликом для дотримання вимог.

Синтезуючи характеристики всіх п'яти груп суб'єктів, необхідно констатувати, що суб'єктний склад правовідносин щодо технологій подвійного призначення є принципово поліцентричним: жоден суб'єкт не є одноосібним і повноцінним носієм прав на технологію подвійного призначення. Ця поліцентрична модель

суб'єктного складу є не випадковим результатом фрагментованого законодавства, а структурною відповіддю на неможливість зосередити в одному суб'єкті повноту прав на технологію, що одночасно є приватним активом і публічним безпековим ресурсом. Саме тому будь-яке регулювання технологій подвійного призначення як об'єктів права інтелектуальної власності є регулюванням складної мережі суб'єктних правовідносин, а не регулюванням ізольованого об'єкту.

Звіт Європейської Комісії 2025 року констатує певний рівень підготовленості України у сфері права інтелектуальної власності і підкреслює необхідність прийняття Національної стратегії розвитку інтелектуальної власності до 2030 року та продовження гармонізації з acquis ЄС в усіх релевантних сферах. Станом на листопад 2025 року Верховна Рада України розпочала публічні консультації щодо змін до Книги 4 «Право інтелектуальної власності» Цивільного кодексу України, серед яких — уточнення переліку об'єктів права інтелектуальної власності, запровадження понять «об'єкти sui generis» і «ноу-хау», уточнення понять «особисті права» та доповнення положень щодо комерційних таємниць. Це реформаторське вікно є унікальною можливістю для включення до Книги 4 ЦК України спеціальних норм щодо режиму охорони технологій подвійного призначення — насамперед щодо секретних патентів, службових розробок у сфері ОПК і обмежень ліцензування іноземним суб'єктам. Україна підтвердила зобов'язання щодо поступової реалізації гармонізації відповідно до Національної програми адаптації законодавства України до права Європейського Союзу, і у 2025–2026 роках планується розробка нових редакцій спеціальних законів щодо окремих об'єктів інтелектуальної власності для подальшого впровадження положень acquis ЄС. Тому, вдосконалення Закону України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» є не менш невідкладним завданням, ніж реформа

власне законодавства про інтелектуальну власність: необхідне концептуальне розмежування між «товарами» і «технологіями» як об'єктами принципово різних правових режимів, запровадження повноцінного механізму контролю за нематеріальною передачею технологій і синхронізація контрольних переліків з оновленим Додатком I до Регламенту (ЄС) 2021/821 на щорічній основі.

Список використаних джерел:

1. 2025 Update of the EU Control List of Dual-Use Items. URL: https://policy.trade.ec.europa.eu/news/2025-update-eu-control-list-dual-use-items-2025-09-08_en

2. Бенедик Я. С. Вплив міжнародних механізмів контролю за трансфером товарів і технологій подвійного призначення на розвиток національно-регуляторних інструментів у відповідній сфері. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2024. Випуск 84. Частина 4. С. 215–222. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/31-3.pdf

3. Грицишен Д. О., Абрамова І. В., Вакун О. В. Система вимог Європейського Союзу до експортного контролю за товарами військового призначення та подвійного використання. *Економіка, управління та адміністрування*. 2025. № 2 (112) С. 177–186.

4. Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання : Закон України від 20 лютого 2003 року № 549-IV. *Відомості Верховної Ради України (ВВР)*. 2003. № 23. Ст. 148. URL: https://zakon.rada.gov.ua/laws/show/549-15#Text

5. AI Model Outputs Demand the Attention of Export Control Agencies. URL: https://www.justsecurity.org/126643/ai-model-outputs-export-control/

6. Best practice guide on un security council Resolution (UNSCR) 1540 Export controls and transshipment URL: https://cdn.osce.org/sites/default/files/f/documents/d/0/41446.pdf

7. Dual Use Technology. Encyclopedia of Espionage, Intelligence, and Security. Encyclopedia.com. 17 Mar. 2026. URL: https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/dual-use-technology

8. Dual-use export controls as tools of EU economic security From coordination to a proactive EU approach. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/777960/EPRS_BRI%282025%29777960_EN.pdf

9. Dual-use export controls. URL: https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html

10. Dual-use items and technology. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al11029

11. Dual-use technologies. URL: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/dual-use-technologies_en

12. Dual-Use Technology and U.S. Export Controls. URL: https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls

13. Export of Commercial or Dual-Use items — EAR. URL: https://www.researchsecurity.pitt.edu/export-commercial-or-dual-use-items-ear

14. Exporting dual-use items. URL: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en

15. Fact Sheet: The Wassenaar Arrangement. URL: https://armscontrolcenter.org/fact-sheet-the-wassenaar-arrangement/

16. Federal Register Notices / Bureau of Industry and Security. URL: https://www.bis.gov/regulations/federal-register-notices?years=2026&categories=Proposed+rules%2CInterim+and+final+rules%2CExport+Administration+Regulations%2CNational+Security+Industrial+Base+Regulations%2CInformation+and+Communication+Technology+and+Services+Regulations%2CChemical+Weapons+Convention+Regulations%2CAdditional+Protocol+Regulations

17. Frequently Asked Questions on Resolution 1540 (2004). URL: https://www.un.org/en/sc/1540/faq.shtml

18. International Export Regulations and Controls: Navigating the global framework beyond WTO rules. URL: https://www.wto.org/english/res_e/publications_e/international_exp_regs_e.htm

19. János Székely. Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies. URL: https://real.mtak.hu/210722/1/309-354.pdf

20. List of Dual-Use Goods and Technologies and Munitions List (WA-LIST (23) 1). Vienna : Wassenaar Arrangement Secretariat, 2023. 312 p. URL: https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf

21. Multilateral Export Control Regimes. URL: https://www.bis.gov/guidance-frequently-asked-questions/multilateral-export-control-regimes

22. Regulation (EU) 2021/821 of The European Parliament and of the council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32021R0821

23. Sebastiaan Bennink, Jan Dunin-Wasowicz, Siqi Zhao, Sally Eshun, 'EU Export Controls on Dual-Use Items: Recent Developments and Emerging Trends', (2025), 20, *Global Trade and Customs Journal,* Issue 2, pp. 89–99. URL: https://kluwerlawonline.com/journalarticle/Global%2BTrade%2Band%2BCustoms%2BJournal/20.2/GTCJ2025011

24. Strategic Goods — Definition And Trade Obligations. URL: https://cgolegal.com/strategic-goods/

25. The Challenge of software and technology transfers to non — Proliferation efforts: Implementing and Complying with Export Controls. URL: https://www.sipri.org/sites/default/files/201804/sipri1804_itt_software_bromley_et_al.pdf

26. The Challenge of software and technology transfers to non — Proliferation efforts: Implementing and Complying with Export Controls.

URL: https://www.sipri.org/sites/default/files/201804/sipri1804_itt_software_bromley_et_al.pdf

27. The Wassenaar Arrangement at a Glance. URL: https://www.armscontrol.org/factsheets/wassenaar

28. Unlocking the strategic power of dual-use Technologies URL: https://www.adlittle.com/en/insights/viewpoints/unlocking-strategic-power-dual-use-technologies

29. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. URL: https://www.wto.org/english/res_e/booksp_e/int_exp_regs_part3_5_e.pdf

30. Wassenaar Arrangement. URL: https://en.wikipedia.org/wiki/Wassenaar_Arrangement

31. What is the Wassenaar Arrangement? URL: https://www.wassenaar.org/the-wassenaar-arrangement/

References:

1. European Commission. (2025). 2025 Update of the EU Control List of Dual-Use Items. Retrieved from https://policy.trade.ec.europa.eu/news/2025-update-eu-control-list-dual-use-items-2025-09-08_en

2. Benedyk, Ya. S. (2024).[The impact of international mechanisms for controlling the transfer of dual-use goods and technologies on the development of national regulatory instruments. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 84(4), 215–222. Retrieved from https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/31-3.pdf

3. Hrytsyshen, D. O., Abramova, I. V., & Vakun, O. V. (2025). EU requirements for export control of military and dual-use goods. *Economy, Management and Administration*, 2(112), 177–186.

4. Law of Ukraine "On State Control of International Transfers of Military and Dual-Use Goods" No. 549-IV (February 20, 2003). Retrieved from https://zakon.rada.gov.ua/laws/show/549-15#Text

5. AI Model Outputs Demand the Attention of Export Control Agencies. Retrieved from https://www.justsecurity.org/126643/ai-model-outputs-export-control/

6. OSCE. Best Practice Guide on UN Security Council Resolution 1540: Export Controls and Transshipment. Retrieved from https://cdn.osce.org/sites/default/files/f/documents/d/0/41446.pdf

7. Dual Use Technology. (2026). Encyclopedia of Espionage, Intelligence, and Security. Retrieved from https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/dual-use-technology

8. European Parliament. (2025). Dual-use export controls as tools of EU economic security: From coordination to a proactive EU approach. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/777960/EPRS_BRI%282025%29777960_EN.pdf

9. European Union. Dual-use export controls. Retrieved from https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html

10. European Union. Dual-use items and technology. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al11029

11. European Commission. Dual-use technologies. Retrieved from https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/dual-use-technologies_en

12. Center for a New American Security (CNAS). Dual-Use Technology and U.S. Export Controls. Retrieved from https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls

13. University of Pittsburgh. Export of Commercial or Dual-Use Items — EAR. Retrieved from https://www.researchsecurity.pitt.edu/export-commercial-or-dual-use-items-ear

14. European Commission. Exporting dual-use items. Retrieved from https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en

15. Arms Control Center. Fact Sheet: The Wassenaar Arrangement. Retrieved from https://armscontrolcenter.org/fact-sheet-the-wassenaar-arrangement/

16. Bureau of Industry and Security. Federal Register Notices. Retrieved from https://www.bis.gov/regulations/federal-register-notices?years=2026&categories=Proposed+rules%2CInterim+and+final+rules%2CExport+Administration+Regulations

17. United Nations. Frequently Asked Questions on Resolution 1540 (2004). Retrieved from https://www.un.org/en/sc/1540/faq.shtml

18. World Trade Organization (WTO). International Export Regulations and Controls. Retrieved from https://www.wto.org/english/res_e/publications_e/international_exp_regs_e.htm

19. Székely, J. Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies. Retrieved from https://real.mtak.hu/210722/1/309-354.pdf

20. Wassenaar Arrangement Secretariat. (2023). List of Dual-Use Goods and Technologies and Munitions List (WA-LIST (23) 1). Retrieved from https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf

21. Bureau of Industry and Security. Multilateral Export Control Regimes. Retrieved from https://www.bis.gov/guidance-frequently-asked-questions/multilateral-export-control-regimes

22. Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 (recast). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32021R0821

23. Bennink, S., Dunin-Wasowicz, J., Zhao, S., & Eshun, S. (2025). EU export controls on dual-use items: Recent developments and emerging trends. *Global Trade and Customs Journal*, 20(2), 89–99. Retrieved from https://kluwerlawonline.com/journalarticle/Global%2BTrade%2Band%2BCustoms%2BJournal/20.2/GTCJ2025011

24. CGO Legal. Strategic Goods — Definition and Trade Obligations. Retrieved from https://cgolegal.com/strategic-goods/

25. SIPRI. The Challenge of Software and Technology Transfers to Non-Proliferation Efforts. Retrieved from https://www.sipri.org/sites/default/files/201804/sipri1804_itt_software_bromley_et_al.pdf

26. SIPRI. The Challenge of Software and Technology Transfers to Non-Proliferation Efforts. Retrieved from https://www.sipri.org/sites/default/files/201804/sipri1804_itt_software_bromley_et_al.pdf

27. Arms Control Association. The Wassenaar Arrangement at a Glance. Retrieved from https://www.armscontrol.org/factsheets/wassenaar

28. Arthur D. Little. Unlocking the Strategic Power of Dual-Use Technologies. Retrieved from https://www.adlittle.com/en/insights/viewpoints/unlocking-strategic-power-dual-use-technologies

29. World Trade Organization (WTO). Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Retrieved from https://www.wto.org/english/res_e/booksp_e/int_exp_regs_part3_5_e.pdf

30. Wassenaar Arrangement. Retrieved from https://en.wikipedia.org/wiki/Wassenaar_Arrangement

31. Wassenaar Arrangement Secretariat. What is the Wassenaar Arrangement? Retrieved from https://www.wassenaar.org/the-wassenaar-arrangement/

ІНФРАСТРУКТУРНА БЕЗПЕКА ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНИХ ІНТЕРЕСІВ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

INFRASTRUCTURE SECURITY AS A COMPONENT OF SAFEGUARDING PUBLIC INTERESTS WITHIN THE NATIONAL SECURITY SYSTEM OF UKRAINE

Dulina O. V.,
PhD in Law, Associate Professor,
Associate Professor of the Department
of Public Administration and Regional Studies,
Institute of Public Service and Administration,
Odesa Polytechnic National University,
Odesa, Ukraine

Abstract. Ensuring the security of critical infrastructure is one of the key areas of modern state policy in the field of national security, since the stability of infrastructure systems determines the ability of the state to provide vital services and functions. In modern conditions of security and technogenic threats, the study of infrastructure security as a component of ensuring the public interests of the state, society and territorial communities in the national security system is of particular importance. **The purpose of** the article is a comprehensive analysis of infrastructure security as a component of the national security of Ukraine, as well as determining the features of the formation and transformation of political and legal mechanisms for its provision.

The logic of the study involves revealing the essence of infrastructure security in the modern national security system, determining the content of public interests in this area, as well as analyzing state policy mechanisms for ensuring the stability and protection of critical infrastructure. **The research methodology** is based on the use of general scientific methods of analysis and synthesis, a systems approach, as well as regulatory and legal analysis. Their application made it possible to generalize scientific approaches to understanding infrastructure security, to investigate the legislative and institutional principles of the functioning of the national critical infrastructure protection system, and to determine the role of public interests in the formation of state policy in this area. **The results of the study** showed that infrastructure security is an important component of the national security system, as it integrates economic, energy, information, defense, environmental and other subsystems of national security and ensures the functioning of society and the country's economy. It is proven that public interests in the field of infrastructure security consist in ensuring the security, stability, adaptability and resiliency of critical infrastructure systems, on which the well-being of the population, economic stability and the effectiveness of public administration depend. The study also substantiates that modern mechanisms for ensuring infrastructure security include strategic planning, regulatory and legal regulation, institutional coordination, public-private partnership, international cooperation and cybersecurity mechanisms. Special attention is paid to the role of the public administration system, since public authorities simultaneously act as subjects of the state critical infrastructure protection system at different levels of management, as well as potential objects of critical infrastructure, in particular due to the need to ensure cybersecurity of management processes and information protection. **The practical significance** lies in the possibility of using the results of the study when improving state policy in the field of critical

infrastructure protection, forming a risk-oriented approach and introducing management innovations in managing the security of infrastructure systems. **Value / originality.** The scientific value of the study lies in the comprehensive consideration of infrastructure security as a mechanism for implementing public interests in the national security system of Ukraine, as well as in substantiating the role of public administration and political and legal mechanisms in ensuring the security and stability of critical infrastructure in the face of modern challenges and threats

Keywords: Infrastructure Security, Public Interests, National Security of Ukraine, Critical Infrastructure, State Security Policy, Protection of Strategic Facilities.

1. Вступ

Сучасний розвиток безпекового середовища характеризується зростанням цифровізації та взаємозалежності інфраструктурних систем, які забезпечують функціонування держави, економіки та суспільства. Енергетична, транспортна, інформаційно-комунікаційна та соціальна інфраструктури, мережі життєзабезпечення, інфраструктура громадської безпеки та цивільного захисту населення і територій забезпечують надання життєво важливих послуг та функцій. У зв'язку з цим можливість відновлення, стійкість до зовнішніх загроз, гнучкість і адаптивність, інтеграція з іншими системами та ефективність управління такими системами набувають стратегічного значення для забезпечення національної безпеки. До основних загроз, що впливають на функціонування критично важливих об'єктів, належать природні та техногенні ризики, загрози, пов'язані зі зміною клімату, гібридні ризики та загрози, ризики терористичних атак, цифрові ризики та кіберзагрози, економічні загрози, а також загрози воєнного часу, які залежно від масштабу та характеру їх наслідків можуть спричиняти значні

соціально-економічні втрати, призводити до дестабілізації системи державного управління та створювати пряму загрозу життю і безпеці населення. Саме тому інфраструктурна безпека розглядається як один із ключових компонентів сучасної системи національної безпеки.

Актуальність дослідження інфраструктурної безпеки особливо зросла в умовах повномасштабної збройної агресії Російської Федерації проти України, коли об'єкти енергетики, транспорту, цифрових комунікацій, житлово-комунального господарства та інших секторів критичної інфраструктури стали безпосередніми цілями військових і диверсійних атак. Військова агресія, терористична діяльність, кібератаки та деструктивні інформаційні впливи значно підвищують вразливість інфраструктурних систем і створюють комплексні ризики для національної безпеки. У таких умовах забезпечення захисту, стійкості та відновлення інфраструктури, та зокрема її критично важливих об'єктів, стає одним із ключових завдань державної безпекової політики.

Важливим аспектом актуальності дослідження є також його нормативно-політичний вимір. У сучасній філософії безпеки, стійкість та динамічна модернізація інфраструктури розглядаються як взаємопов'язані елементи комплексної системи забезпечення національної безпеки, у межах якої фізична захищеність об'єктів поєднується з технологічною, інституційною та управлінською адаптивністю. У цьому контексті **Стратегія національної безпеки України** визначає стійкість (resilience) як базову спроможність держави забезпечувати безперервність функціонування критично важливих систем в умовах турбулентності безпекових викликів та гібридних загроз. Модернізація інфраструктури водночас трактується не лише як технічне оновлення, а як інституційна трансформація відповідно до стандартів НАТО та Європейського Союзу, що спрямована на підвищення координації систем

життєзабезпечення та інтеграцію України до європейського безпекового простору. Подальшу конкретизацію цих підходів забезпечують **стратегічні документи у сфері кібер- та інформаційної безпеки**, які акцентують увагу на необхідності формування кіберстійкості інфраструктурних систем. Йдеться, передусім, про здатність автоматизованих систем управління та цифрових мереж протидіяти деструктивним втручанням, зберігаючи безперервність надання суспільно важливих послуг навіть у разі компрометації окремих елементів системи. У цьому вимірі модернізація передбачає розвиток захищених інформаційних середовищ, диверсифікацію технологічних рішень та створення децентралізованих мереж передачі даних. Водночас сучасна концепція інфраструктурної безпеки дедалі більше інтегрує екологічний та кліматичний виміри, що відображено у **державній політиці екологічної безпеки та адаптації до зміни клімату**. Реалізація принципу *Build Back Better* орієнтує модернізацію інфраструктури на впровадження енергоефективних технологій, розвиток відновлюваної енергетики та децентралізацію енергетичних систем. Такий підхід поєднує екологічну та безпекову складові, підвищуючи стійкість інфраструктури як до воєнних загроз, так і до довгострокових кліматичних ризиків. Водночас забезпечення інфраструктурної безпеки має не лише технічний або управлінський вимір, а й безпосередньо пов'язане з категорією публічного інтересу. Саме через реалізацію публічного інтересу держава виконує свій обов'язок щодо захисту суспільно значущих благ та підтримання соціально-економічної стабільності.

З огляду на зазначене, забезпечення стійкості та модернізації інфраструктури набуває ознак **значущого публічного інтересу**, що зумовлює необхідність формування ефективних правових, організаційних та інституційних механізмів її захисту. Саме комплексність сучасних загроз та стратегічне значення інфраструктурних

систем для життєдіяльності суспільства обумовлюють актуальність наукового осмислення механізмів публічного управління у сфері забезпечення інфраструктурної безпеки.

2. Інфраструктурна безпека у сучасній системі національної безпеки

Інфраструктурну безпеку визначають як стан захищеності інфраструктурних систем, мереж і об'єктів (особливо критичної інфраструктури) від загроз, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість інфраструктури. До таких систем відносять енергетичну, транспортну, інформаційно-комунікаційну, фінансову, комунальну, соціальну та інші види інфраструктури, визначені законодавством як критично важливі. Інфраструктурна безпека виступає важливою складовою системи національної безпеки, оскільки стабільне функціонування інфраструктурних систем забезпечує реалізацію життєво важливих функцій держави, економіки та соціальної сфери. Саме завдяки належному функціонуванню енергетичних, транспортних, інформаційно-комунікаційних та інших інфраструктурних систем створюються умови для сталого розвитку суспільства та підтримання належного рівня життєдіяльності населення.

Водночас трансформація суспільних відносин, зростання масштабів технологічного розвитку та поява нових безпекових викликів, зокрема гібридних загроз, кібернетичних атак і техногенних ризиків, зумовили необхідність переосмислення підходів до організації захисту ключових інфраструктурних систем. Усвідомлення цих змін на рівні державної політики та їх відображення у правовому регулюванні, з урахуванням міжнародного досвіду у сфері захисту критичної інфраструктури, сприяли формуванню нових підходів до визначення об'єктів, що мають стратегічне значення для функціонування держави. Саме у результаті такого еволюційного процесу

в законодавстві та державній політиці поступово сформувалося поняття критичної інфраструктури та були започатковані механізми створення державної системи її захисту.

У цьому контексті критична інфраструктура формується на базі існуючих інфраструктур держави шляхом виокремлення з них систем і активів, що мають життєво важливе значення для функціонування держави та суспільства [1, с. 85]. Вона являє собою системний комплекс стратегічно важливих матеріальних і нематеріальних об'єктів виробничої, невиробничої та соціальної сфер, а також окремих елементів цього комплексу, від стабільності та безперервності функціонування яких залежить забезпечення національної безпеки та суспільної стабільності. Як сукупність об'єктів критична інфраструктура представлена: об'єктами інфраструктури, системами та мережами, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди національним інтересам. А зловмисне втручання у їх функціонування, а також пошкодження, руйнація або виведення з ладу системи або її елементів внаслідок диверсій, техногенних чи природних катастроф, здатне призвести до тяжких наслідків.

Отже, критична інфраструктура — це комплексна система, що складається з об'єктів, систем і ресурсів, життєво важливих для функціонування держави.

Існують різні підходи до визначення інфраструктурної безпеки, однак найбільш поширеним є підхід, відповідно до якого вона розглядається як стан захищеності інфраструктурних систем, мереж і об'єктів від загроз, що забезпечує їх стійке, безперервне та безпечне функціонування. У науковому дискурсі інфраструктурну безпеку також розглядають як окрему складову сектору безпеки й оборони, що інтегрує економічну, енергетичну, інформаційну, оборонну, екологічну та інші підсистеми національної безпеки [2, с. 138]. Через

це реалізація публічних інтересів у сфері інфраструктурної безпеки виступає необхідною умовою досягнення цілей усієї системи національної безпеки — збереження суверенітету, територіальної цілісності, конституційного ладу, прав і свобод людини [3, с. 45].

Державна система захисту критичної інфраструктури являє собою складну соціотехнічну систему, спрямовану на формування та реалізацію державної політики у сфері забезпечення захисту і стійкості критично важливих об'єктів. Її функціонування забезпечується шляхом застосування узгодженого комплексу управлінських, організаційно-правових, наукових, інженерно-технічних, інформаційних, фінансово-економічних та кадрових заходів, що реалізуються уповноваженими суб'єктами.

В українському законодавстві інституційні та правові засади функціонування цієї сфери визначені Законом України «Про критичну інфраструктуру» [4], який встановлює правові та організаційні основи створення та функціонування національної системи захисту критичної інфраструктури. Згідно з положеннями цього закону, захист критичної інфраструктури є складовою забезпечення національної безпеки та передбачає комплекс заходів, спрямованих на запобігання загрозам та забезпечення стійкості інфраструктурних систем. Стратегія національної безпеки України [5] та профільні акти [6] відносять безпеку критичної інфраструктури до пріоритетних завдань держави в контексті захисту національних інтересів від зовнішніх і внутрішніх загроз. Укази Президента [7] та рішення РНБО [8] прямо пов'язують захист інфраструктури з протидією розвідувально-підривній, диверсійній і терористичній діяльності, а також із запобіганням кризовим явищам у сфері енергетики, транспорту, зв'язку тощо.

Відповідно до Закону України «Про критичну інфраструктуру» [4] національна система захисту критичної інфраструктури має багаторівневу структуру. На загальнодержавному рівні

управління здійснюється Кабінетом Міністрів України, Державною службою захисту критичної інфраструктури та забезпечення національної системи стійкості України (утвореною постановою Кабінету Міністрів України від 12 липня 2022 р. № 787 [9]), а в умовах воєнного стану Державною службою спеціального зв'язку та захисту інформації України відповідно до Закону України від 18 жовтня 2022 р. № 2684-IX [10], а також іншими центральними органами виконавчої влади та Національним банком України.

На регіональному та галузевому рівнях управління здійснюється центральними та місцевими органами виконавчої влади. Місцевий рівень представлений органами місцевого самоврядування та місцевими органами виконавчої влади. Об'єктовий рівень охоплює безпосередніх операторів критичної інфраструктури, які забезпечують функціонування та захист конкретних інфраструктурних об'єктів.

Життєво важливі функції та/або послуги, порушення яких призводить до негативних наслідків для національної безпеки України визначені у профільному законі. До них, зокрема належать: урядування та надання найважливіших публічних (адміністративних) послуг, енергозабезпечення; водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека та ін. Безпека цих об'єктів та їх функціонування як у нормальних умовах, так і в умовах надзвичайних ситуацій, таких як воєнний стан, є одним з пріоритетів держави.

Перелік секторів критичної інфраструктури та секторальні органи у сфері захисту критичної інфраструктури затверджено постановою Уряду від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури» [11]. У табл. 1 наведені окремі приклади співвідношення життєво важливих функцій, секторів критичної інфраструктури, об'єктів і послуг критичної інфраструктури.

Таблиця 1 — Життєво важливі функції та сектори критичної інфраструктури

Життєво важливі функції	**Сектор критичної інфраструктури**	**Елементи забезпечення функції / послуги, об'єкти критичної інфраструктури**
Енергозабезпечення	Паливно-енергетичний комплекс	Виробництво та постачання електроенергії, природного газу, нафтопродуктів; мережі передачі та розподілу енергоресурсів; системи технологічного управління роботою об'єктів та мереж тощо
Транспортування	Транспорт	Дороги, центральні вузли перевантажень, вокзали; аеропорти; мости; трубопроводи, канали, фарватери, тунелі, дамби, системи технологічного управління роботою
Водо- та теплопостачання	Мережі життєзабезпечення	Система водопостачання та водовідведення; водозабори, опрацювання стічних вод, системи теплозабезпечення, системи технологічного управління роботою об'єктів та мереж, ресурси питної води тощо
Правопорядок, цивільний захист населення та територій	Громадська безпека та цивільний захист населення і територій	Охорона публічного (громадського) порядку, охорона критичної інфраструктури, реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт
Інформаційні послуги	Цифрові технології	Електронні довірчі послуги та електронна ідентифікація електронні комунікації електронне урядування

Джерело: [12, с. 382]

Аналіз секторів критичної інфраструктури засвідчує їх міжгалузевий характер і ключову роль у забезпеченні базових функцій держави та суспільства.

Суб'єктами національної системи захисту критичної інфраструктури є органи державної влади, сектор безпеки і оборони, регуляторні органи, центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, а також оператори об'єктів критичної

інфраструктури. У табл. 2 наведена систематизація суб'єктів системи державного захисту критичної інфраструктури та головні їх функції.

Таблиця 2 — Суб'єкти, що діють у системі державного захисту критичної інфраструктури

Суб'єкт	Функції
Уповноважений орган у сфері захисту критичної інфраструктури України	Формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури
Функціональні органи у сфері захисту критичної інфраструктури	Органи державної влади, визначені відповідальними за функціонування окремих державних систем захисту та реагування: участь в реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури
Секторальні органи у сфері захисту критичної інфраструктури	Державні органи, визначені відповідальними за захист критичної інфраструктури в окремому секторі критичної інфраструктури: аналіз даних щодо критичної інфраструктури та її функціонування; здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів критичної інфраструктури, формують секторальні переліки, подають інформацію до реєстру
Місцеві органи виконавчої влади та військово-цивільні адміністрації	Затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій; затвердження місцевих планів взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг, планів відновлення функціонування критичної інфраструктури
Оператори критичної інфраструктури	Забезпечення захисту об'єктів критичної інфраструктури, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки; розроблення, виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту.

Джерело: [12, с. 391]

Окремі функції захисту критичної інфраструктури також притаманні системам цивільного захисту, боротьби з тероризмом, кібербезпеки, правоохоронних органів, регулювання енергетики та енергоринку та ін. Таким чином, державна система захисту критичної інфраструктури України має комплексний та багаторівневий характер і спрямована на забезпечення стійкості життєво важливих інфраструктурних систем держави в умовах сучасних безпекових викликів.

Отже, інфраструктурна безпека може бути визначена як комплексний напрям державної політики у сфері національної безпеки, спрямований на захист, забезпечення відновлюваності, стійкості та безперервного функціонування критично важливих систем і об'єктів, а також на реалізацію і захист публічного інтересу держави, суспільства та територіальних громад у збереженні й належному функціонуванні інфраструктурних систем, стабільність яких є необхідною умовою безпеки, сталого розвитку держави та задоволення життєво важливих потреб значної частини населення.

3. Публічні інтереси у сфері інфраструктурної безпеки

Саме поняття «суспільний (публічний) інтерес» та похідні від нього поняття (суспільні потреби, суспільна необхідність, суспільний добробут) широко використовуються у національних та міжнародних актах, а також відповідній судовій практиці. У вітчизняній правовій науці суспільний (публічний) інтерес пропонується визначати як прагнення усього суспільства або переважної його більшості до задоволення благ, як матеріальних, так і нематеріальних, що на противагу особистісному інтересу має неперсоніфікований характер та виникає, змінюється і втрачається в процесі взаємодії людей у суспільних відносинах. Також суспільні та державні інтереси визначають як сформульовані у положеннях чинного законодавства та доктринальних документах правлячих політичних сил

загальні пріоритети держави, які базуються на потребах суспільства, сучасній ідеології, та реалізуються на практиці за допомогою апарату держави [13, с. 14].

На думку М. Бліхара публічний інтерес розглядається як самостійний об'єкт адміністративно-правового захисту, реалізація якого здійснюється через систему спеціальних правових засобів публічного управління. Автор обґрунтовує, що саме адміністративне право забезпечує найбільш ефективні механізми охорони публічного інтересу, оскільки безпосередньо пов'язане з владною діяльністю держави та регулюванням суспільно значущих відносин [14, с. 44]. Такий підхід є концептуально важливим для сфери інфраструктурної безпеки, де захист публічного інтересу неможливий без активної та координуючої ролі держави.

У цьому контексті доцільно звернутися до законодавчого визначення категорії «публічний інтерес». Відповідно до Закону України «Про адміністративну процедуру» [15] публічний інтерес розглядається як інтерес держави, суспільства, територіальної громади, а також інтереси і потреби, що мають значення для великої кількості осіб. Таке визначення підкреслює комплексний характер цієї категорії та її спрямованість на забезпечення суспільно значущих благ і потреб. Попри галузеву специфіку дослідження категорії «публічний інтерес» у межах адміністративного права [16, с. 400] та публічного управління [17, с. 14], її змістовне наповнення має міжгалузевий характер і активно використовується також у доктрині національної безпеки. У сфері національної безпеки національні інтереси України розглядають як сукупність публічних інтересів, що виражають потреби всього суспільства, держави й територіальних громад, а не окремих груп чи приватних осіб [18, с. 407].

Проблематика співвідношення категорій «публічний інтерес» та «національна безпека» посідає важливе місце у сучасному науковому дискурсі, оскільки саме через механізми

реалізації публічних інтересів держава забезпечує стабільність функціонування суспільних інститутів та захист життєво важливих сфер державного і суспільного життя. Як зазначає І. В. Кременовська [19, с. 78], публічний інтерес у сфері управління публічною власністю пов'язаний із необхідністю забезпечення стабільності економічної системи, розвитку стратегічних галузей та захисту суспільно значущих ресурсів, що безпосередньо корелює із завданнями держави щодо забезпечення національної безпеки.

Водночас співвідношення публічного та приватного інтересів у сфері інфраструктурної безпеки є складною та багатоаспектною проблемою. Значна частина об'єктів критичної інфраструктури перебуває у приватній або змішаній формі власності, що зумовлює необхідність узгодження економічних інтересів їх операторів із публічним інтересом у забезпеченні безпеки, стійкості та безперервності надання життєво важливих послуг. У таких умовах саме публічний інтерес виступає правовою та соціальною підставою легітимності державного регулювання і втручання у функціонування та розвиток об'єктів критичної інфраструктури незалежно від форми власності чи організаційно-правового статусу їх операторів.

Органи публічної влади, реалізуючи повноваження від імені держави та суспільства, повинні забезпечувати врахування як загальносуспільних потреб, так і інтересів окремих соціальних груп, життєдіяльність яких безпосередньо залежить від стабільного функціонування критично важливих інфраструктурних систем, зокрема у сферах енергетики, транспорту, зв'язку, водопостачання, охорони здоров'я та інших базових суспільних послуг. Водночас реалізація публічного інтересу у цій сфері має здійснюватися на засадах пропорційності та правового балансу між вимогами безпеки і необхідністю дотримання прав та законних інтересів приватних суб'єктів. Такий баланс є необхідною передумовою ефективного

функціонування системи інфраструктурної безпеки, оскільки забезпечує поєднання публічно-правових механізмів гарантування безпеки з економічною ефективністю діяльності операторів критичної інфраструктури.

Розглядаючи співвідношення категорій «публічний інтерес» і «національна безпека» крізь призму інфраструктурної безпеки, доцільно виходити з того, що публічний інтерес виступає нормативною та ціннісною основою формування державної політики у сфері захисту критичної інфраструктури. Передусім йдеться про забезпечення стійкого та безперервного функціонування енергетичних, транспортних, цифрових і комунальних систем, від яких залежить життєдіяльність населення, стабільність економіки та належне функціонування державних інституцій. У цьому контексті національна безпека постає ширшою категорією, що охоплює систему правових, організаційних та інституційних заходів держави, спрямованих на захист публічних інтересів від внутрішніх і зовнішніх загроз.

Особливої ваги така взаємозалежність набуває в умовах сучасних безпекових викликів, коли об'єкти критичної інфраструктури стають цілями військових, диверсійних і кібернетичних атак. У цьому сенсі забезпечення стійкості критичної інфраструктури є важливим інструментом гарантування публічних інтересів, пов'язаних із доступом до базових життєвих ресурсів, підтриманням соціально-економічної стабільності та безперервністю функціонування систем державного управління.

Отже, категорії «публічний інтерес» і «національна безпека» перебувають у відносинах взаємозумовленості: публічний інтерес визначає стратегічні пріоритети державної політики щодо захисту й розвитку критичної інфраструктури, тоді як національна безпека виступає системою правових та інституційних механізмів реалізації й захисту цих інтересів. У цьому контексті інфраструктурна

безпека є важливою сферою практичної реалізації публічних інтересів держави, суспільства та територіальних громад.

Таким чином, публічний інтерес у сфері інфраструктурної безпеки доцільно визначати як суспільно значущу потребу держави, суспільства та територіальних громад у забезпеченні захищеності, стійкості та безперервного функціонування критичної інфраструктури, реалізація якої здійснюється через систему правових, організаційних та інституційних механізмів національної безпеки України.

Закон України «Про національну безпеку України» [20] закріплює комплексний підхід до забезпечення національної безпеки, який поєднує безпекові, управлінські та правові механізми. У практичному вимірі положення цього закону легітимують активну роль держави у координації діяльності суб'єктів безпеки, запровадженні спеціальних режимів управління та встановленні підвищених вимог до захисту критично важливих систем, що відповідає інноваційному розумінню публічного інтересу як підстави правозастосовних рішень. Такий підхід відображає домінування публічного інтересу як інтересу всього суспільства до стабільності, керованості та захищеності держави, що має безпосередній зв'язок із забезпеченням інфраструктурної безпеки як складової національної безпеки [21, с. 89].

Слід відзначити що, публічний інтерес слугує орієнтиром для діяльності органів публічної влади, визначаючи пріоритети у формуванні політик, у тому числі в секторі безпеки та оборони [22, с. 140]. У сфері інфраструктурної безпеки адміністративні правовідносини, пов'язані з управлінням, контролем і наглядом за об'єктами критичної інфраструктури, мають виразний публічно-управлінський характер і спрямовані на захист колективних потреб суспільства. У цьому контексті публічний інтерес виступає критерієм вибору адміністративно-правових заходів впливу та визначає межі допустимого втручання держави у сферу приватних інтересів. Водночас ступінь його реалізації слугує показником ефективності публічного управління,

оскільки саме забезпечення стабільного, безпечного та безперервного функціонування критичної інфраструктури свідчить про здатність держави належно виконувати свої публічні функції у системі національної безпеки [23, с. 139].

Запровадження міжнародно визнаних механізмів превенції, виявлення та врегулювання конфлікту інтересів забезпечує пріоритет публічного інтересу над приватним у процесах регулювання, управління та відновлення інфраструктурних систем, особливо в умовах війни та підвищених безпекових ризиків, коли прозорість і відповідальність органів влади стають ключовими чинниками стійкості критичної інфраструктури [24, с. 175].

Публічні інтереси у сфері інфраструктурної безпеки це суспільно значущі, гарантовані державою потреби у надійному, безпечному та безперебійному функціонуванні інфраструктурних і насамперед критичних інфраструктурних систем, від яких залежить життєдіяльність населення та стійкість держави. Вони є складовою системи національних інтересів і через це займають самостійне місце в системі національної безпеки України як один із ключових вимірів її забезпечення.

Публічні інтереси у сфері критичної інфраструктури включають вимогу до держави: ідентифікувати об'єкти критичної інфраструктури, створити правові й організаційні механізми їх захисту, забезпечити належний рівень кіберзахисту й фізичної безпеки, впроваджувати стійкі механізми управління ризиками. У фокусі не лише запобігання руйнуванню об'єктів, а й забезпечення їх стійкості та швидкого відновлення після атак чи аварій, що прямо впливає на виживання населення й працездатність економіки в умовах війни.

У сфері інфраструктурної безпеки публічний інтерес має комплексний характер, оскільки поєднує соціальні, економічні та безпекові складові. Соціальний вимір пов'язаний із забезпеченням доступу населення до базових життєво необхідних послуг, зокрема

енергопостачання, водопостачання, транспорту, зв'язку та фінансових сервісів. Економічна складова відображає значення стабільного функціонування інфраструктурних систем для підтримання виробничого потенціалу держави, збереження зайнятості, інвестиційної привабливості та відновлення економіки. Безпековий вимір охоплює захист інфраструктурних об'єктів від воєнних, терористичних, техногенних і кібернетичних загроз, здатних спричинити масштабні порушення функціонування державних інститутів і соціально-економічних процесів.

Водночас реалізація публічного інтересу вимагає його належної пріоритизації у процесі формування та реалізації державної політики у сфері інфраструктурної безпеки. Ключовими критеріями такої пріоритизації є:

— життєзабезпечення, тобто безпосередній вплив інфраструктурного об'єкта або системи на умови життя та безпеку населення;

— критичність, яка визначається рівнем незамінності відповідного інфраструктурного елемента, а також можливістю його оперативного відновлення;

— системні наслідки, що проявляються у масштабі потенційних порушень для інших секторів економіки, системи публічного управління та соціальної стабільності у разі виходу інфраструктурного об'єкта з ладу.

Саме врахування цих критеріїв забезпечує обґрунтоване визначення пріоритетів державної політики та ефективне спрямування ресурсів на захист найбільш значущих елементів критичної інфраструктури.

Аналіз сутності публічного інтересу у сфері інфраструктурної безпеки дає підстави розглядати його не як абстрактну декларативну категорію, а як складне багаторівневе явище, що конкретизується через систему суспільно значущих потреб, цілей та засобів їх правового забезпечення. У цій сфері публічний інтерес об'єктивується

через потребу держави, суспільства і територіальних громад у захищеному, стійкому, доступному та безперервному функціонуванні критично важливих інфраструктурних систем. Такий підхід дозволяє класифікувати публічні інтереси у сфері інфраструктурної безпеки за їх функціональним спрямуванням. Передусім ідеться про інтереси, пов'язані із забезпеченням надійності та безперебійності функціонування інфраструктури, оскільки саме безперервність роботи енергетичних, транспортних, цифрових, комунальних та інших систем є первинною передумовою суспільної стабільності. Наступну групу становлять публічні інтереси, спрямовані на підвищення ефективності та конкурентоспроможності інфраструктури, що охоплюють раціональне управління, оптимізацію функціонування інфраструктурних секторів та забезпечення їх спроможності відповідати сучасним економічним і безпековим викликам. Окрему групу становлять інтереси, пов'язані з модернізацією та розвитком інфраструктури, включно з оновленням об'єктів, впровадженням нових моделей управління та нарощуванням стійкості до кризових впливів. Самостійного значення набувають публічні інтереси у сфері впровадження інноваційних технологій, зокрема цифрових рішень, автоматизованих систем управління, кіберзахисту та технологій резервування. Нарешті, важливе місце посідають інтереси, пов'язані із забезпеченням доступності та якості послуг, тобто гарантованим доступом населення до водопостачання, електроенергії, зв'язку, транспорту та інших базових сервісів належної якості.

Поряд із цим публічні інтереси у сфері інфраструктурної безпеки можуть бути розкриті через ті суспільні блага, які вони матеріалізують. У цьому аспекті вони охоплюють, по-перше, інтереси виживання та суверенітету держави, що виявляються у захисті об'єктів, виведення з ладу яких здатне паралізувати функціонування державного механізму, оборонного сектору та економіки. По-друге, йдеться про інтереси соціальної та гуманітарної безпеки, які реалізуються

через гарантування базових послуг для населення. По-третє, важливого значення набуває цифровий публічний простір, що охоплює кіберзахист об'єктів критичної інфраструктури, інформаційну безпеку та протидію деструктивним інформаційним впливам. По-четверте, у сучасних умовах посилюється значення участі суспільства у забезпеченні інфраструктурної безпеки, що передбачає залучення громадських інституцій, професійних спільнот і територіальних громад до вироблення та реалізації відповідних рішень.

Згідно з класифікацією публічних інтересів, запропонованою Л. О. Золотухіною [25, с. 6] публічні інтереси у сфері інфраструктурної безпеки можуть бути класифіковані за наступними критеріями:

— за суб'єктним складом, інтереси охоплюють інтереси різних носіїв: населення, окремих соціальних груп, територіальних громад, суспільства загалом, держави, а також міжнародної спільноти;

— за територією поширення публічні інтереси у сфері інфраструктурної безпеки можуть мати локальний, регіональний, державний та міжнародний характер; у цьому контексті можна також виокремити внутрішні та зовнішні публічні інтереси, пов'язані відповідно із захистом інфраструктури від внутрішніх і зовнішніх загроз;

— за часом існування у сфері інфраструктурної безпеки виділяють постійні, періодичні, короткострокові та довгострокові публічні інтереси;

— за значенням для носія публічного інтересу інтереси у сфері інфраструктурної безпеки можуть бути фундаментальними та другорядними;

— за сферою реалізації публічні інтереси у сфері інфраструктурної безпеки проявляються у різних галузях суспільного життя, зокрема в енергетичній, транспортній, інформаційно-комунікаційній, комунальній, економічній та оборонній сферах;

— за способом взаємодії носіїв публічного інтересу у сфері інфраструктурної безпеки можна виокремити спільні та взаємні

публічні інтереси. Спільні інтереси виникають у процесі взаємодії держави, органів місцевого самоврядування, суб'єктів господарювання та громадянського суспільства щодо забезпечення належного рівня захисту об'єктів критичної інфраструктури. Взаємні інтереси проявляються у співпраці держави з іншими державами та міжнародними організаціями у сфері забезпечення безпеки транскордонної інфраструктури, енергетичних систем та інформаційно-комунікаційних мереж.

На нашу думку, класифікація публічних інтересів, запропонована Л. О. Золотухіною, дозволяє комплексно охарактеризувати різноманітні прояви публічних інтересів у сфері інфраструктурної безпеки та визначити їх місце у системі забезпечення національної безпеки держави.

Встановлення змісту та різновидів публічних інтересів у цій сфері дає можливість визначити й основні механізми їх охорони. Насамперед такими механізмами є:

— нормативно-правове регулювання, яке закріплює засади державної політики у сфері критичної інфраструктури, визначає статус суб'єктів, правові режими функціонування об'єктів, порядок їх категоризації, планування захисту, відновлення та забезпечення стійкості;

— адміністративний контроль і нагляд, за допомогою яких забезпечується перевірка дотримання обов'язкових вимог безпеки, оцінка ризиків, моніторинг стану критичної інфраструктури та своєчасне реагування на виявлені порушення;

— дозвільні та реєстраційні процедури, які забезпечують ідентифікацію об'єктів критичної інфраструктури, допуск до певних видів діяльності, встановлення спеціальних режимів функціонування та запровадження вимог до операторів;

— заходи адміністративного примусу та юридичної відповідальності, що покликані забезпечити виконання встановлених

правил, запобігти порушенням і мінімізувати наслідки загроз для суспільства та держави.

Водночас зазначені механізми набувають практичного змісту лише через відповідні адміністративно-правові інструменти реалізації публічного інтересу. До таких інструментів належать нормативні приписи, процедури категоризації та реєстрації об'єктів, інспектування, ліцензування, сертифікація, приписи про усунення порушень, адміністративні обмеження, санкції, заходи реагування у кризових ситуаціях, а також інструменти міжвідомчої координації та публічно-приватної взаємодії. Саме через цю систему інструментів публічний інтерес переходить із площини доктринального осмислення у площину практичної управлінської діяльності.

Узагальнюючи результати дослідження, слід зазначити, що публічний інтерес у сфері інфраструктурної безпеки виступає фундаментальною категорією, яка відображає суспільно значущу потребу держави, суспільства та територіальних громад у надійному, безпечному і безперебійному функціонуванні інфраструктурних, передусім критичних, систем. Через ці системи забезпечуються базові умови життєдіяльності населення, стабільність економічних процесів та безперервність функціонування державних інституцій, що зумовлює особливе значення відповідного інтересу у системі національної безпеки України.

4. Трансформація механізмів політико-правового забезпечення інфраструктурної безпеки

Механізми політико-правового забезпечення інфраструктурної безпеки України це сукупність інструментів державної політики та норм права, через які держава формує цілі, розподіляє повноваження, встановлює вимоги до суб'єктів критичної інфраструктури і забезпечує їх виконання. Вони охоплюють конституційні норми, спеціальні закони, підзаконні акти, інституційні

структури, процедури планування, нагляду, реагування та відповідальності у сфері інфраструктурної безпеки та безпеки критичної інфраструктури [26, с. 176]. До політико-правових механізмів інфраструктурної безпеки належить також система стратегій та процедур взаємодії держави, приватного сектору й міжнародних партнерів, спрямована на стійкість і захист критичної інфраструктури.

У цьому контексті доцільно виділити та охарактеризувати основні механізми політико-правового забезпечення інфраструктурної безпеки, серед яких особливе значення мають механізми стратегічного планування, регулятивно-правового регулювання, інституційної координації, публічно-приватного партнерства, міжнародно-правової співпраці, кримінально-правового реагування, а також механізми забезпечення кібер- та інформаційної безпеки. Розгляд їх змісту та особливостей функціонування дозволяє більш комплексно оцінити потенціал державної політики у сфері забезпечення стійкості критичної інфраструктури.

Механізм стратегічного планування у сфері інфраструктурної безпеки передбачає формування довгострокових державних стратегій, програм і планів дій, спрямованих на забезпечення стійкості критичної інфраструктури. Його основою є стратегічні документи державної політики, зокрема Стратегія національної безпеки України, Стратегія кібербезпеки, державні програми розвитку інфраструктури, а також Національний план захисту та забезпечення безпеки і стійкості критичної інфраструктури. Важливою складовою цього механізму є застосування ризик-орієнтованого підходу, який передбачає системний аналіз загроз і планування заходів щодо їх запобігання, а також використання програмно-цільового бюджетування для фінансування заходів із забезпечення безпеки інфраструктурних об'єктів. Напрями трансформації цього механізму пов'язані передусім із переходом від реактивної моделі управління до превентивної та адаптивної моделі. Це передбачає інтеграцію стратегічного

планування із системами управління ризиками, використання аналітики великих даних для прогнозування загроз, а також впровадження підходів стратегічної резильєнтності [27, с. 234].

Слід зазначити, що включення питань інфраструктурної безпеки до стратегій сталого розвитку свідчить про перехід від фрагментарних галузевих рішень до комплексної моделі публічної політики, зорієнтованої на збереження функціональної спроможності держави в умовах довготривалих ризиків. У цьому контексті публічний інтерес набуває «довгої рамки», в межах якої критеріями ефективності стають не лише поточні показники безпеки, а й здатність інфраструктурних систем до адаптації, відновлення та розвитку [28, с. 180].

Регулятивно-правовий механізм включає систему нормативно-правових актів, які визначають правові засади функціонування та захисту критичної інфраструктури. Центральне місце у цій системі займає Закон України «Про критичну інфраструктуру», а також законодавство у сфері кібербезпеки, енергетики, транспорту, телекомунікацій, цивільного захисту та інших секторів, що формують інфраструктурний комплекс держави. Цей механізм встановлює правові вимоги до суб'єктів критичної інфраструктури, визначає процедури ідентифікації об'єктів критичної інфраструктури, порядок оцінки ризиків, планування заходів безпеки, реагування на інциденти та обміну інформацією між суб'єктами системи захисту. Удосконалення регулятивно-правового механізму відбувається шляхом гармонізації українського законодавства із правом Європейського Союзу, зокрема з директивами NIS2 та CER, а також із міжнародними стандартами у сфері управління безпекою. Важливими напрямами трансформації є посилення процедур нагляду, контролю та юридичної відповідальності за порушення вимог захисту критичної інфраструктури [29, с. 74].

Інституційний механізм забезпечення інфраструктурної безпеки полягає у функціонуванні системи органів державної влади

та інших суб'єктів, які здійснюють управління, координацію та контроль у цій сфері. До таких суб'єктів належать органи сектору безпеки і оборони, центральні органи виконавчої влади, Служба безпеки України, спеціалізовані органи у сфері кібербезпеки, а також органи місцевого самоврядування та оператори критичної інфраструктури. Важливим елементом цього механізму є розмежування повноважень між суб'єктами системи забезпечення інфраструктурної безпеки та створення координаційних органів, які забезпечують узгодженість їх діяльності. Модернізація інституційного механізму спрямована на підвищення ефективності міжвідомчої взаємодії, створення інтегрованих систем управління безпекою інфраструктури, а також розвиток мережевих моделей координації між державними, регіональними та місцевими інституціями. Особливого значення набуває розвиток міжсекторальної співпраці та інтеграція державних і приватних суб'єктів у єдину систему управління інфраструктурною безпекою [30, с. 50].

Публічно-приватне партнерство у сфері інфраструктурної безпеки передбачає залучення приватних операторів критичної інфраструктури, бізнес-структур та громадянського суспільства до планування та реалізації заходів із забезпечення безпеки. Значна частина об'єктів критичної інфраструктури перебуває у приватній або змішаній формі власності, що обумовлює необхідність тісної співпраці держави та бізнесу у сфері управління ризиками, обміну інформацією про загрози та реалізації інвестиційних проєктів із модернізації інфраструктури. Розбудова цього механізму полягає у розвитку нових моделей співпраці держави та приватного сектору, зокрема у сфері кібербезпеки, цифрової інфраструктури та інноваційних технологій. Важливим напрямом є створення спільних платформ обміну інформацією про загрози, розвиток інноваційних екосистем безпеки та залучення приватного сектору до формування державної політики у сфері інфраструктурної безпеки [31, с. 8].

Міжнародно-правовий механізм забезпечення інфраструктурної безпеки пов'язаний із інтеграцією України у глобальну систему безпеки та гармонізацією національного законодавства з міжнародними стандартами. Він включає співпрацю з Європейським Союзом, НАТО, міжнародними організаціями та партнерами у сфері кібербезпеки та захисту критичної інфраструктури. Важливими елементами цього механізму є участь у міжнародних програмах і навчаннях, обмін інформацією про загрози, а також впровадження міжнародних стандартів управління безпекою, зокрема стандартів ISO та NIST. Еволюція міжнародно-правового механізму полягає у поглибленні інтеграції України до європейського безпекового простору, адаптації національної системи захисту критичної інфраструктури до стандартів ЄС і НАТО, а також розвитку міжнародної кооперації у сфері кібербезпеки, боротьби з тероризмом та протидії гібридним загрозам [32, с. 460].

Кримінально-правовий механізм забезпечення інфраструктурної безпеки передбачає встановлення юридичної відповідальності за посягання на об'єкти критичної інфраструктури, включаючи диверсії, терористичні акти, кіберзлочини та фінансування тероризму. Він охоплює систему кримінально-правових норм, діяльність правоохоронних органів та спеціальних служб, спрямовану на запобігання, виявлення і припинення злочинів, які становлять загрозу для функціонування критично важливих інфраструктурних систем [33, с. 55].

Трансформація цього механізму пов'язана з адаптацією кримінального законодавства до нових форм загроз, зокрема кіберзлочинності, гібридних атак і диверсій проти інфраструктурних об'єктів. Важливим напрямом є посилення міжнародної співпраці у сфері боротьби з кіберзлочинністю та тероризмом, а також впровадження сучасних технологій у діяльність правоохоронних органів.

Гендерно-правовий механізм передбачає інтеграцію принципів гендерної рівності у політику забезпечення інфраструктурної

безпеки. Його зміст полягає у врахуванні гендерних аспектів під час формування державної політики, планування заходів безпеки та функціонування інфраструктурних систем [34, с. 133]. Це включає забезпечення рівного доступу жінок і чоловіків до участі у процесах прийняття рішень, усунення дискримінаційних бар'єрів у сфері управління безпекою, а також врахування потреб різних соціальних груп під час реагування на кризові ситуації. Розвиток механізму пов'язаний з інтеграцією гендерних підходів у систему управління національною безпекою, розвитком гендерно чутливих політик у сфері цивільного захисту та інфраструктурної безпеки, а також імплементацією міжнародних стандартів гендерної рівності у державне управління [35, с. 44].

Важливим напрямом трансформації політико-правових механізмів забезпечення інфраструктурної безпеки є впровадження інноваційних методів публічного управління. Серед таких методів особливого значення набувають аутсорсинг, який передбачає передачу окремих функцій із забезпечення кібербезпеки спеціалізованим зовнішнім структурам; реінжиніринг управлінських і бізнес-процесів, спрямований на оптимізацію та цифровізацію управлінських процедур; бенчмаркінг, що полягає у використанні кращих міжнародних практик у сфері кібербезпеки; а також краудсорсинг, який передбачає залучення експертної спільноти та громадськості до формування управлінських рішень. У контексті інфраструктурної безпеки значного значення набувають і такі інноваційні підходи як кластеризація, який передбачає інтеграцію зусиль держави, бізнесу та наукових установ у забезпеченні стійкості інфраструктурних систем та форсайт-методи, спрямовані на прогнозування майбутніх ризиків і формування сценаріїв розвитку безпекового середовища [36, с. 202].

Аналіз основних механізмів політико-правового забезпечення інфраструктурної безпеки дозволяє виокремити кілька стратегічних напрямів їх трансформації, а саме:

— перехід від реактивної моделі забезпечення безпеки до превентивної та ризик-орієнтованої, що передбачає системне управління загрозами та підвищення стійкості інфраструктурних систем;

— цифровізація механізмів управління безпекою, яка включає впровадження сучасних інформаційних технологій, автоматизованих систем моніторингу та цифрових платформ координації між суб'єктами системи захисту критичної інфраструктури;

— інституційна інтеграція державних і недержавних суб'єктів, що передбачає розвиток моделей публічно-приватного партнерства та мережевих форм управління [37, с. 70];

— гармонізація національного законодавства із міжнародними стандартами та правом Європейського Союзу, що сприяє інтеграції України до європейського та євроатлантичного безпекового простору [38, с. 9];

— адаптація до гібридних загроз через мережеве управління й міжнародну кооперацію, що передбачає поєднання правових, технологічних, економічних та соціальних інструментів забезпечення безпеки [39, с. 350].

Визначені напрями трансформації механізмів політико-правового забезпечення інфраструктурної безпеки відображають загальну тенденцію модернізації системи національної безпеки України в умовах зростання комплексних загроз та посилення міжсекторальної взаємозалежності інфраструктурних систем. Проте сама наявність трансформаційних змін у нормативно-правовій, інституційній чи управлінській площині не гарантує належного рівня безпеки критичної інфраструктури. Ефективність функціонування таких механізмів визначається не лише їх формальним закріпленням у законодавстві або стратегічних документах, а й здатністю забезпечувати реальну стійкість інфраструктурних систем до сучасних ризиків і загроз.

У цьому контексті особливої актуальності набуває аналіз чинників, які обумовлюють ефективність політико-правових механізмів у системі національної безпеки. Зокрема, результати наукових досліджень свідчать, що результативність таких механізмів залежить від рівня узгодженості нормативно-правової бази, ефективності інституційної координації суб'єктів управління, інтеграції стратегічного планування з управлінням ризиками, а також забезпечення прозорості, підзвітності та відповідальності у процесах прийняття управлінських рішень. Саме ці чинники формують інституційну та правову спроможність держави забезпечувати стабільне функціонування критично важливих інфраструктурних систем.

Однією з ключових умов ефективності політико-правових механізмів є системність правового регулювання. Йдеться про узгодженість стратегічних документів, законодавства та підзаконних актів, що регламентують функціонування різних секторів безпеки. Ефективна політико-правова система повинна забезпечувати інтеграцію інфраструктурної безпеки у загальну архітектуру національної безпеки та сталого розвитку. Відсутність узгодженості між нормативними актами або фрагментарність правового регулювання може призводити до дублювання функцій органів влади, зниження керованості системи та виникнення прогалин у сфері захисту критичної інфраструктури. У контексті трансформації механізмів політико-правового забезпечення інфраструктурної безпеки це зумовлює необхідність формування цілісної нормативної бази, яка поєднує стратегічні, галузеві та безпекові політики.

Ефективність політико-правових механізмів значною мірою залежить від узгодженості інституційної системи управління безпекою. Важливим чинником є чітке розмежування повноважень між органами державної влади, а також наявність механізмів координації між різними суб'єктами системи національної безпеки. Трансформація механізмів політико-правового забезпечення у цьому

напрямі передбачає формування інтегрованої системи управління інфраструктурною безпекою, заснованої на принципах мережевої взаємодії та міжвідомчої координації.

Ефективність політико-правових механізмів значною мірою визначається їх орієнтацією на довгострокові цілі сталого розвитку. Інфраструктурна безпека виступає матеріальною основою реалізації стратегій сталого розвитку, оскільки саме стабільність функціонування енергетичних, транспортних, інформаційних та комунікаційних систем забезпечує економічну та соціальну. Важливим фактором ефективності політико-правових механізмів є застосування ризик-орієнтованого підходу до управління безпекою. Ще одним важливим фактором ефективності політико-правових механізмів є наявність ефективних механізмів підзвітності та контролю за діяльністю суб'єктів забезпечення безпеки [40, с. 8].

Одним із важливих чинників ефективності механізмів політико-правового забезпечення інфраструктурної безпеки в сучасних умовах є формування та розвиток безпечного цифрового публічного простору. Цифровий публічний простір охоплює сукупність інформаційних ресурсів, електронних сервісів, цифрових платформ та комунікаційних мереж, через які здійснюється взаємодія між органами державної влади, суб'єктами господарювання, операторами критичної інфраструктури та громадянами. У контексті забезпечення інфраструктурної безпеки ефективність політико-правових механізмів значною мірою залежить від здатності держави забезпечити належний рівень кіберзахисту об'єктів критичної інфраструктури, стабільність функціонування інформаційно-комунікаційних систем та захист інформаційного середовища від деструктивних впливів.

Цифровізація державного управління та інфраструктурних систем зумовлює необхідність посилення правових і організаційних механізмів кібербезпеки об'єктів критичної інфраструктури.

Це передбачає впровадження сучасних систем моніторингу кіберзагроз, створення механізмів обміну інформацією про інциденти кібербезпеки між суб'єктами національної системи захисту критичної інфраструктури, а також формування єдиних стандартів захисту інформаційних систем, що забезпечують функціонування інфраструктурних об'єктів.

Цифрові технології відіграють ключову роль у забезпеченні ефективного управління різними секторами критичної інфраструктури, зокрема енергетикою, транспортом, телекомунікаціями, системами водопостачання, охороною здоров'я та фінансовим сектором. Використання інтернету речей (IoT), штучного інтелекту, технологій Smart City, аналітики великих даних і сучасних засобів кібербезпеки сприяє підвищенню ефективності управління інфраструктурними об'єктами, їх стійкості та рівня захищеності. Автоматизовані системи моніторингу та управління дозволяють здійснювати прогнозування можливих аварійних ситуацій, оперативно реагувати на загрози та забезпечувати безперервне функціонування критично важливих сервісів. Водночас використання технологій блокчейну підвищує надійність цифрових транзакцій, зокрема у фінансовому секторі, що також сприяє зміцненню інфраструктурної безпеки [36, с. 202].

У ході дослідження встановлено, що трансформація політико-правових механізмів забезпечення інфраструктурної безпеки є відповіддю на зростання системних ризиків, пов'язаних із цифровізацією, міжсекторальною взаємозалежністю та воєнними загрозами. Сучасні механізми публічного управління у цій сфері еволюціонують від фрагментарного та реактивного підходу до комплексної, ризик-орієнтованої моделі, яка поєднує нормативно-правове регулювання, стратегічне планування, інституційну координацію та фінансово-контрольні інструменти.

5. Система державного управління як об'єкт критичної інфраструктури

З позицій системного підходу система державного управління може розглядатися як своєрідна метаінфраструктура, що забезпечує координацію, регулювання та узгоджене функціонування різних секторів критичної інфраструктури держави. Саме через механізми публічного управління здійснюється стратегічне планування, ресурсне забезпечення, нормативно-правове регулювання та організаційна координація діяльності енергетичних, фінансових, оборонних, соціальних та інших інфраструктурних систем. Відтак порушення стабільності функціонування системи державного управління може спричиняти каскадні негативні наслідки для інших секторів критичної інфраструктури. У цьому сенсі система публічного управління виступає не лише суб'єктом, а й самостійним об'єктом критичної інфраструктури, безпека і стійкість якого мають публічно значущий характер.

Як обґрунтовують Дзяна Г. О. та Дзяний Р. Б. [41, с. 375], ключовим критерієм віднесення системи публічного управління до критичної інфраструктури є кібербезпека та захист інформації, оскільки цифрові управлінські системи, державні реєстри, електронні сервіси та інформаційно-аналітичні платформи забезпечують реалізацію суспільно значущих функцій держави. Порушення їх функціонування внаслідок кібератак або втрати даних безпосередньо зачіпає публічний інтерес, оскільки може призвести до паралічу управлінських процесів, збоїв у наданні адміністративних і соціальних послуг, втрати довіри громадян до державних інститутів та унеможливлення ефективного кризового управління. Таким чином, публічний інтерес у цьому випадку полягає у гарантуванні безперервності, надійності та захищеності управлінської інфраструктури як передумови реалізації інших публічних інтересів.

Розширюючи класичне розуміння секторальної структури критичної інфраструктури, А. Л. Помаза-Пономаренко та Д. В. Тарадуда також акцентують увагу на секторі державного управління як на самостійному елементі критичної інфраструктури. На думку авторів, система надання публічних та адміністративних послуг виконує ключову функцію забезпечення соціальної стійкості, правопорядку та керованості держави, а отже прямо пов'язана з реалізацією публічних інтересів у сфері безпеки. В умовах війни навмисні атаки на енергетичну, транспортну, соціальну та іншу інфраструктуру поєднуються з підривом управлінських і сервісних спроможностей держави, що посилює значення безперервності публічних послуг як інфраструктурного пріоритету [42, с. 67].

Зокрема, збої у функціонуванні державного казначейства або бюджетної системи можуть безпосередньо впливати на фінансування оборонних програм, забезпечення соціальних виплат, діяльність медичних установ та реалізацію інших життєво важливих функцій держави. Подібним чином втручання у роботу державних електронних реєстрів або систем електронної взаємодії органів влади здатне поставити під сумнів легітимність прав власності, адміністративних рішень, юридичних статусів та інших ключових елементів правового порядку.

У зв'язку з цим доцільним є застосування концептуальної моделі, відповідно до якої система державного управління розглядається як системоутворюючий кластер об'єктів критичної інфраструктури. У межах такої моделі окремі управлінські підсистеми можуть бути ідентифіковані як об'єкти критичної інфраструктури на основі низки критеріїв, серед яких: масштаб впливу на суспільство та державні процеси, рівень функціональної незамінності, тривалість відновлення після порушення функціонування, а також ступінь залежності від інформаційно-комунікаційних технологій.

Особливо високим рівнем критичності характеризуються державні реєстри, інформаційні системи електронної взаємодії органів

влади та цифрові платформи надання адміністративних послуг, оскільки вони забезпечують реалізацію базових функцій урядування, підтримку правових відносин та доступ громадян до державних сервісів. Відповідно система державного управління може бути віднесена до об'єктів критичної інфраструктури з огляду на потенційні масштаби негативних наслідків у разі порушення функціонування її управлінських та інформаційних систем, зокрема внаслідок кібератак чи інших деструктивних впливів.

Оцінювання критичності окремих управлінських підсистем доцільно здійснювати за комплексом показників, серед яких ключове значення мають: масштаб впливу, що характеризує кількість суб'єктів, на яких може позначитися порушення функціонування системи; каскадний ефект, який відображає рівень взаємозалежності управлінської підсистеми з іншими секторами критичної інфраструктури; рівень кіберзалежності, що визначає ступінь залежності функціонування системи від інформаційно-комунікаційних технологій; а також інституційна незамінність, яка характеризує можливість альтернативного виконання відповідних функцій іншими суб'єктами.

Водночас в умовах повномасштабної збройної агресії проти України оцінювання критичності управлінських підсистем не може обмежуватися лише функціональними або кібербезпековими параметрами. Важливим елементом такого оцінювання має бути територіальний контекст функціонування органів публічної влади, оскільки рівень загроз, інтенсивність деструктивних впливів та стійкість управлінських процесів значною мірою залежать від статусу відповідної території.

З огляду на це доцільно враховувати територіальну диференціацію, визначену постановою Кабінету Міністрів України від 6 грудня 2022 р. № 1364 [43], яка встановлює категорії територій залежно від характеру безпекової ситуації. Зокрема, на територіях

активних або потенційних бойових дій підвищується ризик фізичного ураження органів влади, руйнування інфраструктури та втрати комунікацій. На територіях, де відбувалися бойові дії або які були деокуповані, особливого значення набуває інституційна присутність держави, необхідна для відновлення легітимності публічної влади, реєстрації прав, здійснення соціальних виплат та координації процесів відбудови. Водночас на тимчасово окупованих територіях ключову роль відіграють дистанційні механізми управління, зокрема екстериторіальні адміністративні процедури, електронні сервіси та мобільні центри надання адміністративних послуг. Прикордонні регіони, у свою чергу, характеризуються підвищеною диверсійною та інформаційною активністю, що потребує посилення кіберзахисту та організаційної стійкості органів публічної влади.

Таким чином, територіальний чинник доцільно інтегрувати до методики оцінювання критичності управлінських підсистем як додатковий коригуючий показник, який дозволяє більш адекватно враховувати безпекові ризики та особливості функціонування системи державного управління у різних регіонах держави.

Отже, системний аналіз ролі публічного управління у забезпеченні інфраструктурної безпеки дає підстави стверджувати, що система державного управління має всі ключові характеристики об'єкта критичної інфраструктури. Вона забезпечує реалізацію базових функцій держави, характеризується високим рівнем кіберзалежності, має значний каскадний вплив на інші сектори критичної інфраструктури та фактично не має повноцінних альтернативних механізмів заміщення. Інституціоналізація такого підходу сприятиме підвищенню стійкості управлінських процесів, посиленню захисту державних інформаційних систем та зміцненню національної безпеки України в умовах сучасних безпекових викликів.

6. Висновки

1. У результаті проведеного дослідження встановлено, що інфраструктурна безпека виступає важливою складовою системи національної безпеки України, оскільки забезпечує безперебійне функціонування життєво важливих інфраструктурних систем, від яких залежить життєдіяльність населення, сталий розвиток територій та ефективність публічного управління. У сучасних умовах зростання комплексних загроз, зокрема воєнних, техногенних, кіберзагроз та кліматичних ризиків, інфраструктурна безпека набуває стратегічного значення для забезпечення публічних інтересів держави, суспільства та територіальних громад. Доведено, що інфраструктурна безпека має комплексний та міжгалузевий характер, інтегруючи економічну, енергетичну, інформаційну, оборонну, екологічну та інші підсистеми національної безпеки. Інфраструктурна безпека як комплексний напрям державної політики у сфері національної безпеки передбачає формування та розвиток державної системи захисту критичної інфраструктури, у межах якої визначено об'єкти захисту, встановлено рівні підтримання безпеки критично важливих об'єктів, а також визначено суміжні системи, діяльність яких пов'язана із забезпеченням їх захисту, стійкості та безперервного функціонування.

2. Узагальнюючи результати дослідження, слід зазначити, що публічний інтерес у сфері інфраструктурної безпеки виступає фундаментальною інноваційною категорією, що поєднує доктрину й практику правозастосування та легітимує активну роль держави. Публічний інтерес у сфері інфраструктурної безпеки це відображення суспільно значущої потреби держави, суспільства та територіальних громад у надійному, безпечному і безперебійному функціонуванні інфраструктурних, передусім критичних, систем. Проведений аналіз дає підстави стверджувати, що публічний інтерес у цій сфері має складний і багатовимірний характер, поєднуючи

соціальні, економічні та безпекові аспекти функціонування інфраструктури. Зазначена комплексність зумовлює необхідність системного врахування у державній політиці та правовому регулюванні, оскільки інфраструктурна безпека забезпечує не лише стабільність окремих галузей, а й загальну стійкість суспільства та держави до сучасних викликів і загроз.

Як вираз загального блага, публічний інтерес виступає базовим критерієм оцінки ризиків, зумовлює пріоритет захисту об'єктів критичної інфраструктури над приватними інтересами господарюючих суб'єктів за умови дотримання принципів законності, пропорційності та обґрунтованості. Публічний інтерес виступає ключовим критерієм та ціннісною основою побудови державної політики у сфері інфраструктурної безпеки, а його належне забезпечення є показником ефективності публічного управління та необхідною умовою стійкості національної безпеки України. Матеріальною основою публічного інтересу у сфері інфраструктурної безпеки є об'єкти та системи критичної інфраструктури, які і забезпечують життєдіяльність населення.

Аналіз сутності публічного інтересу у сфері інфраструктурної безпеки дав змогу визначити такі його характеристики:

— по-перше, класифікувати його за основними функціональними та ціннісними вимірами, зокрема за суб'єктним складом, територією поширення, часом існування, значенням для носія інтересу, сферою реалізації та способом взаємодії носіїв публічного інтересу;

— по-друге, визначити ключові механізми його охорони, якими є нормативно-правове регулювання, адміністративний контроль і нагляд, дозвільні та реєстраційні процедури, а також заходи адміністративного примусу та юридичної відповідальності;

— по-третє, окреслити адміністративно-правові інструменти його реалізації до яких належать нормативні приписи, процедури категоризації та реєстрації об'єктів, інспектування, ліцензування,

сертифікація, приписи про усунення порушень, адміністративні обмеження, санкції, заходи реагування у кризових ситуаціях, а також інструменти міжвідомчої координації та публічно-приватної взаємодії.

У зв'язку з обмеженістю ресурсів і різним рівнем значущості інфраструктурних об'єктів важливого значення набуває також визначення пріоритетів реалізації публічного інтересу, що забезпечує спрямування управлінських зусиль на захист тих елементів інфраструктури, від функціонування яких залежить стабільність держави та безпека суспільства. Основними напрямами пріоритезації є забезпечення життєзабезпечення населення, визначення критичності інфраструктурних об'єктів та врахування можливих системних наслідків їхнього виходу з ладу.

Інтереси держави та суспільства у безперебійному функціонуванні життєво важливих систем трансформуються у конкретні адміністративні правовідносини, в межах яких органи публічної влади реалізують владно-управлінські повноваження, запроваджуючи спеціальні режими управління, міжсекторну координацію, стандарти безпеки та превентивні заходи захисту критичної інфраструктури. Активна роль держави у сфері інфраструктурної безпеки є об'єктивно зумовленою також сучасними глобальними викликами, пов'язаними з імплементацією концепції сталого розвитку суспільства та євроінтеграційними прагненнями України.

Таким чином, публічні інтереси у сфері інфраструктурної безпеки становлять важливий концептуальний і практичний орієнтир формування державної політики у сфері національної безпеки, оскільки саме через їх реалізацію забезпечується стійкість інфраструктурних систем, безперервність суспільно значущих процесів і здатність держави ефективно реагувати на сучасні безпекові виклики.

3. Аналіз сучасних наукових досліджень підтвердив, що реалізація публічних інтересів у сфері інфраструктурної безпеки

відбувається через систему взаємопов'язаних політико-правових та управлінських механізмів, спрямованих на забезпечення національної стійкості в парадигмі сталого розвитку. Інфраструктурна безпека у цьому контексті постає не лише об'єктом захисту, а й активним інструментом стратегічного програмування розвитку, що забезпечує узгодження безпекових, соціальних та економічних пріоритетів держави. Встановлено, що сучасні механізми забезпечення інфраструктурної безпеки включають стратегічне планування, нормативно-правове регулювання, інституційну координацію, публічно-приватне партнерство, міжнародно-правову співпрацю, механізми кібербезпеки та кримінально-правового реагування. Їх комплексне застосування спрямоване на підвищення стійкості критичної інфраструктури та запобігання негативним наслідкам кризових ситуацій. Доведено, що важливим напрямом розвитку системи інфраструктурної безпеки є трансформація політико-правових механізмів її забезпечення, яка передбачає перехід від реактивної до превентивної та ризик-орієнтованої моделі управління безпекою, цифровізацію механізмів управління, інтеграцію державних і недержавних суб'єктів у межах моделей публічно-приватного партнерства, а також гармонізацію національного законодавства із міжнародними стандартами та правом Європейського Союзу.

Аналіз ефективності політико-правових механізмів у системі національної безпеки дозволяє зробити висновок, що результативність функціонування механізмів забезпечення інфраструктурної безпеки обумовлюється кількома взаємопов'язаними чинниками: системністю нормативно-правового регулювання, інституційною узгодженістю суб'єктів управління, стратегічною орієнтацією на принципи сталого розвитку, застосуванням ризик-орієнтованого підходу та наявністю ефективних механізмів підзвітності і правової відповідальності. Сукупність цих факторів визначає здатність держави формувати комплексну та адаптивну

модель політико-правового забезпечення інфраструктурної безпеки, що відповідає сучасним викликам і загрозам у сфері національної безпеки.

1. Встановлено, що система органів публічного управління займає центральне місце у забезпеченні інфраструктурної безпеки держави. Її функціонування безпосередньо пов'язане з реалізацією ключових функцій держави, координацією діяльності суб'єктів системи захисту критичної інфраструктури та формуванням державної політики у сфері її захисту. Водночас доведено дуальний характер ролі органів публічної влади у сфері інфраструктурної безпеки, які одночасно виступають як суб'єкти державної системи захисту критичної інфраструктури, так і її потенційні об'єкти, насамперед у частині забезпечення захисту інформації та кібербезпеки. Обґрунтовано, що сучасні умови цифровізації управлінських процесів, зростання рівня кіберзагроз та значний каскадний вплив можливих порушень діяльності органів публічної влади на інші сектори критичної інфраструктури зумовлюють необхідність розглядати органи публічної влади як важливі об'єкти критичної інфраструктури, що забезпечують надання життєво важливих послуг у сфері урядування та надання найважливіших публічних (адміністративних) послуг.

Список використаних джерел:

1. Затонацький Д. А. Критична інфраструктура в структурі економічної безпеки держави. *Фінанси України*. 2025. № 6. С. 83–100. DOI: https://doi.org/10.33763/finukr2025.06.083.

2. Миколайчук М. М., Попов М. П., Тодорова О. Л. Інфраструктурна безпека як складова системи національної безпеки: поняття, сутність, основні підходи. *Наукові перспективи*. 2023. № 3 (33). С. 131–143. DOI: https://doi.org/10.52058/2708-7530-2023-3(33)-131-143.

3. Герасименко О. М., Критична інфраструктура України як предмет наукового пізнання: теоретичний аспект. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2024. Випуск 85. Частина 4. С. 42–49. DOI: https://doi.org/10.24144/2307-3322.2024.85.4.6.

4. Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 07.03.2026).

5. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України від 16.02.2022 № 56/2022 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення: 07.03.2026).

6. Концепція створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 06.12 2017 р. № 1009-р / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 07.03.2026).

7. Концепція забезпечення національної системи стійкості : Указ Президента України від 27.03.2021 р. № 479/2019 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/479/2021?find=1&text=%D1%96%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82#w1_1 (дата звернення: 07.03.2026).

8. Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» : Указ Президента України від 17 жовтня 2023 року № 695/2023 /Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/695/2023#Text (дата звернення: 07.03.2026).

9. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : Постанова Кабінету Міністрів України від 12 липня 2022 р. № 787 /

Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (дата звернення: 07.03.2026).

10. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України : Закон України від 18 жовтня 2022 року № 2684-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text (дата звернення: 07.03.2026).

11. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 07.03.2026).

12. Національна безпека : навчальний посібник. М. М. Іжа, М. М. Миколайчук, М. П. Попов та ін. ; Нац. ун-т «Одеська політехніка». Одеса, 2025. 1005 с.

13. Bernazyuk Y. The concept of public (public) interest in administrative judiciary. *Visegrad Journal on Human Rights*. 2021. № 6. С. 11–16. URL: https://journal-vjhr.sk/wp-content/uploads/2022/02/VJRHR_6_2021_Last.pdf (дата звернення: 07.03.2026).

14. Бліхар М. Адміністративно-правові засоби захисту публічного інтересу. *Юридичний вісник*. 2021. № 3. С. 41–48. DOI: https://doi.org/10.32837/yuv.v0i3.2183.

15. Про адміністративну процедуру : Закон України від 17 лютого 2022 р. № 2073-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2073-20#Text (дата звернення: 07.03.2026).

16. Мельниченко Б. Б. Основні підходи до розуміння сутності публічного інтересу як адміністративно-правової категорії. *Юридичний науковий електронний журнал*. 2023. № 10. С. 399–401. DOI: https://doi.org/10.32782/2524-0374/2023-10/95.

17. Мельник Р. Публічний інтерес у публічному управлінні: вихідні позиції доктринального розуміння і практичного застосування (за законодавством України та Казахстану). *Адміністративне*

право і процес. 2022. № 2 (37). С. 5–20. DOI: https://doi.org/10.17721/2227-796X.2022.2.01.

18. Кушнір І. П., Степанова Ю. П. Публічний інтерес у сфері охорони державного кордону. *Аналітично-порівняльне правознавство*. 2024. № 1. С. 404–410. DOI: https://doi.org/10.24144/2788-6018.2024.01.71.

19. Кременовська І. В. Співвідношення категорій «публічний інтерес» і «національна безпека» крізь призму господарсько-правового забезпечення відносин публічної власності в Україні. *Бюлетень Міністерства юстиції України*. 2013. № 6. С. 74–81.

20. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 07.03.2026).

21. Павленко В. С. Національні інтереси та загрози державній безпеці України. *Наукові записки Львівського університету бізнесу та права. Серія: Економічна. Серія: Юридична*. 2022. Випуск 34. С. 84–92. DOI: http://dx.doi.org/10.5281/zenodo.7105166.

22. Шевчук О. Сектор безпеки України як об'єкт публічного адміністрування. *Підприємство, господарство і право*. 2021. № 2. С. 138–142. DOI: https://doi.org/10.32849/2663-5313/2021.2.25.

23. Древаль Ю. Д., Карамишев Д. В., Величко Д. Ю. Значення категорії «публічний інтерес» у системі публічного управління. *Державне будівництво*. 2024. № 2 (36). С. 136–145. DOI: https://doi.org/10.26565/1992-2337-2024-2-10.

24. Гулєвська Г. Ю., Костроміна О. Г., Прокопенко Б. І. Міжнародні стандарти запобігання і врегулювання конфлікту інтересів у публічному управлінні. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90 (3). С. 172–177. DOI: https://doi.org/10.24144/2307-3322.2025.90.3.24.

25. Золотухіна Л. О. Публічний інтерес як адміністративно-правова категорія : автореф. дис. … д-ра юрид. наук : 12.00.07. Запоріжжя, 2019. 40 с.

26. Ковальчук А. Т. Система правового регулювання захисту об'єктів критичної інфраструктури в Україні: сучасний стан та напрями удосконалення. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2025. Випуск 90. Частина 5. С. 172–184. DOI: https://doi.org/10.24144/2307-3322.2025.90.5.21

27. Дуліна О. В. Ризик-орієнтоване управління інфраструктурною безпекою в умовах сучасних викликів. *Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття* : праці всеукр. наук.-практ. конф., м. Житомир, 12–13 грудня 2024 р. Житомир, 2024. С. 322–325.

28. Куспляк Г., Дуліна О., Ровинська К. Роль інфраструктурної безпеки у стратегіях сталого розвитку: політико-правовий аспект. *Міжнародний науковий журнал "Military Science"*. 2024. № 2 (4). С. 174–187. DOI: https://doi.org/10.62524/msj.2024.2.4.15.

29. Holovko O., Kravchenko O., Pogrebytskyi M., Romaniuk I. Ways to improve legal regulation of critical infrastructure information networks protection. *Social and Legal Studios*. 2025. № 8 (1). P. 70–81. DOI: https://doi.org/10.32518/sals1.2025.70.

30. Шкуропадська Д., Лебедева Л., Гонсалвес Ж. Інституційне забезпечення стійкості критичної інфраструктури ЄС, НАТО та України. *Scientia fructuosa*. 2025. № 1 (159). С. 45–60. DOI: https://doi.org/10.31617/1.2025(159)03.

31. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. К. : НІСД, 2018. 84 с.

32. Герасименко О., Сірий О. Нормативно-правове забезпечення міжнародного співробітництва Служби безпеки України під час боротьби зі злочинними правопорушеннями на об'єктах критичної інфраструктури. *Аналітична та порівняльна юриспруденція*. 2025. Випуск № 03. Частина 3. С. 451–464. DOI: https://doi.org/10.24144/2788-6018.2025.03.3.70.

33. Павлов Д., Кучерина С., Євтушенко І. Напрями підвищення ефективності організаційно-правового забезпечення захисту критичної інфраструктури. *Честь і Закон*. 2022. № 1 (80). С. 51–57. DOI: https://doi.org/10.33405/2078-7480/2022/1/80/262464.

34. Дуліна О., Попов М., Ровинська К. Нормативно-правове регулювання гендерної політики у сфері забезпечення інфраструктурної безпеки. *Національні інтереси України*. 2025. № 4 (9). С. 130–143. DOI: https://doi.org/10.52058/3041-1793-2025-4(9)-130-143.

35. Попов М. П., Дуліна О. В., Куспляк Г. І. Гендерні аспекти інфраструктурної безпеки в контексті сталого розвитку регіонів. *Соціально-економічні проблеми сучасного періоду України*. 2024. Вип. 4 (168). С. 33–39 DOI: https://doi.org/10.36818/2071-4653-2024-4-5.

36. Дуліна О. Інноваційні підходи в управлінні безпекою критичної інфраструктури: цифрові рішення та стратегічна стійкість. *Scientific Innovation: Theoretical Insights and Practical Impacts* : праці II міжнар. Наук.-практ. конф., м. Неаполь, Італія 10–12 березня 2025 р. Неаполь, 2025. С. 200–203.

37. Павлов Д., Микитюк М. Правові та організаційні принципи забезпечення захисту критичної інфраструктури в контексті формування нової парадигми безпеки України. *Честь і право*. 2020. № 4 (75). С. 69–77. DOI: https://doi.org/10.33405/2078-7480/2020/4/75/220748.

38. Возненко О. М. Забезпечення безпеки об'єктів критичної інфраструктури: європейський і національний підходи. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Публічне управління та адміністрування*. 2023. Т. 34 (73). № 4. С. 7–12. DOI: https://doi.org/10.32782/TNU-2663-6468/2023.4/02.

39. Папирін Д. О. Трансформація механізмів державного регулювання економічної безпеки в умовах сучасних гібридних загроз: європейський досвід та українські реалі. *Теорія та практика державного управління*. 2024. Вип. 2 (79). С. 342–362. DOI: http://doi.org/10.26565/1727-6667-2024-2-17.

40. Ровинська К. І., Дуліна О. В., Куспляк Г. І. Ефективність політико-правових механізмів забезпечення сталого розвитку в системі національної безпеки України. *Актуальні питання національної безпеки і оборони*. 2025. № 2. С. 3–10. DOI: https://doi.org/10.33099/2618-1614-2025-29-2-3-10.

41. Дзяна Г. О., Дзяний Р. Б. Система публічного управління як об'єкт критичної інфраструктури за критерієм «кібербезпека та захист інформації». *Національні інтереси України*. 2024. № 2 (24). С. 370–379. DOI: https://doi.org/10.52058/3041-1793-2024-2(2)-370-379.

42. Помаза-Пономаренко А. Л., Тарадуда Д. В. Державне управління як критична інфраструктура. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. Випуск 3. С. 64–70. DOI: https://doi.org/10.51547/ppp.dp.ua/2024.3.10.

43. Деякі питання формування переліку територій, на яких ведуться (велися) бойові дії або тимчасово окупованих Російською Федерацією : Постанова Кабінету Міністрів України від 6 грудня 2022 р. № 1364 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1364-2022-%D0%BF#Text (дата звернення: 07.03.2026).

References:

1. Zatonatskyi, D. A. (2025). Critical infrastructure in the structure of economic security of the state. *Finansy Ukrainy*, no. 6, pp. 83–100. https://doi.org/10.33763/finukr2025.06.083 (in Ukrainian).

2. Mykolaichuk, M. M., Popov, M. P., & Todorova, O. L. (2023). Infrastructure security as a component of the national security system: concept, essence, main approaches. *Naukovi perspektyvy*, no. 3 (33), pp. 131–143. https://doi.org/10.52058/2708-7530-2023-3(33)-131-143 (in Ukrainian).

3. Herasymenko, O. M. (2024). Critical infrastructure of Ukraine as a subject of scientific cognition: theoretical aspect. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia PRAVO*, issue 85, part 4, pp. 42–49. https://doi.org/10.24144/2307-3322.2024.85.4.6 (in Ukrainian).

4. Law of Ukraine "On Critical Infrastructure" of November 16, 2021 No. 1882-IX. (2021). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text (in Ukrainian).

5. Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine of December 30, 2021 'On the Strategy for Ensuring State Security'" of February 16, 2022 No. 56/2022. (2022). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/56/2022#Text (in Ukrainian).

6. Order of the Cabinet of Ministers of Ukraine "Concept for the creation of the state system for protection of critical infrastructure" of December 6, 2017 No. 1009-r. (2017). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (in Ukrainian).

7. Decree of the President of Ukraine "Concept of ensuring the national resilience system" of March 27, 2021 No. 479/2021. (2021). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/479/2021 (in Ukrainian).

8. Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine of October 17, 2023 'On the organization of protection and ensuring the security of functioning of critical infrastructure and energy facilities of Ukraine under conditions of military operations'" of October 17, 2023 No. 695/2023. (2023). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/695/2023#Text (in Ukrainian).

9. Resolution of the Cabinet of Ministers of Ukraine "On the establishment of the State Service for the Protection of Critical Infrastructure and Ensuring the National Resilience System of Ukraine" of July 12, 2022 No. 787. (2022). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (in Ukrainian).

10. Law of Ukraine "On amendments to certain laws of Ukraine regarding the powers of the authorized body in the field of protection of critical infrastructure of Ukraine" of October 18, 2022

No. 2684-IX. (2022). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/2684-20#Text (in Ukrainian).

11. Resolution of the Cabinet of Ministers of Ukraine "Some issues of critical infrastructure facilities" of October 9, 2020 No. 1109. (2020). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (in Ukrainian).

12. Izha, M. M., Mykolaichuk, M. M., Popov, M. P., et al. (2025). National security. Odesa : Natsionalnyi universytet "Odeska politekhnika" (in Ukrainian).

13. Bernazyuk, Y. (2021). The concept of public (public) interest in administrative judiciary. *Visegrad Journal on Human Rights*, no. 6, pp. 11–16. Retrieved from https://journal-vjhr.sk/wp-content/uploads/2022/02/VJRHR_6_2021_Last.pd

14. Blikhar, M. (2021). Administrative and legal means of protecting public interest. *Yurydychnyi visnyk*, no. 3, pp. 41–48. https://doi.org/10.32837/yuv.v0i3.2183 (in Ukrainian).

15. Law of Ukraine "On Administrative Procedure" of February 17, 2022 No. 2073-IX. (2022). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/2073-20#Text (in Ukrainian).

16. Main approaches to understanding the essence of public interest as an administrative-legal category. *Yurydychnyi naukovyi elektronnyi zhurnal*, no. 10, pp. 399–400. https://doi.org/10.32782/2524-0374/2023-10/95 (in Ukrainian).

17. Melnyk, R. (2022). Public interest in public administration: initial positions of doctrinal understanding and practical application (according to the legislation of Ukraine and Kazakhstan). *Administratyvne pravo i protses*, no. 2 (37), pp. 5–20. https://doi.org/10.17721/2227-796X.2022.2.01 (in Ukrainian).

18. Kushnir, I. P., & Stepanova, Yu. P. (2024). Public interest in the sphere of protection of the state border. *Analitychno-porivnialne pravoznavstvo*, no. 1, pp. 404–410. https://doi.org/10.24144/2788-6018.2024.01.71 (in Ukrainian).

19. Kremenovska, I. V. (2013). Correlation of the categories "public interest" and "national security" through the prism of economic and legal support of public property relations in Ukraine. *Biuleten Ministerstva yustytsii Ukrainy*, no. 6, pp. 74–81. (in Ukrainian).

20. Law of Ukraine "On National Security of Ukraine" of June 21, 2018 No. 2469-VIII. (2018). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text (in Ukrainian).

21. Pavlenko, V. S. (2022). National interests and threats to the state security of Ukraine. Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna. *Seriia yurydychna*, issue 34, pp. 84–92. http://dx.doi.org/10.5281/zenodo.7105166 (in Ukrainian).

22. Shevchuk, O. (2021). Security sector of Ukraine as an object of public administration. *Pidpryiemstvo, hospodarstvo i pravo*, no. 2, pp. 138–142. https://doi.org/10.32849/2663-5313/2021.2.25 (in Ukrainian).

23. Dreval, Yu. D., Karamyshev, D. V., & Velychko, D. Yu. (2024). The significance of the category "public interest" in the system of public administration. *Derzhavne budivnytstvo*, no. 2 (36), pp. 136–145. https://doi.org/10.26565/1992-2337-2024-2-10 (in Ukrainian).

24. Hulievska, H. Yu., Kostromina, O. H., & Prokopenko, B. I. (2025). International standards for preventing and resolving conflicts of interest in public administration. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*, issue 90 (3), pp. 172–177. https://doi.org/10.24144/2307-3322.2025.90.3.24 (in Ukrainian).

25. Zolotukhina, L. O. (2019). Public interest as an administrative-legal category. Extended abstract of Doctor's thesis. Zaporizhzhia (in Ukrainian).

26. Kovalchuk, A. T. (2025). The system of legal regulation of protection of critical infrastructure facilities in Ukraine: current state and directions for improvement. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo*, issue 90, part 5, pp. 172–184. https://doi.org/10.24144/2307-3322.2025.90.5.21 (in Ukrainian).

27. Dulina, O. V. (2024). Risk-oriented management of infrastructure security in the context of modern challenges. *In Natsionalna bezpeka*

v umovakh viiny, pisliavoiennoi vidbudovy ta hlobalnykh vyklykiv XXI stolittia : pratsi vseukr. nauk.-prakt. konf. (Zhytomyr, 12–13 hrudnia 2024 r.), pp. 322–325. Zhytomyr (in Ukrainian).

28. Kuspliak, H., Dulina, O., & Rovynska, K. (2024). The role of infrastructure security in sustainable development strategies: political and legal aspect. *Military Science*, no. 2 (4), pp. 174–187. https://doi.org/10.62524/msj.2024.2.4.15 (in Ukrainian).

29. Holovko, O., Kravchenko, O., Pohrebytskyi, M., & Romaniuk, I. (2025). Ways to improve legal regulation of critical infrastructure information networks protection. *Social and Legal Studios*, no. 8 (1), pp. 70–81. https://doi.org/10.32518/sals1.2025.70 (in English).

30. Shkuropadska, D., Lebedeva, L., & Gonsalves, Zh. (2025). Institutional support for the resilience of critical infrastructure of the EU, NATO and Ukraine. *Scientia fructuosa*, no. 1 (159), pp. 45–60. https://doi.org/10.31617/1.2025(159)03 (in Ukrainian).

31. Dubov, D. (Ed.). (2018). Public-private partnership in cybersecurity: international experience and opportunities for Ukraine. Kyiv : NISD (in Ukrainian).

32. Herasymenko, O., & Siryi, O. (2025). Legal regulation of international cooperation of the Security Service of Ukraine in combating criminal offenses at critical infrastructure facilities. *Analitychna ta porivnialna yurysprudentsiia*, issue 03, part 3, pp. 451–464. https://doi.org/10.24144/2788-6018.2025.03.3.70 (in Ukrainian).

33. Pavlov, D., Kucherina, S., & Yevtushenko, I. (2022). Directions for improving the effectiveness of organizational and legal support for the protection of critical infrastructure. *Chest i Zakon*, no. 1 (80), pp. 51–57. https://doi.org/10.33405/2078-7480/2022/1/80/262464 (in Ukrainian)

34. Dulina, O., Popov, M., & Rovynska, K. (2025). Legal regulation of gender policy in the field of infrastructure security. *Natsionalni interesy Ukrainy*, no. 4 (9), pp. 130–143. https://doi.org/10.52058/3041-1793-2025-4(9)-130-143 (in Ukrainian).

35. Popov, M. P., Dulina, O. V., & Kuspliak, H. I. (2024). Henderni aspekty infrastrukturnoi bezpeky v konteksti staloho

rozvytku rehioniv [Gender aspects of infrastructure security in the context of sustainable development of regions]. *Sotsialno-ekonomichni problemy suchasnoho periodu Ukrainy*, issue 4 (168), pp. 33–39. https://doi.org/10.36818/2071-4653-2024-4-5 (in Ukrainian).

36. Dulina, O. (2025). Innovative approaches in critical infrastructure security management: digital solutions and strategic resilience. *In Scientific Innovation: Theoretical Insights and Practical Impacts* : Proceedings of the II International Scientific and Practical Conference (Naples, Italy, March 10–12, 2025), pp. 200–203. Naples (in Ukrainian).

37. Pavlov, D., & Mykytiuk, M. (2020). Legal and organizational principles of ensuring the protection of critical infrastructure in the context of forming a new security paradigm of Ukraine. *Chest i Pravo*, no. 4 (75), pp. 69–77. https://doi.org/10.33405/2078-7480/2020/4/75/220748 (in Ukrainian).

38. Voznenko, O. M. (2023). Ensuring the security of critical infrastructure facilities: European and national approaches. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia*, vol. 34 (73), no. 4, pp. 7–12. https://doi.org/10.32782/TNU-2663-6468/2023.4/02 (in Ukrainian).

39. Papyrin, D. O. (2024). Transformation of mechanisms of state regulation of economic security under modern hybrid threats: European experience and Ukrainian realities. *Teoriia ta praktyka derzhavnoho uprlinnia*, issue 2 (79), pp. 342–362. http://doi.org/10.26565/1727-6667-2024-2-17 (in Ukrainian).

40. Rovynska, K. I., Dulina, O. V., & Kuspliak, H. I. (2025). Effectiveness of political and legal mechanisms for ensuring sustainable development in the system of national security of Ukraine. *Aktualni pytannia natsionalnoi bezpeky i oborony*, no. 2, pp. 3–10. https://doi.org/10.33099/2618-1614-2025-29-2-3-10 (in Ukrainian).

41. Dziana, H. O., & Dzianyi, R. B. (2024). The system of public administration as an object of critical infrastructure according to the criterion "cybersecurity and information protection". *Natsionalni*

interesy Ukrainy, no. 2 (24), pp. 370–379. https://doi.org/10.52058/3041-1793-2024-2(2)-370-379 (in Ukrainian).

42. Pomaza-Ponomarenko, A. L., & Taraduda, D. V. (2024). Public administration as critical infrastructure. *Dniprovs'kyi naukovyi chasopys publichnoho upravlinnia, psykholohii*, prava, issue 3, pp. 64–70. https://doi.org/10.51547/ppp.dp.ua/2024.3.10 (in Ukrainian).

43. Resolution of the Cabinet of Ministers of Ukraine "Some issues of forming the list of territories where hostilities are (were) conducted or temporarily occupied by the Russian Federation" of December 6, 2022 No. 1364. (2022). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/1364-2022-%D0%BF#Text (in Ukrainian).

ЕМПІРИЧНИЙ АНАЛІЗ КЕЙСУ КІБЕРАТАКИ: МЕХАНІЗМ, НАСЛІДКИ ТА ПОЛІТИКО-ПРАВОВА КВАЛІФІКАЦІЯ

EMPIRICAL ANALYSIS OF THE CYBERATTACK CASE: MECHANISM, CONSEQUENCES AND POLITICAL AND LEGAL QUALIFICATION

Zavhorodnia Y. V.,
Doctor of Political Sciences, Associate Professor,
Professor of the Department of Political Theories,
National University "Odesa Law Academy",
Odesa, Ukraine

Abstract. The chapter of the monograph is devoted to a comprehensive empirical analysis of a cyberattack case as a complex phenomenon of contemporary international relations, formed at the intersection of technological, political, and legal processes. The main idea of the study is to demonstrate that cyberattacks in the modern security environment function not only as technical incidents but also as instruments of political influence and hybrid confrontation, capable of significantly affecting the functioning of state institutions, critical infrastructure, and international security.

The subject of the research includes the mechanisms of carrying out cyberattacks, their technological structure, institutional and societal consequences, as well as the political and legal qualification of such actions in the context of international law and national legislation. Particular attention is paid to the analysis of the stages of preparation

and implementation of a cyberattack, tools of penetration into digital systems, the scale of damage caused, as well as the problem of attribution of cyber incidents and the determination of their legal status within the system of international security.

The aim of the monograph chapter is to conduct a systematic empirical analysis of a specific cyberattack case in order to identify its structural characteristics, assess its consequences for public administration and information security, and substantiate possible approaches to the political and legal qualification of such actions within the framework of international legal norms and the practice of international organizations. The study is aimed at identifying effective mechanisms for responding to cyber threats and developing strategies for countering cyberattacks as a tool of hybrid warfare.

The research methodology is based on a combination of general scientific and special approaches. The empirical method is used to analyze factual data regarding the course of the cyberattack and its technical characteristics; the system approach is applied to consider the cyber incident as a complex phenomenon encompassing technological, political, and legal aspects; the comparative legal method is used to examine international standards for regulating cyberspace and the practice of qualifying cyber operations; formal-legal and analytical methods are applied to interpret legal acts, international documents, and cybersecurity strategies. The conceptual foundation of the study is formed by theories of cybersecurity, hybrid warfare, and international information security.

The conclusions substantiate that cyberattacks are acquiring a systemic character and are increasingly used as instruments of political pressure and strategic influence in international relations. Their consequences extend far beyond technical disruptions, encompassing the sphere of public administration, economic stability, and public trust in institutions. Effective counteraction to such threats

requires a comprehensive approach combining technical cybersecurity mechanisms, improvement of international legal norms, and the development of interstate cooperation in the field of cybersecurity. The study demonstrates that proper political and legal qualification of cyberattacks and the formation of a system of international responsibility for their commission are essential prerequisites for ensuring stability and security in the global digital environment.

Keywords: Cyberattack, Cybersecurity, Political and Legal Qualification, Cyber Threats, Information Security, Digital Risks.

1. Вступ

Стрімкий розвиток інформаційно-комунікаційних технологій та цифровізація державного управління суттєво трансформують сучасний безпековий простір, формуючи нові виклики для національної та міжнародної безпеки. У цьому контексті кіберпростір дедалі частіше стає ареною політичного протистояння, де поряд із традиційними інструментами впливу застосовуються кібероперації, спрямовані на порушення функціонування інформаційних систем, дестабілізацію державних інституцій та завдання економічних і репутаційних збитків. Кібератаки поступово перетворюються на один із ключових інструментів гібридного протиборства, що дозволяє здійснювати вплив на критичну інфраструктуру, інформаційні ресурси та системи управління без прямого застосування збройної сили. За таких умов аналіз конкретних кейсів кібератак набуває особливого значення для розуміння їх механізмів, наслідків та політико-правових характеристик.

Актуальність дослідження зумовлена необхідністю глибокого емпіричного осмислення природи сучасних кіберзагроз та вироблення ефективних підходів до їх правової кваліфікації й протидії. Кібератаки здатні спричиняти масштабні порушення у функціонуванні державних інституцій, фінансових систем, енергетичної

та транспортної інфраструктури, а також впливати на інформаційну стабільність суспільства. Водночас особливості кіберпростору — анонімність, складність атрибуції та транснаціональний характер — суттєво ускладнюють визначення суб'єктів відповідальності та застосування існуючих норм міжнародного права. Це зумовлює потребу у формуванні сучасних наукових підходів до аналізу механізмів здійснення кібератак, оцінки їх наслідків і визначення можливих моделей правової кваліфікації у системі міжнародної безпеки.

Наукова новизна дослідження полягає у комплексному підході до аналізу кібератаки як багатовимірного явища, що поєднує технологічні, політичні та правові аспекти. У роботі обґрунтовується необхідність розгляду кіберінцидентів не лише як технічних порушень інформаційної безпеки, а й як інструментів стратегічного впливу, здатних впливати на політичні процеси та міжнародні відносини. Запропоновано системне бачення механізму кібератаки, що охоплює етапи її підготовки, реалізації та наслідків, а також розкрито взаємозв'язок між технологічними характеристиками кібероперацій і їх політико-правовою оцінкою у міжнародному праві.

Метою дослідження є з'ясування за результатами комплексного емпіричного аналізу механізму здійснення кібератаки, оцінка її соціально-економічних та інституційних наслідків, а також обґрунтування підходів до політико-правової кваліфікації кіберінцидентів у контексті сучасного міжнародного правопорядку.

Для досягнення поставленої мети визначено такі науково-дослідницькі завдання: дослідити технологічну структуру та етапи реалізації кібератаки, зокрема механізми проникнення до інформаційних систем, інструменти кібероперацій та способи експлуатації вразливостей цифрової інфраструктури; проаналізувати інституційні, економічні та суспільні наслідки кіберінциденту, включаючи його вплив на функціонування державних органів і критичної

інфраструктури; розкрити проблему атрибуції кібератак та складність ідентифікації суб'єктів, причетних до їх здійснення; визначити можливі підходи до політико-правової кваліфікації кібератак у контексті міжнародного права, міжнародної безпеки та національного законодавства.

Методологія дослідження базується на поєднанні загальнонаукових і спеціальних методів. Емпіричний метод застосовано для аналізу фактичних даних щодо перебігу кібератаки та її технічних характеристик. Системний підхід використано для розгляду кіберінциденту як комплексного явища, що охоплює технологічні, політичні та правові аспекти. Порівняльно-правовий метод дозволив дослідити міжнародні стандарти регулювання кіберпростору та практику кваліфікації кібероперацій. Формально-юридичний та аналітичний методи забезпечили аналіз нормативно-правових актів, міжнародних документів і стратегій кібербезпеки. Концептуальною основою дослідження виступають теорії кібербезпеки, гібридної війни та міжнародної інформаційної безпеки.

Логіка подання матеріалу зумовлена метою та завданнями дослідження. У першому параграфі розглядається технологічний механізм кібератаки та етапи її реалізації, включаючи інструменти проникнення у цифрові системи та використані кібероперaційні методи. Другий параграф присвячений аналізу соціально-економічних та інституційних наслідків кібератаки, зокрема її впливу на функціонування державних інституцій і критичної інфраструктури. У третьому параграфі досліджуються підходи до політико-правової кваліфікації кібератаки у системі міжнародної безпеки, а також проблеми міжнародної відповідальності за здійснення кібероперацій. Така структура забезпечує послідовний перехід від аналізу технічних аспектів кіберінциденту до оцінки його суспільних наслідків і правових характеристик у сучасному міжнародному правопорядку.

2. Емпірико-технологічні механізми реалізації кібератаки

В останні роки розвиток технологій цифрового зв'язку та зростання дистанційної роботи по всьому світу через глобальне поширення коронавірусної хвороби (пандемія COVID-19) [1] підвищили ймовірність кібератак у світовій спільноті, які впливають на широкий спектр галузей, таких як охорона здоров'я, транспорт та енергетика. Зловмисники розвивають свої навички в геометричній прогресії, і, незважаючи на постійні зусилля щодо технологічного прогресу в галузі безпеки, все ще важко реагувати на нові кіберзагрози та/або реагувати на поточні події безпеки в кіберзалежних інфраструктурах.

Згідно з Директивою ЄС 2008/114/ЄС про ідентифікацію та позначення європейських критичних інфраструктур (ЕКІ) та оцінку необхідності покращення їхнього захисту (Директива ЕКІ), критичні інфраструктури (КІ) вважаються тими, що є «необхідними для підтримки життєво важливих суспільних функцій, здоров'я, безпеки, захисту, економічного чи соціального благополуччя людей», а їх порушення або знищення може призвести до значного впливу на державу-члена ЄС через «нездатність підтримувати ці функції» [2]. Крім того, Директива ЕКІ вважає критичними інформаційними інфраструктурами (КІ) ті системи інформаційно-комунікаційних технологій (ІКТ), які є «критичними інфраструктурами самі по собі або які є важливими для функціонування критичних інфраструктур» (наприклад, телекомунікації, комп'ютери / програмне забезпечення, Інтернет, супутники тощо) [2].

Протягом останнього десятиліття висококваліфікованим хакерам (наприклад, "Anonymous", "FireEye", "Shadow Brokers", "Baby Elephant" тощо) вдалося здійснити численні та складні атаки через ІКТ-мережі, тобто атаки Advanced Persistent Threat (APT). Крім того, досвідчені кіберзлочинці націлюються на гетерогенні КІІ галузей, проникаючи у взаємопов'язані вузли як трамплін, або для

глибокого проникнення в такі інфраструктури та завдавання серйозної шкоди різноманітним взаємопов'язаним організаціям, або для досягнення конкретної цілі для досягнення зловмисних цілей. Значними прикладами кібератак з великим впливом є атаки програм-вимагачів WannaCry 2017 року, коли було скомпрометовано чверть мільйона машин у понад 150 країнах світу, що вплинуло на кілька організацій, включаючи NHS, іспанську Telefonica, американську компанію FedEx [2], та атаку програм-вимагачів Colonial Pipeline 2021 року [2].

Щоб реагувати на постійно мінливий спектр загроз, методи управління ризиками повинні зосереджуватися на дослідженні особливостей кібератак, таких як напрямок кібератак, профіль зловмисника, потенціал кібератак, місцезнаходження зловмисника в мережі тощо, для виявлення загроз та оцінки ризиків для КІІ. Дерева атак або графи атак визнані як усталені підходи до використання моделювання загроз, дослідження та аналізу поширення ризиків під час оцінки ризиків. Крім того, вони спрямовані на представлення потенційних шляхів атаки, які можуть бути використані зловмисниками для проникнення в системи та отримання несанкціонованого доступу шляхом поступового використання серії вразливостей (ланцюжків вразливостей) серед взаємопов'язаних активів. Кілька алгоритмів виявлення шляхів атаки в літературі здатні ефективно оцінювати та надавати всі можливі шляхи атаки, якими зловмисник може слідувати для компрометації КІІ. Тим не менш, все ще існує простір для дослідження та вдосконалення оцінки шляхів атаки на основі реальних (підтверджених) подій безпеки шляхом аналізу цифрових артефактів, отриманих з різних джерел (наприклад, даних трафіку, файлів журналів). У цьому відношенні ІТ-фахівці та фахівці з безпеки можуть використовувати індикатори компрометації (IoC), які вважаються критичними елементами аналізу інцидентів (наприклад, дані, знайдені в системі) та позначають

потенційно шкідливу активність у системі чи мережі, для кращого розуміння стану безпеки своєї організації. У цьому ключі дослідження генерації атак необхідно вдосконалювати за допомогою підходів, що поєднують різну інформацію, пов'язану з безпекою, включаючи IoC та результати оцінки вразливостей [2].

Запропонований підхід до моделювання атак та генерації ланцюжків доказів має на меті посилити обізнаність про поверхню кібератаки. Він дозволяє представляти знання з кібербезпеки, моделювати та оцінювати можливі кіберзагрози, а також шляхи атак та ланцюжки доказів, пов'язані з підтвердженими небажаними подіями безпеки, що тривають. Інформація, пов'язана з інцидентами, що знаходиться в різних та гетерогенних ІКТ-системах, може включати різні типи даних (наприклад, активні / невиправлені вразливості в технологічній інфраструктурі; виявлення неправильного використання / аномалій у мережі або в системах, моніторинг використання мережі та пропускної здатності; вразливості SCADA тощо) [1].

З цією метою модель моделювання атак та генерації ланцюжків доказів має на меті використовувати алгоритм виявлення шляхів атаки, який обчислює всі можливі шляхи атаки, якими може пройти зловмисник стосовно (а) конкретної підтвердженої події (подій) безпеки, використовуючи інформацію, пов'язану з інцидентами, з різних джерел (наприклад, файли журналів, аналіз мережевого трафіку). Розроблена модель використовує гібридний підхід, який поєднує аналіз інцидентів та аналіз вразливостей, і тому вона може бути корисною для прийняття рішень операторами КІІ як проактивно, так і для обробки інцидентів. Крім того, запропонований підхід моделює атаки шляхом розробки реальних сценаріїв, що дає можливість подальшого експериментування з результатами та перевірки процедур.

Методи моделювання атак можуть додатково допомогти в оцінці конфіденційності. З 2018 року компанії заохочуються

дотримуватися Загального регламенту про захист даних (GDPR) у глобальному масштабі [4]. Цей процес дотримання вимог вже був складним завданням і схильним до помилок для багатьох підприємств через дві виявлені проблеми, згідно з [4]: перша виникає через необізнаність та невизначеність людей щодо правил, які мають застосовуватися, а друга полягає в тому, що деякі організації не мають можливості розробляти політики, які б забезпечували дотримання вимог. Нездатність організацій усвідомлювати конфіденційність створювала проблеми та питання, які дозволяють здійснювати успішні кібератак, що можуть мати значний вплив на організацію (наприклад, атака програм-вимагачів, що скомпрометує конфіденційну інформацію).

Запропонований підхід спирається на методологію оцінки ризиків на основі стандартів, яка враховує стандарти інформаційної безпеки та управління безпекою. Модель моделювання атаки та генерації ланцюжків доказів виявляє та оцінює вразливості шляхом об'єднання та аналізу даних про інциденти під час процесу оцінки ризиків. У цьому контексті модель може досліджувати вразливості, пов'язані з конфіденційністю, розробляти шляхи атаки, пов'язані з інцидентами конфіденційності, такими як порушення даних та витоки інформації, а також аналізувати технічні аспекти атаки. У цьому ключі вона може допомогти операторам КІІ покращити процес прийняття рішень щодо посилення захисту від ризиків конфіденційності та таким чином посилити свою відповідність GDPR [4].

Моделювання змагальних симуляцій за допомогою машинного навчання (ML) — це зростаюча техніка в галузі кібербезпеки, де моделі ML навчаються розпізнавати моделі поведінки, що вказують на кібератак. Моделюючи атаки на систему за допомогою цих моделей ML, організації можуть краще зрозуміти потенційний вплив кібератак та покращити свою загальну безпеку. Виявлення та реагування на змодельовані атаки в режимі реального часу дозволяють

алгоритмам ML забезпечувати проактивний захист від кіберзагроз. Швидкий розвиток штучного інтелекту (ШІ) відкрив можливості для створення червоних команд за допомогою ШІ або навіть автономних. Завдяки навчанню та тренінгам ШІ можна розвинути передові можливості динамічного прийняття рішень, що дозволяє здійснювати нові дії атаки в складних мережевих кіберсистемах, які експерти червоних команд можуть не передбачати або не розробляти [4]. Ці червоні команди використовують ШІ для розробки нових та інноваційних способів атаки на складні кіберсистеми, часто виявляючи вразливості, які експерти червоних команд, можливо, ще не виявили [4]. Це дозволяє організаціям випереджати кіберзлочинців та проактивно захищати свої системи від потенційних загроз. Використання машинного навчання (ML) для симуляції збройних сил виявилося дуже ефективною стратегією посилення кіберзахисту. Оскільки кіберзагрози стають складнішими, очікується, що інтеграція методів ML стане ще більш важливою, дозволяючи організаціям краще виявляти та пом'якшувати потенційні ризики.

Наукове дослідження емпірико-технологічних механізмів реалізації кібератак має важливе значення не лише для технічного аналізу кіберзагроз, але й для формування політико-правових механізмів забезпечення кібербезпеки. У сучасних умовах кіберпростір перетворюється на окрему сферу політичної взаємодії держав, де кібератаки виступають інструментом геополітичного впливу, економічного тиску та інформаційної боротьби. Саме тому дослідження технічних аспектів кібератак — зокрема механізмів проникнення в інформаційні системи, використання ланцюгів вразливостей, формування шляхів атак (attack paths) та аналізу індикаторів компрометації (IoC) — створює емпіричну основу для розробки ефективних політико-правових стратегій протидії кіберзагрозам.

З наукової точки зору, інтеграція результатів технічного аналізу кібератак у політико-правові дослідження дозволяє сформувати

комплексний підхід до регулювання кіберпростору. Такий підхід передбачає поєднання технологічних інструментів аналізу кіберінцидентів із нормативно-правовими механізмами управління ризиками, що включають міжнародні стандарти інформаційної безпеки, політики захисту критичної інфраструктури та вимоги щодо захисту персональних даних [6]. Зокрема, використання моделей моделювання атак, графів атак та симуляцій кіберінцидентів сприяє більш точному визначенню потенційних загроз для критичних інформаційних інфраструктур, що, у свою чергу, дозволяє державним органам формувати обґрунтовані рішення у сфері кіберполітики та правового регулювання.

Крім того, емпіричні дослідження кібератак створюють аналітичну основу для розробки міжнародних механізмів співпраці у сфері кібербезпеки. Умови глобалізації та цифрової трансформації державного управління зумовлюють необхідність гармонізації національних правових систем із міжнародними стандартами, такими як регуляції Європейського Союзу у сфері захисту даних та безпеки мережевих і інформаційних систем [5]. Аналіз технічних характеристик кібератак дозволяє визначати нові типи кіберзагроз, оцінювати їхній потенційний вплив на державні інститути та розробляти правові механізми запобігання кіберінцидентам.

Таким чином, міждисциплінарне поєднання технічного аналізу кібератак із політико-правовими дослідженнями сприяє формуванню цілісної системи кібербезпеки, яка охоплює як технологічні, так і нормативно-інституційні інструменти захисту цифрового середовища. У цьому контексті наукове вивчення механізмів кібератак виступає важливим елементом розробки державної політики кібербезпеки, спрямованої на підвищення стійкості критичних інфраструктур, захист інформаційних ресурсів та забезпечення цифрового суверенітету держави.

3. Соціально-економічні та інституційні наслідки кібератаки

Протягом останніх десятиліть розвиток економіки знань підкреслив важливість та цінність інформаційних технологій для комерційних структур для створення та підтримки конкурентних переваг у сучасному швидкозмінному та технологічно керованому бізнес-середовищі. Швидке поширення інформаційних технологій вплинуло на всі сектори, а новітні розробки сприяли ефективній комунікації, співпраці та інноваційним практикам завдяки підключення до Інтернету. Хоча зростаюча залежність від інформаційно-технологічних систем та платформ здебільшого корисна для бізнес-практик, вона одночасно призвела до збільшення ризику кіберзагроз. Збільшення частоти, різноманітності та складності несприятливих кіберподій призвели до значних фінансових збитків для суб'єктів господарювання.

Так, наукові дослідження визначають кіберподії як «результат будь-яких окремих несанкціонованих зусиль або кульмінацію багатьох таких технічних дій, які зловмисники, використовуючи комп'ютерні технології та мережі, використовують для створення бажаного первинного ефекту на ціль» [7].

Акт кібертероризму передбачає використання Інтернету та інших форм інформаційно-комунікаційних технологій для погроз або заподіяння тілесних ушкоджень з метою отримання політичної чи ідеологічної влади шляхом погроз чи залякування. Крадіжка даних, маніпулювання даними та порушення роботи життєво важливих послуг — все це форми кібератак. Оскільки цифрова інфраструктура стає все більш критичною, а бар'єри для входу зловмисників зменшуються, кібертероризм стає все більшою проблемою. Виявлення, реагування та запобігання цьому злочину створює унікальні виклики для правоохоронних органів та урядів, що вимагає багатогранного підходу [8].

Кібертероризм може мати руйнівні наслідки для широкого кола людей та організацій. Репутація та стабільність країни можуть

бути пошкоджені, можуть виникнути фінансові втрати, а в деяких випадках навіть можуть бути втрачені життя. В результаті кібератак критична інфраструктура, така як електромережі, лікарні та транспортні системи, також може бути порушена, що призводить до широкомасштабних збоїв та лиха. За останні десять років по всьому світу сталося кілька кібератак, включаючи атаку WannaCry (2017), витоки даних Yahoo (2013–2014), витік даних OPM (2015), атаку на ланцюг поставок SolarWinds (2020) тощо [10].

Кібертероризм стосується використання Інтернету, інформаційних середовищ та комунікаційних платформ для здійснення терористичних атак або просування терористичних ідей. Ці атаки можуть приймати різні форми, такі як поширення пропаганди, крадіжка або маніпулювання даними, або порушення роботи критичної інфраструктури. Також його можна називати актом несанкціонованих атак та створення загроз проти комп'ютерів, мереж та даних, які вони зберігають та поширюють [11].

Для досягнення політичної чи соціальної мети це робиться шляхом залякування або погроз уряду чи його громадянам. Кібератаки високої інтенсивності також можуть спричинити насильство щодо осіб чи майна, або, принаймні, завдати достатньої шкоди, щоб викликати страх. У більшості випадків кібертероризм може призвести до смерті або фізичної шкоди, вибуху, авіакатастрофи, забруднення води або значних економічних чи політичних втрат. Якщо він має великий вплив, кібертероризм може бути спрямований проти життєво важливої інфраструктури [9].

Про атаки, які перешкоджають наданню непотрібних послуг або є просто незручністю, не потрібно повідомляти. Кібертероризм — це навмисне використання кіберможливостей, часто недержавними суб'єктами, з основною метою викликати масовий страх, паніку або порушення порядку серед населення, уряду чи організації. Акти кібертероризму зазвичай включають політично,

ідеологічно або соціально мотивовані атаки, спрямовані на критичну інфраструктуру, призводять до значної шкоди або становлять серйозну загрозу національній безпеці [12]. Кібертероризм відрізняє від інших кібератак, таких як кіберзлочинність або хактивізм, явний намір підбурювати до терору або дестабілізувати суспільства, часто переслідуючи політичні чи ідеологічні цілі, а не суто фінансову вигоду чи досягнення соціальних чи етичних цілей. Кібертероризм прагне створити страх, хаос та недовіру у більших масштабах, часто з потенціалом для реальної шкоди або руйнувань.

Оскільки технології використовуються ширше, а їхній злочинний потенціал стає ширше визнаним, деякі форми кібератак, про які повідомляє промисловість, здається, зростають за масштабами та широтою. Також зросла обізнаність громадськості, як і визнання з боку урядів, бізнесу та правових систем. Було важко точно виміряти масштаби та тенденції кіберзлочинності (не лише атаки), або оцінити шкоду та наслідки, спричинені успішними атаками [12].

У сучасному світі актуальне поняття «кібервійни». Кібервійни — це загальний термін для позначення атак на комп'ютерні мережі та захисту від них, а також унікальних технологічних видів діяльності. Кібервійни — це термін, що використовується для опису випадків, коли країна використовує цифрові атаки, такі як комп'ютерні віруси та хакерство, для пошкодження, знищення та знищення критично важливих комп'ютерних систем іншої країни [11].

У майбутньому хакери воюватимуть разом із традиційною зброєю, такою як зброя та ракети, атакуючи інфраструктуру супротивника за допомогою комп'ютерного коду. Кібервійни стали регулярним та смертельним аспектом міжнародного конфлікту у світі, який досі наповнений шпигунами, хакерами та надсекретними програмами цифрової зброї. Однак зараз існує реальний ризик того, що ситуації швидко вийдуть з-під контролю через постійну

конкуренцію у сфері озброєнь у кібервійні та відсутність чітких правил, що регулюють онлайн-бойові дії [13].

Кібертероризм викликає зростаюче занепокоєння через зростаючу залежність від інформаційних технологій у багатьох аспектах суспільства та потенціал для значних порушень або шкоди, спричиненої кібератаками. Він мав значний вплив у всьому світі та продовжує загрожувати різним аспектам стабільності країни. Одним з найбільших наслідків кібератак є порушення роботи життєво важливої інфраструктури, такої як транспортні мережі, електромережі та банківські мережі. Спрямовані атаки на ці системи можуть мати широкомасштабні наслідки, включаючи відключення електроенергії, затримки транспорту та фінансові втрати [9].

Крім того, кібертероризм використовувався для поширення пропаганди та маніпулювання громадською думкою, а також для крадіжки конфіденційної інформації, такої як інтелектуальна власність або персональні дані. Страх перед кібертероризмом також призвів до збільшення витрат на заходи кібербезпеки з боку урядів та приватних компаній. Світ постраждав від кібератак кількома способами, включаючи пошкодження інфраструктури, грошову кризу, економічну кризу, поширення пропаганди або дезінформації, втрату конфіденційної інформації та порушення конфіденційності тощо. Кібертероризм може призвести до значних фінансових втрат для бізнесу та урядів, а також до шкоди репутації країни та економічній стабільності. Його можна використовувати для поширення пропаганди та маніпулювання громадською думкою, що може призвести до соціальної та політичної нестабільності [10]. Кібератаки можуть призвести до крадіжки конфіденційної інформації, такої як інтелектуальна власність або персональні дані, що може мати серйозні наслідки для окремих осіб та організацій.

Страх перед втручанням у жорстокий акт кібервторгнення призвів до збільшення витрат на заходи кібербезпеки з боку урядів та

приватних компаній. Кібератаки можуть призвести до втрати конфіденційності, оскільки персональні дані крадуться або оприлюднюються [13]. Загалом, кібертероризм може завдати значних збоїв та шкоди як окремим особам, так і суспільству.

Кібератаки можуть мати значний вплив на економіку країни. Деякі зі способів, якими кібератак може вплинути на економіку країни, включають прямі фінансові втрати, зниження продуктивності, збільшення бюджету на встановлення заходів безпеки від вторгнення, фінансові крадіжки та пошкодження репутації перед усім світом. Кібератаки можуть призвести до прямих фінансових втрат для бізнесу та урядів, а також до шкоди репутації та економічній стабільності країни. Ці вторгнення можуть порушити роботу підприємств та організацій, що призведе до зниження продуктивності та втрати доходів. Урядам та підприємствам, можливо, доведеться витрачати більше коштів на заходи кібербезпеки, щоб захистити себе від майбутніх атак.

Крадіжка конфіденційної інформації, такої як інтелектуальна власність або комерційна таємниця, може завдати шкоди економіці країни, надаючи конкурентам перевагу. Це може зашкодити репутації країни, що призведе до втрати довіри до її бізнесу та установ [13]. Це може вплинути на здатність країни залучати іноземні інвестиції та мандрівників. Загалом, кібератаки можуть мати значний вплив на економіку країни, тому урядам та корпораціям вкрай важливо вживати запобіжних заходів проти цих ризиків. Найголовніше, що коли країна стає жертвою значної кібератаки, страждає її репутація, що призводить до втрати довіри людей до її інституцій та компаній. Це може вплинути на здатність країни залучати інвестиції, які є важливим джерелом доходу для багатьох країн. Було кілька випадків, коли кібератаки сприяли економічним кризам. У 2017 році атака програми-вимагача NotPetya [8] вразила підприємства та державні установи в Україні та інших країнах,

що призвело до прямих фінансових втрат та зниження продуктивності. За оцінками, атака коштувала підприємствам мільярди доларів. У 2017 році атака програми-вимагача WannaCry [8] вразила підприємства та державні установи у понад 150 країнах, що призвело до прямих фінансових втрат та зниження продуктивності. За оцінками, атака коштувала підприємствам мільярди доларів. У 2020 році було виявлено, що компанія SolarWinds, значний постачальник програмного забезпечення для моніторингу IT, зазнала проникнення [10], що дозволило групі хакерів отримати доступ до мереж клієнтів SolarWinds. Численні компанії та урядові установи в США та в усьому світі постраждали від атаки, що призвело до негайних фінансових втрат та втрати продуктивності.

Історична природа кіберзлочинності в Пакистані [10] виявляє два основні типи кібератак: низькорівневі атаки з боку окремих індійських хакерів та атаки як місцевих, так і міжнародних хакерів, які прагнуть фінансової вигоди. Один із значних інцидентів стосувався злому банку Meezan, в результаті якого було викрито 69 189 даних карток для продажу та спричинено втрату даних банком приблизно на 3,5 мільйона доларів. Крім того, K-electric зазнала порушення безпеки, коли хакери вимагали викуп у розмірі 3,5 мільйона доларів.

Однак через тиждень викуп подвоївся до 7 мільйонів доларів, але K-electric не виконав вимогу, що призвело до витоку викраденої інформації в Інтернеті, включаючи конфіденційні дані клієнтів, такі як імена, адреси, CNIC та реквізити банківського рахунку. Незважаючи на серйозність ситуації, K-electric не сплатила викуп і не вжила достатніх заходів для покращення своєї кібербезпеки, що зрештою призвело до витоку 8,5 ГБ даних хакером. Ці інциденти підкреслюють нагальну потребу в кращих заходах кібербезпеки в Пакистані для захисту від таких загроз та захисту конфіденційної інформації [11].

Кібертероризм також може мати значний вплив на політику кількома способами, включаючи зрив виборів, поширення дезінформації, пропаганди, порушення державної таємниці та порушення конфіденційності. Кібератаки на виборчі системи або кампанії можуть саботувати виборчий процес та підірвати довіру громадськості до чесності виборів. Кібертерористи можуть використовувати інтернет та соціальні мережі для поширення пропаганди та маніпулювання громадською думкою, що може впливати на політичні події та формувати державну політику.

Кібератаки на системи зв'язку, такі як електронна пошта або телефонні мережі, можуть перешкоджати політичним лідерам та організаціям спілкуватися один з одним та з громадськістю. Кібератаки, які призводять до втрати конфіденційності, можуть підірвати довіру до політичних лідерів та інституцій [13]. Загалом, кібертероризм може мати глибокі наслідки для політичного ландшафту країни та може сприяти соціальній та політичній нестабільності.

Якщо метою зловмисників є зрив виборів, атаки на виборчі системи або інфраструктуру можуть порушити процес голосування та перешкодити людям проголосувати. Винні можуть поширювати дезінформацію або пропаганду через соціальні мережі та інші онлайн-платформи, щоб вплинути на результати виборів. Напади на політичні кампанії можуть порушити роботу кампаній та поставити під загрозу конфіденційні дані кампаній. Вторгнення у виборчі системи або кампанії може підірвати довіру до виборчого процесу та призвести до втрати впевненості в чесності виборів. Кібертерористи можуть використовувати інтернет та соціальні мережі для поширення пропаганди та маніпулювання громадською думкою, що може призвести до соціальної та політичної нестабільності та потенційно до краху уряду [14].

Вони можуть призвести до втрати конфіденційності або конфіденційної інформації, підриваючи довіру до уряду та потенційно

до його краху. Важко з упевненістю сказати, чи якийсь уряд падав виключно через кібертероризм, оскільки більшість великих подій мають кілька причин. Однак було кілька випадків, коли кібератаки відіграли певну роль у соціальній та політичній нестабільності та падінні урядів.

У 2011 році [14] серія протестів та повстань прокотилася по Близькому Сходу та Північній Африці, що призвело до повалення кількох урядів. Використання соціальних мереж для організації та поширення інформації відіграло значну роль в Арабській весні, і деякі експерти вважають, що кібератаки на урядові системи зв'язку могли сприяти цій нестабільності. Під час президентських виборів у США 2016 року [15], було виявлено, що російські хакери були спрямовані проти передвиборчої кампанії Гілларі Клінтон та зламали електронні адреси посадовців Демократичної партії, що призвело до розголошення конфіденційної інформації через WikiLeaks. Деякі експерти вважають, що ці атаки могли вплинути на результат виборів. У 2020 році [13] було виявлено, що група хакерів скомпрометувала програмне забезпечення SolarWinds, головного постачальника програмного забезпечення для управління IT, щоб отримати доступ до мереж клієнтів SolarWinds.

Атака торкнулася кількох урядових установ у Сполучених Штатах, що викликало занепокоєння щодо цілісності систем уряду США та можливості подальшої шкоди. Концепцію кібертероризму можна простежити до 1990-х років [12], коли зростання популярності Інтернету та дискусії про «інформаційне суспільство» викликали занепокоєння щодо потенційних ризиків для США з високим рівнем мережевої взаємодії.

Наслідки кібератаки можуть бути серйозними, тому важливо вживати заходів для боротьби з кібертероризмом, оскільки кібератаки можуть мати серйозні наслідки. Існує потенціал для економічних втрат, шкоди репутації та стабільності країни і навіть втрати

життя через кібертероризм. Також можуть виникнути широкомасштабні збої та хаос, коли порушується робота критичної інфраструктури, такої як електромережі та лікарні. Безпека та надійність технологій також можуть бути підірвані кібератаками, що робить людей невпевненими щодо безпеки та надійності їхніх систем [19]. Вжиття превентивних заходів та пом'якшення потенційних наслідків кібератаки — це два найважливіші заходи, які окремі особи та організації можуть вжити, щоб зменшити ризики стати жертвою кібератаки.

4. Політико-правова кваліфікація кібератаки у системі міжнародної безпеки

Наразі немає міжнародно визнаних критеріїв для визначення того, чи є кібератака національної держави застосуванням сили, еквівалентним збройному нападу, який може спровокувати військову відповідь. Так само, досі не було розроблено жодних міжнародних, юридично обов'язкових документів, які б чітко регулювали міждержавні відносини в кіберпросторі. Самооборона та контрзаходи у разі збройних нападів дозволені міжнародним правом, коли воюючи сторона порушує міжнародне право в мирний час або порушує право збройного конфлікту (ПЗК) у воєнний час. Однак термін «збройний напад» не має загальноприйнятого визначення щодо кібератак. Окрім того, що являє собою збройний напад у кіберпросторі, залишаються питання щодо того, які положення чинного міжнародного права регулюють ведення війни в кіберпросторі.

У вересні 2012 року Державний департамент публічно висловився щодо того, чи може кібердіяльність вважатися застосуванням сили згідно зі статтею 2(4) Статуту Організації Об'єднаних Націй (ООН) [15] та звичаєвим міжнародним правом. За словами тодішнього юрисконсульта Держдепартаменту Гарольда Коха, «кібердіяльність, яка безпосередньо призводить до смерті, поранень або значних руйнувань, ймовірно, розглядатиметься як застосування

сили». Прикладами були провокування аварії на атомній електростанції, відкриття дамби та спричинення пошкоджень від повені, а також спричинення катастроф літаків через перешкоджання управлінню повітряним рухом. Зосереджуючись на досягнутих цілях, а не на засобах, за допомогою яких вони здійснюються, це визначення кібервійни, можливо, відповідає чинним міжнародно-правовим рамкам. Якщо суб'єкт використовує кіберзброю для створення кінетичних ефектів, які можуть відтворити вогневу міць за інших обставин, то використання цієї кіберзброї піднімається до рівня застосування сили.

Однак Сполучені Штати визнають, що кібератаки без кінетичного ефекту також є елементом збройного конфлікту за певних обставин. Кох пояснив, що кібератаки на інформаційні мережі під час триваючого збройного конфлікту регулюватимуться тими ж принципами пропорційності, що застосовуються до інших дій згідно з Локомотивом боротьби з вогнепальною дією (LOAC). Ці принципи включають відплату у відповідь на кібератаку з пропорційним використанням кінетичної сили. Крім того, «діяльність у комп'ютерних мережах, яка рівнозначна збройному нападу або його безпосередній загрозі», може призвести до права країни на самооборону згідно зі статтею 51 Статуту ООН. У Міжнародній стратегії щодо кіберпростору 2011 року [16] підтверджено, що «коли це виправдано, Сполучені Штати реагуватимуть на ворожі дії в кіберпросторі так само, як і на будь-яку іншу загрозу нашій країні».

У Міжнародній стратегії щодо кіберпростору та цифрової політики 2024 року [17] зазначається, що Сполучені Штати працюють над просуванням відповідальної поведінки держав на основі схваленої ООН системи щодо «застосування чинного міжнародного права, дотримання глобально визнаних та добровільних норм поведінки держав у мирний час, розробки та впровадження заходів довіри для зменшення ризику конфлікту в кіберпросторі».

Це стосується мети Кіберстратегії Міністерства оборони (DOD) на 2023 рік, яка полягає в тому, щоб «зміцнити відповідальну поведінку держав шляхом заохочення дотримання міжнародного права та міжнародно визнаних норм кіберпростору».

У розділі XVI Посібника Міністерства оборони з питань воєнного права [18] зазначається, що Сполучені Штати прагнуть співпрацювати з іншими державами не для того, щоб з'ясувати, чи застосовується міжнародне право до кіберпростору, а для того, щоб з'ясувати, як. Як Державний департамент, так і Міністерство оборони стверджують, що кібератаки, що досягають рівня збройного нападу, можуть призвести до зобов'язань за договорами про взаємну оборону, хоча поняття збройного нападу в кіберпросторі залишається невизначеним.

У 2009 році Центр спільної кіберзахисту Організації Північноатлантичного договору (НАТО) [14] скликав міжнародну групу незалежних експертів для розробки посібника з питань права, що регулює кіберконфлікти. Перший Талліннський посібник, як його називають, був опублікований у 2013 році та пропонує 95 «правил чорної літери», що стосуються суверенітету, відповідальності держав, Закону про конфіденційність, гуманітарного права та права нейтралітету. Талліннський посібник є академічним текстом і як такий не має обов'язкової сили. Талліннський посібник 2.0 від лютого 2017 року розширює перший і пропонує 154 правила чорної літери, що регулюють кібероперації, зокрема в мирний час.

У положеннях статті 5 Північноатлантичного договору напад на одного члена вважається нападом на всіх, що надає військову допомогу відповідно до статті 51 Статуту ООН. Однак НАТО наразі не визначає кібератаки як чіткі військові дії. Талліннський посібник прирівнює застосування сили до тих кібероперацій, «наслідки яких... були аналогічними тим, що виникли б в результаті дій, які

в іншому випадку кваліфікуються як кінетична збройна атака». Стаття 4 Північноатлантичного договору застосовує принципи колективних консультацій до будь-якої держави-члена, чия безпека та територіальна цілісність опинилася під загрозою; однак незрозуміло, як ця стаття застосовуватиметься до різних категорій кібератак, деякі з яких можуть не мати кінетичних еквівалентів. Також незрозумілою є концепція юрисдикції та те, що являє собою територіальна цілісність для тих держав-членів, які розглядають кіберпростір як глобальну сферу або спільне надбання.

Так зване «Право війни», також відоме як ПВК, втілене в Женевській та Гаазькій конвенціях і Статуті ООН, може застосовуватися до кібератак, але немає конкретної угоди щодо його застосування. До ускладнюючих факторів належать труднощі з атрибуцією, потенційне використання віддалених комп'ютерів та можлива шкода третім сторонам від кіберконтратак, які може бути важко стримати. Крім того, як і у випадку з доктриною НАТО, залишаються питання територіальних кордонів та того, що вважається збройним нападом у кіберпросторі. Застосування цього права виглядало б найчіткішим у ситуаціях, коли кібератака завдає фізичної шкоди, такої як порушення роботи електромережі. Як згадувалося вище, Талліннський посібник розглядає багато з цих питань. За відсутності договірного визначення того, що вважається збройним нападом або застосуванням сили в кіберпросторі, співавтор Талліннського посібника Міхаель Шмітт запропонував у своїх академічних публікаціях критерії для аналізу згідно з міжнародним правом. Основні принципи, викладені в Гаазьких конвенціях щодо застосування збройних сил, — це військова необхідність, пропорційність, гуманність та лицарство. Країну, чиї військові збройні сили проводять кібероперації відповідно до цих принципів, можна вважати такою, що бере участь у кібервійні.

Кібертероризм значно вплинув на світові правові системи. Використання терористами інформаційно-комунікаційних технологій (ІКТ), особливо Інтернету та нових технологій, що дозволяють анонімне спілкування, викликає зростаюче занепокоєння. Управління ООН з боротьби з тероризмом розробляє всеохоплюючу стратегію кібербезпеки. Хоча деякі країни прийняли національне законодавство про боротьбу з кібертероризмом (наприклад, розділ 33 Закону Кенії про зловживання комп'ютерами та кіберзлочини 2018 року та розділ 10 Закону Пакистану про запобігання електронним злочинам 2016 року [19; 20]), кібертероризм прямо не заборонений міжнародним правом. Концепція кібертероризму пронизує широкий порядок денний національної безпеки Китаю, який спрямований на ретельне управління, регулювання, сек'юритизацію та моніторинг його кіберсуверенітету, що підтверджується китайським законодавством, політикою та судовою практикою [10].

Це свідчить про те, що Китай прийняв комплексну стратегію управління своїм кіберпростором для захисту своїх інтересів у національній безпеці [11]. Кібертероризм має широкий спектр впливу на правову систему США, включаючи систему кримінального правосуддя, національну безпеку, економіку та громадянські свободи. Загроза, яку кібертероризм становить для традиційних методів розслідування, є одним з найважливіших його наслідків для правової системи США. Виявити та затримати відповідальних за кібератаки може бути складно, оскільки вони часто походять від людей або організацій, розкиданих по всьому світу. Процес розслідування та судового переслідування ще більше ускладнюється тим фактом, що кібератаки можуть бути здійснені з будь-якого місця, де є підключення до Інтернету.

Як результат, правовій системі довелося створити нові підходи до розслідування та судового розгляду справ про кібертероризм.

Для запобігання кібертероризму Сполучені Штати запровадили кілька правових заходів та законів. Наприклад, Закон про комп'ютерне шахрайство та зловживання (CFAA) 1986 року визнає незаконними кілька комп'ютерних правопорушень, таких як злом та несанкціонований доступ до комп'ютерних систем. Після терактів 11 вересня Конгрес ухвалив Патріотичний акт, який розширив можливості уряду щодо спостереження та дозволив збір даних електронних комунікацій [8].

Для вирішення проблеми кібербезпеки та кіберзлочинності Росія запровадила кілька законів. «Закон Ярової», який зобов'язує операторів зв'язку зберігати дані користувачів до трьох років і надавати ФСБ доступ до цих даних, був прийнятий Державною Думою (нижньою палатою парламенту Росії) у 2016 році. Противники закону стверджують, що він порушує конфіденційність користувачів і надає уряду надмірні повноваження для відстеження та регулювання онлайн-активності. Росія також уклала союзи та угоди про співпрацю з іншими країнами [10]. Щоб посилити співпрацю у запобіганні кібератак та сприяти розвитку глобальних норм і правил у кіберпросторі, Росія та Китай опублікували спільну заяву про співпрацю в галузі міжнародної інформаційної безпеки у 2020 році.

Кібертероризм був криміналізований на міжнародному рівні за допомогою різних правових засобів, включаючи законодавчу, регуляторну та правоохоронну діяльність. Створення міжнародно-правових баз, що пропонують напрямки щодо запобігання та переслідування кіберзлочинів, стало значним завданням [10]. Як приклад, Конвенція Ради Європи про кіберзлочинність, прийнята у 2001 році, пропонує основу для гармонізації національного законодавства щодо кіберзлочинності та сприяє міжнародній співпраці у запобіганні та переслідуванні кіберзлочинності. Багато країн створили власні закони та правила.

Наприклад, CFAA та Patriot Act надають уряду США юридичні повноваження розслідувати та переслідувати кіберзлочини, а NIST створив основу для посилення кібербезпеки критичної інфраструктури (Baldassarre, 2023). Враховуючи, що кібератаки часто відбуваються з-за меж національних кордонів, міжнародна співпраця також є важливою у боротьбі з кібертероризмом. Для заохочення обміну даними та спільних досліджень багато країн утворили альянси та угоди.

Наприклад, для заохочення співпраці з питань кібербезпеки та кіберзлочинності США та Велика Британія приєдналися до Діалогу з кібербезпеки між США та Великою Британією. На завершення, було вжито низку міжнародно-правових заходів для боротьби з кібертероризмом, включаючи створення міжнародно-правових рамок, розробку національного законодавства та нормативних актів, створення спеціалізованих підрозділів для боротьби з кіберзлочинністю та заохочення глобальної співпраці та партнерства. Очікується, що країни продовжуватимуть розробляти та адаптувати правові заходи та політику для боротьби з цією зростаючою загрозою в міру розвитку кібертероризму [11].

Ось більш детальний опис кожного контрзаходу:

1. Освіта та обізнаність: Сприяння освіті та обізнаності з питань кібербезпеки серед громадськості, державних службовців та операторів критичної інфраструктури є важливим для того, щоб окремі особи та організації знали про потенційні загрози та способи їх пом'якшення.

2. Надійний кіберзахист: Розробка та підтримка надійних заходів кібербезпеки, включаючи брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення, має вирішальне значення для ефективного запобігання кібератак та реагування на них.

3. Міжнародна співпраця: Співпраця з іншими країнами та міжнародними організаціями є важливою для обміну

розвідувальною інформацією про загрози, розслідування кіберінцидентів та розробки скоординованої глобальної відповіді на кібертероризм.

4. Дослідження та розробки: Інвестиції в дослідження та розробки в галузі кібербезпеки необхідні для того, щоб випереджати нові загрози та розробляти інноваційні технології та стратегії захисту від кібертероризму.

5. Реагування на кіберінциденти: Розробка чітко визначеного плану реагування на інциденти допомагає ефективно керувати кіберінцидентами та пом'якшувати їх наслідки, коли вони трапляються.

6. Міцна правова база: Впровадження та забезпечення дотримання законів і правил кібербезпеки забезпечує правову основу для переслідування кіберзлочинців та стримування зловмисників.

7. Міжнародні угоди та норми: Участь у міжнародних угодах, нормах та договорах, пов'язаних з кіберпростором, та їх просування може допомогти встановити правила поведінки та співпраці в цифровій сфері.

8. Безперервний моніторинг та розвідка: Безперервний моніторинг мереж та систем, разом зі збором та аналізом розвідувальних даних, дозволяє раннє виявлення кіберзагроз та прийняття кращих рішень у відповідь на ці загрози.

9. Співпраця з приватним сектором: Співпраця з організаціями приватного сектору, які часто володіють та експлуатують критично важливу інфраструктуру, є життєво важливою. Державно-приватне партнерство може покращити обмін інформацією та посилити заходи кібербезпеки.

Впроваджуючи ці контрзаходи, держави можуть значно покращити свою стійкість до кібертероризму та інших кіберзагроз. Важливо адаптувати та розвивати ці заходи, щоб враховувати зміну характеру кіберзагроз та залишатися проактивними у захисті національної безпеки та критичної інфраструктури.

Економічні, соціальні та політичні наслідки кібератак, включаючи кібертероризм, є далекосяжними та глибокими:

— кібератаки призвели до значних фінансових втрат для постраждалих організацій через крадіжки, шахрайство або порушення роботи бізнесу, що спричинило значні витрати на відновлення, включаючи інвестиції в кібербезпеку. Коли дані клієнтів скомпрометовано або послуги перервано, підприємства можуть зазнати шкоди репутації, що може призвести до втрати довіри клієнтів та зменшення доходів. Зростання страхових премій та франшиз на кібербезпеку обтяжило підприємства, впливаючи на їхні операційні витрати. Кібератаки на критично важливу інфраструктуру порушили ланцюги поставок, впливаючи на виробництво, доставку та економіку загалом;

— витоки даних призвели до розкриття конфіденційної особистої інформації, що порушило конфіденційність людей і потенційно призвело до крадіжки особистих даних або шахрайства. Страх і тривога, спричинені кібертерористичними атаками, мають психологічний вплив на людей і суспільство, підриваючи почуття безпеки та довіри. У деяких випадках, особливо коли порушується робота критично важливих послуг, виникали соціальні заворушення, оскільки люди розчарувалися через неможливість доступу до основних послуг;

— кібератаки на урядові установи, оборонні системи або критичну інфраструктуру становили значну загрозу національній безпеці, потенційно ставлячи під загрозу здатність країни захищатися.

Кібератаки або кібершпигунство, що спонсоруються державами, загострили міжнародну напруженість та загострили дипломатичні відносини між країнами. Гучні кібератаки призвели до змін у політиці, нових правил та посилення участі уряду в кібербезпеці, що вплинуло на підприємства та окремих осіб. Нездатність захиститися від кібератак підірвала довіру громадськості до уряду та його здатності забезпечувати національну безпеку та стійкість інфраструктури.

Загрозі необхідно протидіяти, незалежно від того, наскільки критичною вона є. Тому, з огляду на постійно зростаючу загрозу кібертероризму, було запроваджено різноманітні глобальні політичні заходи та контрзаходи. У рамках зусиль Китаю щодо протидії загрозі кібертероризму в межах своїх кордонів було вжито низку заходів [12]. У рамках плану кібербезпеки Державної ради, опублікованого минулого року, країна окреслила заходи щодо посилення кіберзахисту країни, такі як покращення здатності країни виявляти та реагувати на кіберзагрози, а також посилення захисту критичної інфраструктури від кібератак.

Щоб захистити себе від кібератак, Китай, окрім цих зусиль, вжив низку технічних заходів. Для захисту мереж і систем використовуються брандмауери, системи виявлення вторгнень та інші технології. Китай також прийняв кілька правил і законів у сфері кібербезпеки, таких як Закон Китайської Народної Республіки про кібербезпеку, який набрав чинності у 2017 році.

Мета цього закону — захист конфіденційної інформації жителів країни, а також ключової інфраструктури федерального уряду та загальної кібербезпеки країни. Крім того, Китай створив кілька агентств та організацій з кібербезпеки з метою координації зусиль щодо боротьби з кіберзагрозами. Координаційний центр технічної групи реагування на надзвичайні ситуації в національних комп'ютерних мережах (CNCERT), який координує реагування на надзвичайні ситуації в кіберпросторі, та Адміністрація кіберпростору Китаю, яка контролює управління політикою кібербезпеки країни, є двома організаціями, відповідальними за це [13].

Кілька агентств та організацій у Сполучених Штатах отримали завдання боротися із загрозою кібертероризму та захищатися від кібератак для протидії їй. Серед обов'язків Міністерства внутрішньої безпеки (DHS) є захист критичної інфраструктури країни від кіберзагроз, а також координація зусиль щодо боротьби

з кібератаками. Обмін інформацією та реагування на інциденти здійснює Національний центр кібербезпеки та інтеграції комунікацій (NCCIC), підрозділ DHS. Розслідування та переслідування кіберзлочинів, включаючи кібертероризм, є відповідальністю Федерального бюро розслідувань (ФБР) [13]. Для захисту військових систем та мереж від кібератак Міністерство оборони (DOD) запровадило кілька ініціатив у сфері кібербезпеки. Сполучені Штати також запровадили кілька законів та нормативних актів для вирішення питань кібербезпеки. Серед них Закон про кібербезпеку 2015 року [17] та Закон про Агентство з кібербезпеки та безпеки інфраструктури 2018 року.

Вони встановлюють основу для обміну інформацією та реагування на інциденти, а також посилення кібербезпеки критичної інфраструктури. Федеральна служба безпеки Росії (ФСБ) відповідає за розслідування та переслідування кіберзлочинів, а також за захист від кіберзагроз. Федеральна служба охорони Росії (ФСО) захищає урядові системи зв'язку та інформації від кібератак [15]. Федеральна служба з технічного та експортного контролю (ФСТЕК), яка контролює кібербезпеку, регулює ключові галузі інфраструктури Росії. Росія прийняла кілька законів та нормативних актів, що стосуються кібербезпеки, на додаток до Федерального закону про інформацію, інформаційні технології та захист інформації. Також він описує, як державні установи та компанії повинні реагувати на кіберзагрози та як має бути захищена персональна інформація.

Саудівська Аравія створила Національний центр кібербезпеки (NCSC), який відповідає за координацію зусиль щодо захисту від кіберзагроз та сприяння кібербезпеці в Саудівській Аравії [13]. Під керівництвом Національного управління кібербезпеки (NCA) у країні впроваджуються заходи кібербезпеки та дотримуються нормативних актів. Серед іншого, у Саудівській Аравії діє закон про кіберзлочинність, який також криміналізує кібертероризм. Особи та

організації, причетні до кіберзлочинів, можуть бути розслідувані та притягнуті до відповідальності відповідно до цього закону. Національні правила кібербезпеки Саудівської Аравії та Національна стратегія кібербезпеки Саудівської Аравії стосуються кібербезпеки.

Ці правила спрямовані на посилення кібербезпеки критичної інфраструктури та створення системи для обміну інформацією та реагування на інциденти. Двома установами та організаціями, створеними Саудівською Аравією для боротьби з наслідками кіберзлочинності, є Валютне управління Саудівської Аравії (SAMA) та Генеральне інвестиційне управління Саудівської Аравії (SAGIA) відповідно [14].

Національне управління електронної безпеки ОАЕ (NESA) контролює заходи кібербезпеки та захищає країну від кіберзагроз [16]. Для боротьби з кіберзагрозами було створено кілька агентств та організацій з кібербезпеки, включаючи Національне управління з питань криз та ліквідації наслідків стихійних лих (NCEMA) та Національну групу реагування на комп'ютерні надзвичайні ситуації (aeCERT) [15]. В Ірані Національний центр кіберпростору (NCC) відповідає за координацію зусиль щодо захисту від кіберзагроз та сприяння кібербезпеці [16]. В Ірані було створено кілька агентств та організацій з кібербезпеки для координації зусиль щодо боротьби з кіберзагрозами, таких як Центр стратегічних досліджень кіберпростору (CSSC) та Національна група реагування на комп'ютерні надзвичайні ситуації (MAHER) [17].

Аналогічно, такі країни, як Франція, Туреччина, Німеччина, Англія, Японія, Гонконг, Корея, Бельгія, Малайзія, Індонезія, Індія, Пакистан та інші країни світу мають власні спеціалізовані агентства та установи, які спеціально виявляють будь-які види вторгнення або вторгнення із зовнішнього джерела та намагаються протидіяти їм на місці. Крім того, всі країни мають власний набір правил, механізмів, законів та процедур для запобігання будь-якій міжрегіональній або внутрішньорегіональній кібертерористичній діяльності.

Ці превентивні заходи допомагають значно зменшити кібертероризм, але з плином часу технології розвиваються, а зловмисники знаходять інноваційні способи порушення безпеки. Саме тому важливо постійно відстежувати наслідки останніх кібератак та запропоновані контрзаходи проти них [18].

Посилення кібербезпеки та ефективна протидія кібертероризму вимагає комплексного підходу, який включає уряди та організації. Уряди повинні розробити національну стратегію кібербезпеки, яка чітко визначає цілі, ролі та обов'язки. Щоб зміцнити свою правову базу, вони повинні прийняти та забезпечити виконання суворих законів та правил кібербезпеки, щоб притягнути зловмисників до відповідальності.

Крім того, слід визначити та класифікувати правопорушення, пов'язані з кібертероризмом. Вони повинні впроваджувати захисні заходи для критичної інфраструктури, такої як енергетична, транспортна та охорона здоров'я, а також проводити регулярні оцінки та аудити безпеки. Більше того, уряди повинні співпрацювати з іншими країнами для обміну розвідувальною інформацією про загрози, розслідування транскордонної кіберзлочинності та участі в міжнародних угодах та нормах для сприяння відповідальній поведінці в кіберпросторі [17].

Аналогічно, вони повинні тісно співпрацювати з приватним сектором для покращення обміну інформацією, розробки передового досвіду та посилення колективної оборони. Тим часом вони повинні інвестувати в програми освіти та навчання з кібербезпеки, щоб вирішити проблему нестачі кваліфікованих фахівців з кібербезпеки та сприяти поширенню обізнаності та передового досвіду серед громадськості щодо кібербезпеки. Вони повинні створити національні групи реагування на інциденти, проводити регулярні навчання для підготовки до кіберінцидентів та розробити чіткий ланцюг командування для реагування на інциденти. Зрештою, слід

заохочувати обмін передовою розвідувальною інформацією про загрози між державними установами, приватними організаціями та міжнародними партнерами [19].

Міжнародна правова база та національні закони та нормативні акти відіграють центральну роль у визначенні, переслідуванні та запобіганні кібертероризму. Наприклад, Організація Об'єднаних Націй (ООН) була на передовій боротьби з кібертероризмом через резолюції Генеральної Асамблеї, які заохочують держави-члени до співпраці та розробки норм відповідальної поведінки держав у кіберпросторі [17]. Талліннський посібник, необов'язковий документ, розроблений експертами, надає тлумачення чинного міжнародного права, що застосовується до кіберпростору, пропонуючи рекомендації щодо правової бази, що стосується кібероперацій [18]. Будапештська конвенція про кіберзлочинність, також відома як Конвенція Ради Європи про кіберзлочинність, є багатостороннім договором, спрямованим на гармонізацію законів та посилення міжнародного співробітництва у боротьбі з кіберзлочинністю, який включає положення, пов'язані з кібертероризмом [19].

5. Висновки

Проведене дослідження дозволяє зробити висновок, що сучасні кібератаки є складним багатовимірним явищем, яке поєднує технологічні, соціально-економічні та політико-правові аспекти. Розвиток цифрових технологій, глобалізація інформаційних мереж та зростання залежності держав і суспільств від інформаційно-комунікаційної інфраструктури створюють нові можливості для реалізації кіберзагроз, що здатні впливати не лише на окремі організації, але й на функціонування державних інститутів та міжнародної системи безпеки загалом.

Аналіз емпірико-технологічних механізмів реалізації кібератак свідчить, що сучасні кібероперації здійснюються за допомогою

комплексних методів, які включають використання вразливостей програмного забезпечення, соціальної інженерії, шкідливого програмного забезпечення, а також застосування інструментів автоматизованого аналізу даних і машинного навчання. Моделювання атак, використання графів атак та аналіз індикаторів компрометації дозволяють більш ефективно ідентифікувати потенційні загрози, прогнозувати сценарії їх реалізації та розробляти механізми протидії.

Водночас кібератаки мають значні соціально-економічні та інституційні наслідки. Порушення функціонування критичної інфраструктури, фінансові втрати, витоки конфіденційної інформації, а також дестабілізація політичних процесів демонструють, що кіберпростір перетворився на один із ключових вимірів сучасної безпеки. Зростання кількості кіберінцидентів підтверджує необхідність посилення інституційних механізмів кіберзахисту, удосконалення політики управління ризиками та розвитку міжнародного співробітництва у сфері кібербезпеки.

Особливого значення набуває політико-правова кваліфікація кібератак у системі міжнародної безпеки. Нормативно-правове регулювання кіберпростору поступово формується на основі норм міжнародного права, міжнародних договорів та національного законодавства держав. Водночас швидкий розвиток технологій та складність атрибуції кібератак створюють нові виклики для існуючих правових механізмів, що потребує подальшого вдосконалення міжнародно-правових інструментів регулювання кіберконфліктів.

Кібертероризм передбачає використання комп'ютерних та інтернет-технологій для вчинення актів насильства. Може використовуватися різноманітний спектр методів, включаючи злом комп'ютерних систем для крадіжки конфіденційної інформації, поширення шкідливого програмного забезпечення для порушення роботи, а також підбурювання до насильства або сіяння розбрату в соціальних мережах. Фінансові втрати, втрати життя, репутаційна шкода

та втрата стабільності можуть бути результатом кібертероризму. Докладаються глобальні зусилля для підвищення кібербезпеки та зміцнення стійкості критично важливих систем до цих атак, що викликає зростаюче занепокоєння урядів та бізнесу.

В рамках цих зусиль впроваджуються нетехнічні та технічні заходи, такі як навчання персоналу та плани реагування на інциденти. Прикладами технологічних заходів є брандмауери та антивірусне програмне забезпечення. Однак, незважаючи на ці зусилля, кібертероризм продовжує залишатися значною загрозою. Це пов'язано з постійно мінливою природою Інтернету, а також зі зростаючою залежністю від технологій у всіх сферах суспільства через постійно зростаюче використання технологій. Обидва фактори сприяють подальшому існуванню кібертероризму. Щоб захистити себе від цієї загрози, окремі особи та організації повинні залишатися пильними та регулярно оновлювати свої заходи безпеки для захисту від неї.

Таким чином, комплексний аналіз технологічних, соціально-економічних та політико-правових аспектів кібератак свідчить про необхідність формування інтегрованого підходу до забезпечення кібербезпеки. Поєднання технічних інновацій, ефективних інституційних механізмів та міжнародно-правових норм є ключовою передумовою для зміцнення стійкості держав і суспільств до сучасних кіберзагроз.

Список використаних джерел:

1. Kalogeraki E.-M., Papastergiou S., Panayiotopoulos T. An attack simulation and evidence chains generation model for critical information infrastructures. *Electronics*. 2022. Vol. 11. DOI: https://doi.org/10.3390/electronics11030404.

2. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (ECI Directive). *Official Journal of the European Union*. 2008. No. 345. P. 75–82.

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114

3. Polatidis N., Pavlidis M., Mouratidis H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*. 2018. Vol. 56. P. 74–82.

4. Oh S. H., Kim J., Park J. Dynamic cyberattack simulation: integrating improved deep reinforcement learning with the MITRE-ATT&CK framework. *Electronics*. 2024. Vol. 13. DOI: https://doi.org/10.3390/electronics13142831.

5. Завгородня Ю. В. Можливості політики кіберзахисту в зовнішніх та внутрішніх процесах. *Актуальні проблеми філософії та соціології*. 2024. № 48. URL: http://apfs.nuoua.od.ua/archive/48_2024/31.pdf

6. Завгородня Ю. В. Зовнішня політика України у сфері енергетичної безпеки: глобальний та регіональний аспекти. *Актуальні проблеми політики*. Одеса, 2025. Вип. 75. С. 210–215.

7. Ahmad A., Desouza K. C., Maynard S. B., Naseer H., Baskerville R. How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*. 2019. Vol. 71. No. 8. P. 939–953.

8. Akram M. S., Mir M. J., Rehman A. Dimension of cyber-warfare in Pakistan's context. *Journal of Positive School Psychology*. 2023. Vol. 7. No. 6. P. 82–94.

9. Wicki-Birchler D. The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*. 2020. Vol. 1. P. 63–72.

10. Iftikhar S. Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*. 2024. Vol. 10. e1772. DOI: https://doi.org/10.7717/peerj-cs.1772.

11. Schmitt M. N. The use of cyber force and international law. In: Weller M. (ed.). The Oxford Handbook of the Use of Force in International Law. Oxford : Oxford University Press, 2015. DOI: https://doi.org/10.1093/law/9780199673049.003.0053.

12. Schmitt M. N. The use of cyber force and international law. In: Weller M. (ed.). The Oxford Handbook of the Use of Force in International Law. Oxford : Oxford University Press, 2015. DOI: https://doi.org/10.1093/law/9780199673049.003.0053.

13. Feng W. Y. The legal boundaries of cyber warfare. Scientific *Journal of Humanities and Social Sciences*. 2025. Vol. 7. No. 7. P. 154–160. DOI: https://doi.org/10.54691/wn8ffm76.

14. Статут Організації Об'єднаних Націй : міжнародний документ від 26 червня 1945 р. URL: https://www.un.org/en/about-us/un-charter

15. Північноатлантичний договір (Вашингтонський договір) : міжнародний договір від 4 квітня 1949 р. URL: https://www.nato.int/cps/en/natolive/official_texts_17120.htm

16. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, DC : The White House, 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

17. United States International Cyberspace and Digital Policy Strategy: Toward an Innovative, Secure, and Rights-Respecting Digital Future. Washington, DC : United States Department of State, 2024. URL: https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

18. Department of Defense Law of War Manual. Washington, DC : United States Department of Defense, 2015 (updated December 2023). URL: https://media.defense.gov/2023/Dec/13/2003367763/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-DECEMBER-2023.PDF

19. Computer Misuse and Cybercrimes Act, 2018 (No. 5 of 2018) : Act of Parliament of the Republic of Kenya. Nairobi, 2018. URL: https://www.kenyalaw.org/lex/rest/db/kenyalex/Kenya/Legislation/English/Acts/C/Computer%20Misuse%20and%20Cybercrimes%20Act%20No.%205%20of%202018/docs/ComputerMisuseandCybercrimesAct5of2018.pdf

20. Prevention of Electronic Crimes Act, 2016 (PECA) : Act of Parliament of the Islamic Republic of Pakistan. Islamabad, 2016. URL: https://www.pakistani.org/pakistan/legislation/2016/PECA.html

References:

1. Kalogeraki, E.-M., Papastergiou, S., & Panayiotopoulos, T. (2022). An attack simulation and evidence chains generation model for critical information infrastructures. *Electronics*, 11(3). https://doi.org/10.3390/electronics11030404.

2. The Council of the European Union. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (ECI Directive). *Official Journal of the European Union*, L345, 75–82. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114

3. Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, 56, 74–82.

4. Oh, S. H., Kim, J., & Park, J. (2024). Dynamic cyberattack simulation: Integrating improved deep reinforcement learning with the MITRE-ATT&CK framework. *Electronics*, 13, 2831. https://doi.org/10.3390/electronics13142831.

5. Zavgorodnia, Y. V. (2024). Mozhlyvosti polityky kiberzakhystu v zovnishnikh ta vnutrishnikh protsesakh. *Aktualni problemy filosofii ta sotsiolohii*, 48. Retrueved from http://apfs.nuoua.od.ua/archive/48_2024/31.pdf

6. Zavgorodnia, Y. V. (2025). Zovnishnia polityka Ukrainy u sferi enerhetychnoi bezpeky: hlobalnyi ta rehionalnyi aspekty. *Aktualni problemy polityky*, 75, 210–215.

7. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. (2019). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939–953.

8. Akram, M. S., Mir, M. J., & Rehman, A. (2023). Dimension of cyber-warfare in Pakistan's context. *Journal of Positive School Psychology*, 7(6), 82–94.

9. Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? *International Cybersecurity Law Review*, 1, 63–72.

10. Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science*, 10, e1772. https://doi.org/10.7717/peerj-cs.1772.

11. Schmitt, M. N. (2015). The use of cyber force and international law. In M. Weller (Ed.), The Oxford Handbook of the Use of Force in International Law. Oxford : Oxford University Press. https://doi.org/10.1093/law/9780199673049.003.0053.

12. Schmitt, M. N. (2015). The use of cyber force and international law. In M. Weller (Ed.), The Oxford Handbook of the Use of Force in International Law. Oxford : Oxford University Press. https://doi.org/10.1093/law/9780199673049.003.0053.

13. Feng, W. Y. (2025). The legal boundaries of cyber warfare. *Scientific Journal of Humanities and Social Sciences*, 7(7), 154–160. https://doi.org/10.54691/wn8ffm76.

14. United Nations. (1945). Charter of the United Nations. https://www.un.org/en/about-us/un-charter

15. North Atlantic Treaty Organization. (1949). The North Atlantic Treaty (Washington Treaty). https://www.nato.int/cps/en/natolive/official_texts_17120.htm

16. The White House. (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, DC. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

17. United States Department of State. (2024). United States International Cyberspace and Digital Policy Strategy: Toward an Innovative, Secure, and Rights-Respecting Digital Future. Washington, DC. https://www.state.gov/wp-content/uploads/2024/07/United-States-

International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

18. Department of Defense. (2023). Department of Defense Law of War Manual. Washington, DC: U.S. Department of Defense. https://media.defense.gov/2023/Dec/13/2003367763/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-DECEMBER-2023.PDF

19. Republic of Kenya. (2018). Computer Misuse and Cybercrimes Act (No. 5 of 2018). https://www.kenyalaw.org/lex/rest/db/kenyalex/Kenya/Legislation/English/Acts/C/Computer%20Misuse%20and%20Cybercrimes%20Act%20No.%205%20of%202018/docs/ComputerMisuseandCybercrimesAct5of2018.pdf

20. Islamic Republic of Pakistan. (2016). Prevention of Electronic Crimes Act (PECA). https://www.pakistani.org/pakistan/legislation/2016/PECA.html

ПОНЯТТЯ, ОЗНАКИ ТА ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ФІНАНСОВИХ САНКЦІЙ У МИРНИЙ ПЕРІОД ТА В УМОВАХ ВОЄННОГО СТАНУ

CONCEPT, SIGNS, AND FEATURES OF LEGAL REGULATION OF FINANCIAL SANCTIONS IN PEACETIME AND UNDER MARTIAL LAW

Ivanskyy A. Y.,
Doctor of Law, Professor, Honored Lawyer of Ukraine,
Master of European Law (Austria),
Lawyer's Office in Vienna
Vienna, Austria

Abstract. The monographic study is devoted to a comprehensive theoretical and applied analysis of the concept, features, and peculiarities of the legal regulation of financial sanctions in peacetime and under martial law. The relevance of the research is due to the ongoing transformation of financial law under conditions of systemic crises, in particular those related to military aggression, which necessitates a rethinking of the legal nature of these measures, their functional purpose, and the limits of permissible state interference in the property sphere of an individual. The absence of a unified doctrinal and legislative approach to defining financial sanctions, as well as the fragmentation of their legal regulation across tax, budgetary, banking, currency, and sanctions legislation, further complicates the formation of a coherent legal model of this

institution. This fragmentation also leads to inconsistencies in law enforcement practice, which, in turn, undermines legal certainty and complicates the predictability of state intervention.

Particular attention is paid to the constitutional foundations of the said instruments, including the principles of the rule of law, protection of property rights, legal certainty, proportionality, and the guarantee of judicial protection. These principles function not only as formal legal benchmarks but also as substantive limits that define the permissible limits of state intervention in the sphere of private property interests. The study emphasizes that financial sanctions inherently involve a significant degree of interference with property rights and economic freedom; therefore, their application must comply with strict legal standards and be subject to effective judicial control. In this regard, the research highlights the growing importance of procedural guarantees, proper reasoning of decisions, and the availability of remedies for challenging sanction measures [1; 2].

The subject of the study is the system of legal relations arising in connection with the establishment, application, and implementation of the said instruments in Ukraine, as well as doctrinal approaches to their understanding and comparative legal frameworks of their regulation in peacetime and under martial law. The subject also encompasses the interaction between financial sanctions and related legal institutions, including financial control measures, security measures, and restrictive measures in the field of national security.

The purpose of the study is to develop a holistic theoretical concept of financial sanctions as a legal institution, to identify their essential features and functional characteristics, and to determine the specific patterns of their legal regulation in different legal regimes — peacetime and martial law. The research also aims to substantiate the transformation of these measures from a predominantly reactive form of liability into a proactive instrument of financial governance and

security, as well as to formulate proposals for improving legislation and legal practice.

It is concluded that financial sanctions in the contemporary legal order should be conceptualized as a complex, hybrid institution that combines elements of legal liability, regulatory intervention, and security policy. The effectiveness of such an approach depends on the institutional capacity of public authorities, the quality of legal regulation, and the level of coordination between regulatory, supervisory, and law enforcement bodies. Their evolution under martial law reflects a broader transformation of financial law toward risk-based and security-oriented regulation. At the same time, this transformation must remain within the limits defined by the principles of legality, legal certainty, proportionality, good governance, and effective judicial control [1; 3]. Ensuring a balance between state interests in financial security and the protection of individual rights is identified as the key condition for the legitimacy of the sanctions mechanism.

The findings of the study may be used for further doctrinal development of financial law, improvement of legislation on these measures, and enhancement of law enforcement and judicial practice in both peacetime and emergency conditions.

Keywords: Financial Sanctions, Legal Regulation, Martial Law, Peacetime Period, Economic Security, Sanctions Policy.

1. Вступ

Сучасний розвиток фінансового права характеризується суттєвим ускладненням правових механізмів державного впливу на економічні процеси, обумовлено як глобалізаційними трансформаціями, так і внутрішніми викликами, пов'язаними з необхідністю забезпечення фінансової стабільності, бюджетної дисципліни та економічної безпеки держави. У сучасних умовах фінансові

інструменти державного впливу дедалі частіше набувають комплексного характеру, поєднуючи елементи регуляторного, контрольного та примусового впливу. Це, своєю чергою, зумовлює необхідність переосмислення традиційних підходів до їх класифікації та правової природи. У цьому контексті особливого значення набувають фінансові санкції як інструмент публічно-владного впливу, спрямований на забезпечення належного функціонування системи публічних фінансів [4].

Фінансові санкції посідають особливе місце в системі правових засобів державного регулювання, оскільки поєднують у собі ознаки юридичної відповідальності, державного примусу та регуляторного впливу. Ці заходи застосовуються у різних сферах фінансових правовідносин (податковій, бюджетній, банківській, валютній, сфері фінансового моніторингу) та виконують не лише каральну, але й превентивну, компенсаційну та стабілізаційну функції [5]. До таких сфер, зокрема, належать податкові правовідносини (штрафи, пені), бюджетні правопорушення (заходи впливу за порушення бюджетного законодавства), валютне регулювання (санкції за порушення валютних операцій), а також сфера фінансового моніторингу.

Разом із тим, відсутність єдиного законодавчо закріпленого підходу до визначення фінансових санкцій, їх правової природи та місця в системі права обумовлює наявність значних доктринальних дискусій [1]. Нормативне регулювання цього інституту характеризується фрагментарністю, що ускладнює його системне сприйняття та практичне застосування [2]. Це проявляється у відсутності єдиного кодифікованого акту, який би системно визначав підстави, види, порядок застосування та оскарження фінансових санкцій. Особливої гостроти ці проблеми набувають в умовах воєнного стану, коли фінансові санкції трансформуються із класичного

інструменту відповідальності у складову механізму забезпечення національної безпеки [6].

Воєнний стан спричиняє якісні зміни у правовому регулюванні фінансових відносин, у тому числі, у підходах до застосування санкцій. Зокрема, відбувається зміщення акценту з каральної функції на превентивну та безпекову, що відповідає загальній тенденції сек'юритизації фінансового права.

У таких умовах фінансові санкції дедалі частіше використовуються не лише як реакція на вже вчинене правопорушення, а як засіб попередження ризиків, обмеження економічної діяльності суб'єктів, пов'язаних із державою-агресором, а також для забезпечення стабільності фінансової системи та запобігання загрозам економічній безпеці держави [2; 6]. Особливого значення набуває ризикорієнтований підхід до застосування фінансових санкцій, який відповідає міжнародним стандартам FATF [7]. Такий підхід передбачає оцінку не лише факту правопорушення, а й потенційної загрози фінансовій системі, що суттєво розширює межі застосування санкційних заходів. У зв'язку з цим змінюється не лише функціональне призначення фінансових санкцій, а й їх правова природа, що потребує ґрунтовного наукового осмислення.

Водночас розширення дискреційних повноважень органів державної влади у сфері застосування фінансових санкцій актуалізує питання дотримання принципів верховенства права, правової визначеності та пропорційності втручання у майнову сферу особи [3; 4; 8]. Саме баланс між публічним інтересом та захистом прав суб'єктів господарювання є ключовим критерієм легітимності санкційного механізму в умовах як мирного часу, так і воєнного стану. Недотримання цього балансу може призвести до надмірного втручання держави у господарську діяльність та порушення принципу справедливості.

У структурному відношенні дослідження побудоване таким чином, щоб забезпечити послідовне розкриття як теоретичних, так і прикладних аспектів правового регулювання фінансових санкцій. Розглядаються: теоретико-методологічні основи фінансових санкцій, зокрема їх поняття, ознаки та місце в системі фінансового права; правова природа фінансових санкцій та їх відмежування від суміжних правових інститутів; трансформація правового режиму фінансових санкцій у зв'язку із запровадженням воєнного стану, а також визначаються межі допустимого втручання держави у фінансову сферу; міжнародний досвід та судова практика тощо.

Метою дослідження є комплексний аналіз правової природи фінансових санкцій, визначення їх ознак, функцій та місця в системі права, а також виявлення особливостей їх правового регулювання у мирний період та в умовах воєнного стану. *Методологічну основу дослідження* становить сукупність загальнонаукових і спеціально-юридичних методів. Діалектичний метод використано для аналізу розвитку фінансових санкцій як динамічного правового явища. Формально-юридичний метод застосовано для тлумачення норм законодавства [4; 9]. Порівняльно-правовий метод дав змогу зіставити національне регулювання із міжнародними стандартами [2; 7; 9; 10]. Системний метод дозволив розглянути фінансові санкції як елемент цілісної правової системи.

2. Теоретико-методологічні основи фінансових санкцій

2.1. Поняття та юридична природа фінансових санкцій

Однією з фундаментальних проблем сучасної науки фінансового права є відсутність єдиного, доктринально усталеного та законодавчо уніфікованого підходу до визначення поняття фінансових санкцій, їх місця у системі юридичної відповідальності, а також до розмежування цього інституту з іншими формами

державного примусу у сфері публічних фінансів. Ускладнення зумовлене насамперед тим, що чинне законодавство України не містить універсальної дефініції фінансових санкцій, натомість використовує суміжні або галузево фрагментовані конструкції: «штрафні (фінансові) санкції», «пеня», «заходи впливу», «заходи захисту», «блокування активів», «обмеження фінансових операцій», «зупинення операцій», «санкції», «особливі економічні та інші обмежувальні заходи». Таке нормативне розмаїття зумовлює необхідність побудови ширшої наукової конструкції, здатної поєднати фінансово-правові, адміністративно-правові та безпекові аспекти санкційного впливу [1; 3; 5]. При цьому слід враховувати, що різні законодавчі конструкції відображають не лише термінологічні відмінності, але й різну функціональну спрямованість відповідних заходів, що ускладнює їх узгодження в межах єдиної теоретичної моделі.

Разом із тим слід зауважити, що фрагментарність нормативного регулювання призводить не лише до термінологічної невизначеності, але й до різної правозастосовної практики, що ускладнює забезпечення принципу правової визначеності та передбачуваності санкційного впливу [4]. На практиці це може призводити до ситуацій, коли ідентичні за змістом правопорушення тягнуть різні правові наслідки залежно від галузевої належності правовідносин.

Конституційне підґрунтя дослідження фінансових санкцій визначається насамперед статтями 8, 41, 55, 64 і 67 Конституції України. Саме ці приписи задають базові координати аналізу: верховенство права, захист права власності, гарантованість судового захисту, допустимість лише законних і тимчасових обмежень прав в умовах воєнного стану та загальний обов'язок кожного сплачувати податки й збори у порядку і розмірах, встановлених законом [3]. Отже, проблема фінансових санкцій не є лише спеціально-галузевою; вона безпосередньо пов'язана з конституційними межами втручання

держави у майнову сферу особи та з допустимими межами публічного примусу в демократичній правовій державі.

Зазначене набуває особливої актуальності у світлі практики Європейського суду з прав людини, який послідовно підкреслює необхідність забезпечення справедливого балансу між публічним інтересом і правами особи у випадках втручання в майнову сферу [8].

У вітчизняній доктрині фінансового права простежуються щонайменше три концептуальні підходи до розуміння правової природи фінансових санкцій. Перший підхід зводить їх до різновиду фінансово-правової відповідальності, тобто до негативних майнових наслідків, які застосовуються за порушення фінансово-правових обов'язків. Другий підхід розглядає фінансові санкції як особливу форму державного примусу у сфері публічних фінансів, що ширша за класичну відповідальність і охоплює також превентивні та забезпечувальні форми впливу. Третій, найбільш адекватний сучасному стану правового регулювання, полягає в інтерпретації фінансових санкцій як комплексного інструменту фінансово-правового регулювання, кризового управління та фінансової безпеки. Саме третій підхід, на мою думку, найповніше відображає реалії воєнного часу, коли санкція дедалі частіше функціонує не лише як реакція на порушення, а як механізм випереджального блокування ризиків. Його перевага полягає також у здатності інтегрувати нові інструменти фінансового впливу, які не вкладаються у класичну модель юридичної відповідальності.

За таких умов фінансові санкції доцільно визначати як передбачені законом заходи майнового, організаційно-обмежувального або публічно-владного впливу, що застосовуються уповноваженими суб'єктами у сфері публічних фінансів, фінансового контролю, валютного регулювання, банківського нагляду, фінансового моніторингу та фінансової безпеки держави з метою припинення правопорушень, відновлення порушеного фінансового правопорядку,

попередження ризиків для бюджетної, податкової, валютної та банківської системи, а також забезпечення економічного суверенітету й національної безпеки держави. Така дефініція дозволяє охопити як традиційні, так і новітні форми санкційного впливу, що виникають у зв'язку з цифровізацією фінансової системи та розвитком глобальних фінансових ринків.

Варто підкреслити, що таке розширене розуміння фінансових санкцій дозволяє охопити не лише традиційні інструменти податкового впливу, а й сучасні механізми фінансового моніторингу, включаючи замороження активів, обмеження доступу до фінансових ресурсів та інші заходи, що застосовуються у межах міжнародних санкційних режимів.

Правова природа фінансових санкцій у сучасному правопорядку є складною, багаторівневою та міжгалузевою. Її неможливо коректно описати в межах лише однієї категорії — «покарання», «відповідальність», «заходи контролю» або «обмеження». У матеріальному сенсі фінансові санкції поєднують щонайменше чотири функціональні виміри: каральний, компенсаційний, превентивний і регуляторно-безпековий. У науковій літературі ці функції нерідко перетинаються, утворюючи змішані форми правового впливу, що ускладнює їх однозначну класифікацію [1; 5].

При цьому співвідношення зазначених функцій не є статичним і змінюється залежно від правового режиму: у мирний період домінує карально-компенсаційний елемент, тоді як в умовах воєнного стану та фінансової нестабільності пріоритет набувають превентивні та безпекові функції.

У класичній податковій або бюджетній моделі санкція виникає як наслідок уже вчиненого порушення; натомість у санкційному режимі воєнного стану або в системі фінансового моніторингу вона дедалі частіше виконує функцію випереджального фінансового стримування, спрямованого на недопущення

використання фінансової системи у шкоду державі, суспільству чи міжнародній безпеці [6].

Саме тому юридична природа фінансових санкцій у XXI столітті дедалі більше визначається не лише через класичні категорії відповідальності, а й через доктринальні конструкції фінансової стабільності, risk-based regulation, good governance, financial resilience та economic security law. Така трансформація відповідає загальносвітовій тенденції переходу від реактивного до превентивного регулювання фінансових відносин.

Зазначений підхід корелює з практикою Суду Європейського Союзу, який у справах щодо обмежувальних заходів наголошує на їх регуляторному, а не каральному характері, а також на необхідності дотримання принципів пропорційності та ефективного судового контролю [9; 10].

Отже, фінансові санкції в сучасному українському правопорядку слід розглядати як комплексний міжгалузевий інститут, що поєднує ознаки фінансово-правової відповідальності, державного примусу, макрофінансового регулювання та економіко-безпекового управління. Саме ця багатошаровість обумовлює складність їх правового регулювання та призводить до потреб в систематизації законодавства, доктринальному уточненні понятєвий апарату і побудові єдиної моделі тлумачення і застосування санкцій у мирний і воєнний періоди.

2.2. Ознаки фінансових санкцій як самостійного правового інституту

Для теоретично коректного осмислення інституту фінансових санкцій недостатньо лише сформулювати його дефініцію. Не менш важливо виокремити системоутворюючі ознаки, які дозволяють відмежувати фінансові санкції від суміжних правових явищ та обґрунтувати їх як самостійний інститут сучасного фінансового права. У цьому контексті доцільно виділити щонайменше вісім основних ознак. При цьому слід враховувати, що наведені ознаки

мають не ізольований, а взаємопов'язаний характер, утворюючи цілісну конструкцію, яка забезпечує внутрішню узгодженість інституту фінансових санкцій та його відмежування від інших форм публічно-владного впливу [1; 5].

По-перше, фінансові санкції мають майновий або економічно-обмежувальний характер. Навіть якщо окремі санкції формально виражаються не в прямому стягненні коштів, а в блокуванні активів, обмеженні доступу до рахунків, зупиненні операцій або забороні розпорядження майном, усі вони так чи інакше спрямовані на економічну сферу адресата. Саме через майновий елемент санкційний примус проявляється найчіткіше. При цьому ступінь такого впливу може варіюватися від незначних фінансових втрат до повного блокування економічної діяльності суб'єкта.

Ця ознака набуває особливого значення в умовах глобалізації фінансових ринків, де обмеження доступу до фінансових ресурсів або платіжної інфраструктури може мати значно більш відчутні наслідки, ніж класичні штрафні санкції.

По-друге, фінансові санкції мають публічно-владну природу. Це зумовлює необхідність чіткого нормативного визначення меж дискреції органів влади при застосуванні санкцій. Їх застосування ґрунтується не на диспозитивній волі сторін, а на владному рішенні держави або уповноваженого нею суб'єкта. Це принципово відрізняє фінансові санкції від приватноправових штрафних механізмів, договірної неустойки чи інших інструментів цивільноправовий відповідальності. З огляду на це фінансові санкції виступають формою реалізації публічного інтересу у сфері фінансів, що вимагає підвищених стандартів обґрунтованості, прозорості та підконтрольності рішень органів влади [4].

По-третє, фінансові санкції характеризуються спеціальною сферою застосування. Водночас межі цієї сфери поступово розширюються у зв'язку з інтеграцією фінансових і безпекових механізмів. Вони

функціонують не в будь-яких правовідносинах, а саме у сфері податкових, бюджетних, валютних, банківських, санкційних, моніторингових і безпеково-фінансових відносин. Така галузева спеціалізація обумовлює необхідність врахування специфіки кожного сегмента фінансової системи, що, у свою чергу, ускладнює уніфікацію правового регулювання та потребує міжгалузевого підходу [2; 5].

По-четверте, фінансові санкції застосовуються лише спеціально уповноваженими суб'єктами, компетенція яких прямо визначена законом. До таких суб'єктів належать податкові органи, органи державного фінансового контролю, Національний банк України, Держфінмоніторинг, інші фінансові регулятори, а в окремих випадках — Рада національної безпеки й оборони України. Ця ознака забезпечує інституційну визначеність санкційного механізму та виступає гарантією недопущення довільного втручання у фінансову сферу з боку неналежних суб'єктів.

По-п'яте, фінансові санкції пов'язані або з порушенням, або з ризиком порушення фінансового порядку. У класичній мирній моделі домінує перший елемент: санкція є наслідком уже встановленого правопорушення. Проте в умовах воєнного стану та сучасного AML/CFT-регулювання дедалі більшого значення набуває другий елемент — санкційне реагування на ризик. Саме тут проявляється перехід до risk-based підходу, який передбачає можливість застосування обмежувальних заходів ще до настання негативних наслідків, якщо існує обґрунтована загроза фінансовій системі чи національній безпеці. Це означає, що критерії застосування санкцій дедалі більше ґрунтуються на оцінці ризиків, а не лише на факті порушення.

По-шосте, фінансові санкції є багатофункціональними. Така універсальність робить їх одним із ключових інструментів сучасної фінансової політики держави. Вони виконують не лише каральну та компенсаційну, а й превентивну, регуляторну, стабілізаційну та безпекову функції. Функціональна багатовимірність санкцій

дозволяє розглядати їх як універсальний інструмент державної фінансової політики, здатний адаптуватися до різних економічних та правових режимів.

По-сьоме, фінансові санкції мають підвищений ступінь втручання у право власності та економічну свободу особи. Саме тому вони повинні підпорядковуватися суворим вимогам законності, правової визначеності, необхідності, пропорційності та доступності судового контролю. Європейська судова практика, зокрема практика ЄСПЛ і Суду ЄС, підтверджує, що навіть у сфері санкцій держави не звільняються від обов'язку забезпечення ефективного судового захисту та належного обґрунтування обмежень [8; 9; 10].

По-восьме, фінансові санкції завжди передбачають спеціальний процесуальний режим. Недотримання процесуальних вимог може стати підставою для визнання санкції незаконною незалежно від наявності матеріальних підстав. Це означає, що вони застосовуються не довільно, а в межах адміністративної, регуляторної, фінансово-контрольної або змішаної процедури.

Процесуальний аспект санкцій має вирішальне значення, оскільки саме через процедуру реалізуються гарантії прав особи, включаючи право бути вислуханим, право на оскарження та право на ефективний засіб юридичного захисту [4; 8].

Отже, сукупність наведених ознак дає підстави стверджувати, що фінансові санкції є не випадковою сукупністю окремих правових заходів, а самостійним, складним і багатофункціональним правовим інститутом, який має власний предмет регулювання, власну логіку функціонування і специфічне місце у системі сучасного публічного права. Такий підхід дозволяє перейти від фрагментарного сприйняття санкцій до їх системного розуміння як елементу єдиної архітектури фінансового права [1; 5].

2.3. Місце фінансових санкцій у системі фінансового права та юридичної відповідальності

Питання про місце фінансових санкцій у системі права має не лише теоретичне, а й безпосереднє практичне значення. Особливо це проявляється у судовій практиці, де правильна кваліфікація санкції визначає застосовувані стандарти доказування. Від його вирішення залежить визначення підстав застосування санкцій, допустимих меж дискреції, стандартів обґрунтованості рішень, процесуальних гарантій та способів оскарження. Крім того, правильне визначення місця фінансових санкцій впливає на кваліфікацію правовідносин, вибір правозастосовних процедур та визначення юрисдикції судів при розгляді відповідних спорів [4].

У доктринальному сенсі ключовим є з'ясування, чи є фінансові санкції лише різновидом юридичної відповідальності, чи вони утворюють ширший режим публічно-владного впливу у сфері фінансів [5; 11].

Перший підхід, класичний для науки фінансового права, полягає у тому, що фінансові санкції є різновидом фінансово-правової відповідальності. При цьому цей підхід не враховує розвиток превентивних інструментів фінансового контролю. У межах цього підходу санкція розуміється як негативний наслідок порушення фінансового обов'язку, який покладається на правопорушника з метою покарання та відновлення порушеного публічного фінансового інтересу.

Перевагою цього підходу є його чіткість і визначеність, однак він не дозволяє повною мірою пояснити сучасні санкційні механізми, що не пов'язані безпосередньо з фактом правопорушення [11].

Другий підхід трактує фінансові санкції як особливу форму державного примусу у сфері публічних фінансів, що не вичерпується межами класичної відповідальності. Це вимагає встановлення чітких меж між санкційними та несакційними формами примусу.

Цей підхід дозволяє ширше охопити регуляторні інструменти впливу, однак водночас створює ризик надмірного розширення поняття фінансових санкцій, що може негативно вплинути на принцип правової визначеності [5].

Третій підхід, який, на нашу думку, є найбільш переконливим в умовах воєнного стану, полягає в розумінні фінансових санкцій як комплексного інструменту фінансово-правового регулювання, відповідальності та безпеки, що функціонує на перетині фінансового права, адміністративного права, банківського регулювання, AML/CFT, санкційного законодавства та права національної безпеки.

Саме цей підхід дозволяє пояснити сучасну трансформацію санкцій як інструменту не лише реагування, а й превентивного управління фінансовими ризиками, що особливо актуально в умовах воєнного стану та глобальних економічних викликів.

Отже, у системі фінансового права фінансові санкції займають особливе, міжгалузево опосередковане, але системно пов'язане з публічними фінансами місце. Вони поєднують матеріально-правовий елемент, процесуальний елемент, інституційний елемент і функціональний елемент.

Таке багатовимірне положення фінансових санкцій зумовлює необхідність їх розгляду не лише як інструменту відповідальності, але і як ключового елементу механізму забезпечення фінансової стабільності та економічної безпеки держави.

У зв'язку з цим фінансові санкції є одним із ключових механізмів забезпечення фінансової дисципліни, бюджетної стійкості, податкової стабільності, контролю за фінансовими потоками та загальної керованості публічних фінансів у мирний і воєнний час.

У цьому контексті фінансові санкції виступають важливим елементом державної політики у сфері фінансового суверенітету, що набуває особливого значення в умовах зовнішніх загроз та економічної нестабільності.

3. Правова природа та межі відмежування фінансових санкцій

Однією з найскладніших проблем правозастосування є нечіткість меж між власне фінансовими санкціями та суміжними правовими засобами державного впливу. У мирний час ця проблема має переважно доктринальне значення, однак в умовах воєнного стану вона набуває безпосередньої практичної ваги, оскільки від правильної кваліфікації залежить і вибір процедури застосування заходу, і межі дискреції органу, і характер судового контролю [4; 6]. Це пов'язано з тим, що помилкова кваліфікація може призвести до порушення процесуальних прав особи.

Особливої актуальності ця проблема набуває в умовах розширення повноважень органів публічної влади, коли спрощення процедур та підвищення швидкості реагування можуть призводити до змішування контрольних, забезпечувальних і санкційних механізмів у межах одного правозастосовного рішення. У таких умовах зростає ризик підміни правових підстав застосування заходів, що, своєю чергою, може негативно впливати на гарантії прав суб'єктів господарювання та ефективність судового захисту [3; 4; 6].

Передусім фінансові санкції слід відмежовувати від заходів фінансового контролю. Їх застосування зазвичай має тимчасовий характер і обмежене конкретною процесуальною метою. Податкова перевірка, камеральний контроль, аудит, бюджетна ревізія, валютний нагляд, due diligence клієнта у фінансовому моніторингу самі по собі санкціями не є. Вони являють собою контрольні процедури, які можуть передувати санкції, бути її підставою або забезпечувати перевірку дотримання законодавства. Санкційного характеру вони набувають лише тоді, коли за їх результатами до суб'єкта застосовується негативний майновий чи організаційно-обмежувальний вплив.

Ключовим критерієм відмежування у цьому випадку є наявність владного припису, спрямованого не лише на встановлення фактичних обставин, а й на безпосереднє обмеження прав чи покладення

додаткового фінансового обов'язку. Саме трансформація результату контролю у формалізоване рішення про відповідальність (наприклад, податкове повідомлення-рішення) є тим моментом, коли контроль переходить у санкцію. До цього етапу діяльність органу залишається в межах превентивної або діагностичної функції держави.

Окремо слід відмежовувати фінансові санкції від забезпечувальних заходів, метою яких є не покарання, а тимчасове недопущення ризиків або забезпечення майбутнього виконання обов'язку. До таких заходів можуть належати тимчасове зупинення операцій, арешт коштів у процесуальному порядку, призупинення розрахунків, тимчасове блокування транзакцій до з'ясування обставин. Такі заходи можуть мати санкційний ефект, але з юридичної точки зору вони відрізняються тимчасовим, забезпечувальним і попереджувальним характером [4; 7].

Крім того у практиці правозастосування нерідко виникають ситуації, коли забезпечувальні заходи фактично виконують каральну функцію через їх тривалість або інтенсивність. У таких випадках особливого значення набуває принцип пропорційності, який вимагає співвіднесення втручання у майнову сферу суб'єкта із легітимною метою держави. Якщо тимчасовий захід стає надмірним або невиправдано тривалим, він може бути перекваліфікований судом як санкція з відповідними процесуальними наслідками [4; 8; 9].

Найскладнішим є розмежування фінансових санкцій та спеціальних економічних і інших обмежувальних заходів у сфері національної безпеки, передбачених Законом України «Про санкції» [12]. Це пояснюється їх подвійною правовою природою — одночасно фінансовою і безпековою. З формально-юридичної точки зору санкції РНБО, блокування активів, заборона окремих фінансових операцій, обмеження доступу до ресурсів або припинення економічної взаємодії не завжди є класичними фінансовими санкціями у вузькому сенсі, оскільки не обов'язково пов'язані з уже

встановленим фінансовим правопорушенням. Їх підставою можуть бути загроза національній безпеці, пов'язаність із державою-агресором, ризик фінансування терористичної діяльності або участь у схемах обходу санкцій.

Це спричиняє їх особливу правову природу як превентивно-безпекових заходів, що поєднують елементи адміністративного, фінансового та міжнародного права. Вони мають не ретроспективний, а проспективний характер, тобто спрямовані на недопущення шкоди, а не лише на реагування на вже вчинене правопорушення. Саме ця ознака відрізняє їх від класичних фінансово-правових санкцій, які традиційно пов'язуються з юридичною відповідальністю [12].

Окрему увагу слід приділити практиці міжнародних судових інституцій, зокрема Суду Європейського Союзу та Європейського суду з прав людини, які сформували підхід до оцінки обмежувальних заходів через призму фундаментальних прав людини. У справах Kadi та Rosneft було підкреслено необхідність забезпечення ефективного судового контролю навіть щодо заходів безпекового характеру, що підтверджує їх наближення до санкційних механізмів за рівнем втручання у права особи [9; 10].

Тому з наукової точки зору доцільно виходити з такого підходу: фінансові санкції не є тотожними ані заходам фінансового контролю, ані забезпечувальним заходам, ані всім обмежувальним заходам у сфері національної безпеки; однак в умовах воєнного стану між цими інститутами відбувається функціональне зближення, унаслідок чого вони дедалі частіше формують єдиний механізм захисту фінансової безпеки держави [6; 12]. Такий механізм характеризується високим рівнем інтеграції правових інструментів та інституцій.

Таке зближення має системний характер і свідчить про формування інтегрованої моделі фінансово-безпекового регулювання, у межах якої класичні галузеві межі поступово розмиваються. За таких умов важливим завданням юридичної науки є вироблення

чітких критеріїв кваліфікації відповідних заходів, що дозволить забезпечити баланс між ефективністю державного реагування та дотриманням принципу верховенства права, зокрема вимог правової визначеності, пропорційності та належної правової процедури.

4. Трансформація режиму фінансових санкцій: від мирного часу до воєнного стану

4.1. Особливості правового регулювання фінансових санкцій у мирний період

Правовий режим фінансових санкцій у мирний період характеризується відносно стабільною нормативною структурою, вищим рівнем передбачуваності правозастосування та домінуванням класичної моделі юридичної відповідальності. У звичайних умовах санкція функціонує переважно як ретроспективний інструмент державного реагування на вже вчинене порушення. Базова логіка її застосування вибудовується за моделлю: «порушення фінансового обов'язку → встановлення факту порушення → застосування санкції → судовий контроль» [4; 9; 11].

Водночас така модель передбачає чітке розмежування матеріальних і процесуальних елементів відповідальності, що забезпечує належний баланс між публічними інтересами та правами платників. Саме в мирний період найбільш повно реалізуються гарантії процедурної справедливості, зокрема право бути вислуханим, право на оскарження та право на ефективний судовий захист, що формує стійку практику правозастосування [4; 5]. Важливим елементом такої практики є також усталені підходи адміністративних судів до оцінки правомірності податкових повідомлень-рішень та актів фінансового контролю. Зокрема, судова практика виробила критерії перевірки обґрунтованості донарахувань, допустимості доказів, меж дискреції контролюючих органів і стандартів доказування

у податкових спорах. Це забезпечує відносну стабільність інтерпретації фінансово-правових норм.

У такій моделі фінансові санкції мають переважно карально-компенсаційний характер. Їхнє основне призначення полягає у покаранні порушника, відновленні фінансового правопорядку, компенсації втрат публічних фінансів і стимулюванні правомірної поведінки на майбутнє. Саме ця модель найяскравіше проявляється у податкових і бюджетних правовідносинах, де закон досить чітко визначає склад порушення, вид санкції, порядок її застосування, строки, процесуальні форми та інструменти оскарження [5; 9; 11].

Крім того, у мирний період важливу роль відіграє стабільність правових позицій судів, що забезпечує єдність правозастосування та підвищує рівень довіри до фінансово-правових інститутів. Така стабільність дозволяє суб'єктам господарювання прогнозувати наслідки своєї діяльності та мінімізувати правові ризики [4]. У цьому контексті важливу роль відіграє також принцип legitimate expectations (захист обґрунтованих очікувань), який поступово імплементується у національну практику через рішення судів. Він обмежує можливість різкої зміни підходів держави до оцінки поведінки платника податків.

До ключових ознак мирного режиму фінансових санкцій належать: відносно чітка правова визначеність; формалізований характер адміністративних і фінансово-контрольних процедур; домінування концепції відповідальності за правопорушення; відносно нижчий рівень дискреції уповноважених органів; більш усталений судовий контроль. Саме тому в мирний період фінансові санкції найбільш тісно пов'язані з принципом nulla poena sine lege — жодна санкція не може бути застосована інакше як на підставі закону [3; 4; 9].

Цей принцип виступає ключовим гарантом правової визначеності, оскільки виключає можливість довільного розширення підстав відповідальності та забезпечує чіткість нормативного регулювання санкційних механізмів [3; 4].

4.2. Трансформація фінансових санкцій у період воєнного стану

В умовах воєнного стану правове регулювання фінансових санкцій зазнає не просто кількісних змін у вигляді розширення повноважень окремих органів чи збільшення кількості обмежень, а саме якісної трансформації, яка торкається правової природи, функцій, підстав застосування та інституційної архітектури санкційного механізму [6; 12]. Закон України «Про правовий режим воєнного стану» визначає воєнний стан як особливий правовий режим, що передбачає надання органам державної влади, військовому командуванню та військовим адміністраціям повноважень, необхідних для відвернення загрози та забезпечення національної безпеки, а також допускає тимчасове обмеження конституційних прав і свобод із зазначенням строку дії таких обмежень [6].

Це означає, що правове поле фінансових санкцій розширюється за рахунок включення безпекових компонентів, які раніше не були домінуючими, що змінює логіку їх функціонування [3; 6].

Ключова авторська теза полягає в тому, що в період воєнного стану фінансові санкції трансформуються з переважно реактивного механізму фінансово-правової відповідальності у проактивний інструмент кризового фінансового управління та фінансової безпеки держави [6; 11; 12]. У мирний період держава переважно реагує на вже вчинене порушення: несплату податку, порушення бюджетної дисципліни, недотримання валютних правил, порушення банківських нормативів. У воєнний період санкція дедалі частіше застосовується не лише post factum, а й ante factum — на підставі загрози, ризику, підозрілої операції, пов'язаності із підсанкційним середовищем або можливої участі у схемах обходу санкцій [7; 12].

Такий підхід свідчить про перенесення фокусу з юридичної відповідальності на управління ризиками, що є характерною рисою сучасних фінансово-безпекових режимів у глобальному

контексті [7]. Аналогічні тенденції простежуються у практиці Європейського Союзу та Сполучених Штатів, де фінансові санкції застосовуються як інструмент стратегічного стримування, зокрема через механізми OFAC, санкційні списки ЄС та вторинні санкції. Це свідчить про глобальну уніфікацію підходів до санкцій як елементу фінансової безпеки.

Першим проявом такої трансформації є **зміщення акценту з покарання на захист фінансової безпеки**. Якщо в мирний час санкція покликана передусім відновити порушений фінансовий порядок і компенсувати втрати публічних фінансів, то в умовах війни її головне призначення полягає у запобіганні відтоку капіталу, блокуванні ресурсної бази агресора, недопущенні використання фінансової системи для підривної діяльності, забезпеченні бюджетної та валютної стабільності, збереженні платоспроможності банківського сектору і підтриманні керованості публічних фінансів. Відтак санкція в умовах війни набуває ознак не лише фіскального чи карального, а й **оборонного правового інструменту** [2; 12; 13].

У такому разі фінансові санкції стають складником економічної оборони держави, що об'єднує фінансове право з правом національної безпеки та міжнародним санкційним правом [2; 10].

Другим проявом є **посилення превентивної функції**. У мирний період превенція є допоміжним елементом санкційної системи, тоді як у період воєнного стану вона набуває центрального значення. Законодавство про санкції, валютне регулювання та фінансовий моніторинг функціонує таким чином, щоб держава могла реагувати на ризик ще до настання незворотних негативних наслідків. У цій площині особливо важливу роль відіграє Закон України № 361-IX [14], який будує систему фінансового моніторингу на ризикоорієнтованому підході, а міжнародні стандарти FATF прямо закріплюють risk-based approach як основу сучасного targeted financial sanctions framework. Отже, превенція в сучасному

санкційному праві перестає бути факультативною і стає конструктивною характеристикою самого інституту [7].

Превентивний характер санкцій дозволяє державі діяти на випередження, що особливо важливо в умовах гібридних загроз та фінансових операцій, які можуть мати латентний характер і проявлятися із запізненням [7].

Третім проявом трансформації є **розширення дискреційних повноважень**. Воєнний стан об'єктивно потребує більшої оперативності державного реагування, а отже — ширшого розсуду органів, які ухвалюють санкційні рішення або забезпечують їх виконання. Це проявляється у більш активній ролі РНБО, Президента України, Національного банку України, Держфінмоніторингу, податкових і митних органів, а також у посиленні ролі підзаконного регулювання та індивідуальних актів. Крім того розширення дискреції є двоєдиним явищем: з одного боку, воно забезпечує гнучкість і швидкість реагування; з іншого — створює підвищені ризики правової невизначеності, overreach, надмірного обмеження прав та різнотлумачення критеріїв «ризику», «загрози», «пов'язаності», «обходу санкцій» тощо. З огляду на це в умовах війни дискреція повинна компенсуватися посиленими вимогами до мотивування, внутрішнього контролю та судового перегляду [6; 13].

Однак розширення дискреції водночас підвищує ризики неоднакового застосування норм та зловживань, що вимагає підсилення механізмів внутрішнього контролю, прозорості та обґрунтованості рішень [4; 8].

Четвертим проявом є **посилення ролі приватного сектору**. У сучасній санкційній архітектурі банки, небанківські фінансові установи, суб'єкти первинного фінансового моніторингу, комплаєнс-підрозділи та оператори ринкової інфраструктури вже не є лише пасивними виконавцями державних рішень. Вони фактично перетворюються на функціональних співвиконавців

санкційної політики держави. У воєнний період саме через банківський сектор, AML/CFT-процедури, транзакційний моніторинг і системи перевірки контрагентів реалізується значна частина практичного санкційного впливу. У цьому сенсі формується нова модель **distributed enforcement**, у якій держава встановлює правову рамку, а приватний сектор забезпечує її операційну реалізацію. Така модель зближує українську практику з підходами ЄС і США, де compliance architecture давно є невід'ємною частиною санкційного режиму [7; 15].

Це формує нову модель «розподіленого правозастосування», у межах якої приватні суб'єкти виконують квазірегуляторні функції, що змінює класичне розуміння меж публічної влади у фінансовій сфері [7; 15].

П'ятим проявом виступає **інтеграція санкцій з механізмами національної безпеки**. У мирний період фінансові санкції здебільшого мають внутрішньофінансову або фіскальну спрямованість. У період війни вони вбудовуються у ширший механізм економічної оборони, контррозвідувального захисту, міжнародного тиску на агресора, захисту критичної інфраструктури та забезпечення фінансової стійкості держави. У результаті санкція перестає бути лише технікою фінансового примусу й набуває значення **елемента обороноздатності держави**, що безпосередньо впливає на структуру її правового режиму [12]. В українських умовах це проявляється, зокрема, у синхронізації національних санкцій із міжнародними режимами, що підсилює їх ефективність і водночас ускладнює правозастосування через необхідність врахування зовнішніх джерел регулювання.

У результаті санкції перестають бути ізольованим інструментом фінансового примусу та перетворюються на елемент комплексної стратегії державної безпеки, що охоплює економічний, фінансовий і міжнародно-правовий виміри [2; 12].

Отже, еволюція санкційного механізму у період воєнного стану має системний характер і охоплює одночасно функції, підстави застосування, інституційний склад і ступінь дискреції.

Це дозволяє говорити про формування окремого, спеціального правового режиму фінансових санкцій воєнного часу, який не може бути повністю пояснений через категорії мирного правопорядку [6; 11].

4.3. Порівняльна характеристика фінансових санкцій у мирний період та в умовах воєнного стану

Для цілісного наукового осмислення трансформації фінансових санкцій доцільно порівняти їх правовий режим у мирний період та під час воєнного стану за ключовими критеріями, що дозволяють виявити не лише формальні відмінності, а й глибинні зміни у самій логіці санкційного регулювання. Відповідна концепція дає змогу простежити еволюцію фінансових санкцій від інструменту юридичної відповідальності до елементу системи забезпечення фінансової безпеки держави [6; 11].

У мирний період функціональне призначення фінансових санкцій визначається передусім їх карально-компенсаційною природою. Санкція є наслідком уже вчиненого правопорушення і спрямована на відновлення порушеного фінансового порядку, відшкодування шкоди та формування належної поведінки у майбутньому [5; 9]. У період воєнного стану відбувається істотне зміщення акцентів: санкції набувають превентивного, регуляторного та безпекового змісту, дедалі частіше виконуючи функцію запобігання загрозам, а не лише реагування на них [6; 12].

У цьому контексті змінюється і критерій ефективності санкції: якщо раніше він визначався здатністю відновити порушений стан, то в умовах війни ключовим стає здатність запобігати негативним наслідкам для фінансової системи та держави в цілому [6; 7].

Аналогічна трансформація простежується у підставах застосування санкцій. У мирний період такою підставою виступає встановлений факт порушення фінансового законодавства, що підтверджується у визначеній процедурі [9]. В умовах воєнного стану підстави значно розширюються і включають не лише правопорушення, а й ризик, загрозу національній безпеці, пов'язаність із підсанкційними суб'єктами або підозрілі фінансові операції [7; 12; 14].

Це означає, що поряд із доказуванням факту правопорушення суттєво зростає роль аналітичних інструментів, оцінки ризиків та прогнозування поведінки суб'єктів, що наближає санкційне право до моделей управління ризиками, характерних для міжнародних фінансових стандартів [7]. У зв'язку з цим змінюється і характер доказування: поряд із традиційними доказами правопорушення дедалі більшого значення набувають аналітичні звіти, фінансові профілі, транзакційні патерни та індикатори ризику, що не завжди мають класичну доказову форму.

Ступінь формалізації процедур також зазнає змін. Мирний період характеризується відносно чіткими процедурами, визначеними строками, усталеними формами рішень та передбачуваними механізмами оскарження [4]. У воєнний період спостерігається тенденція до спрощення процедур і підвищення оперативності прийняття рішень, що супроводжується зростанням ролі оцінювальний понять і risk-based підходів [6; 7].

Хоча така гнучкість є функціонально необхідною, вона разом із тим створює напругу між ефективністю державного реагування та вимогами правової визначеності, що потребує додаткових гарантій передбачуваності правозастосування [4].

Суттєвою відмінністю є і рівень дискреції уповноважених органів. У мирний період дискреційні повноваження обмежені законом і практикою його застосування, що забезпечує відносну стабільність правових рішень [4; 11]. У період воєнного стану дискреція

об'єктивно розширюється, охоплюючи як державні органи, так і приватних учасників санкційного механізму — банки, фінансові установи, суб'єктів фінансового моніторингу [7; 15].

Крім того розширення дискреції змінює саму природу правозастосування, перетворюючи його з формалізованої діяльності на процес прийняття управлінських рішень в умовах невизначеності, що підвищує вимоги до обґрунтованості та прозорості таких рішень. Це також означає зміну ролі правозастосувача: від формального інтерпретатора норми до суб'єкта, який здійснює оцінку складних економічних і поведінкових моделей.

Інтенсивність втручання у права особи також істотно різниться. У мирний період санкції здебільшого мають обмежений майновий характер — штрафи, пені, окремі фінансові обмеження. У воєнний період вони можуть набувати значно більшого масштабу, включаючи блокування активів, обмеження доступу до фінансових ресурсів, припинення економічної діяльності.

Це призводить до якісного зростання рівня втручання у право власності та економічну свободу, що, у свою чергу, вимагає застосування більш жорстких стандартів перевірки їх правомірності, насамперед через принцип пропорційності.

Роль судового контролю у цій системі також зазнає трансформації. У мирний період він виконує функцію класичного механізму перевірки законності рішень [4]. У воєнний період його значення істотно зростає, оскільки саме суд має компенсувати розширення дискреції та спрощення процедур [4; 8].

Судовий контроль у таких умовах набуває більш змістовного характеру, охоплюючи не лише формальну законність, а й оцінку меж розсуду, обґрунтованість втручання та відповідність заходу поставленій меті [7].

У підсумку порівняльний аналіз свідчить, що відмінності між мирним і воєнним режимами полягають не лише у масштабі

застосування санкцій, а у зміні їх юридичної природи. Відбувається перехід від реактивної моделі, заснованої на відповідальності за правопорушення, до проактивної моделі, орієнтованої на управління ризиками та забезпечення фінансової безпеки держави [6; 8]. Ключові емпіричні індикатори цієї трансформації та відповідні тенденції правозастосування узагальнено в Додатку 1.

Слід зазначити, що така трансформація не означає відмову від принципів верховенства права, а лише змінює механізми їх реалізації в умовах підвищеної правової та безпекової складності [3; 4].

4.4. Особливості правового режиму фінансових санкцій у воєнний період: межі допустимої трансформації

Попри об'єктивну необхідність посилення санкційного механізму в умовах війни, його трансформація не може бути безмежною. Воєнний стан не скасовує фундаментальних засад правової держави, а лише допускає тимчасову модифікацію правового режиму за умов, визначених Конституцією та законом. Саме тому санкційний режим воєнного часу повинен розглядатися як режим підвищеної гнучкості, але не режим юридичної вседозволеності [3; 6]. Такий підхід відповідає конституційній моделі обмеження прав, яка передбачає, що навіть у надзвичайних умовах держава залишається зв'язаною правом і не може діяти поза межами правового поля.

З огляду на це ключовим завданням є не лише забезпечення ефективності санкцій, а й збереження їх легітимності через дотримання базових правових принципів [3].

Принцип законності залишається базовою вимогою санкційного регулювання. Жодна фінансова санкція не може застосовуватися без належної правової підстави. Умови війни не дають державі права довільно втручатися у фінансову сферу без достатнього нормативного підґрунтя. До того, чим інтенсивнішим є санкційне втручання, тим вищими мають бути вимоги до законодавчої

визначеності його підстав, меж і наслідків. Зогляду на це важливо, щоб підзаконне регулювання залишалося вторинним щодо закону, а не фактично підміняло його [3; 6].

Особливої ваги набуває питання співвідношення закону та підзаконного регулювання, оскільки розширення останнього не повинно призводити до фактичного створення нових санкцій поза межами законодавчої процедури [3].

Не менш важливим є принцип правової визначеності. Суб'єкти господарювання, банки, інвестори та інші учасники фінансового ринку повинні мати можливість хоча б у розумних межах передбачити правові наслідки своєї поведінки. Воєнний стан не скасовує потреби в ясності правових норм. Навпаки, в умовах кризи вимога legal certainty стає ще більш значущою, оскільки саме дефіцит визначеності стимулює over-compliance, регуляторну паніку та зниження довіри до правового середовища [4].

Недостатній рівень визначеності призводить до явища over-compliance, коли суб'єкти уникають навіть правомірних операцій через страх санкцій, що негативно впливає на економічну активність та фінансову стабільність [7]. У довгостроковій перспективі це може призводити до звуження фінансових ринків, зменшення інвестиційної активності та підвищення вартості фінансових ресурсів.

Принцип пропорційності виступає центральним критерієм допустимості санкційного втручання. Будь-яке втручання у майнову сферу має бути співмірним із метою, яку переслідує держава. Це означає, що санкція повинна бути придатною для досягнення цієї мети, необхідною та такою, що не покладає на особу явно надмірного тягаря. Саме принцип пропорційності є центральним критерієм допустимості сучасних фінансових санкцій і спільним ядром українського, європейського та міжнародного санкційного підходу. У сфері інтенсивних майнових обмежень без пропорційності санкція втрачає легітимність [8; 9].

У контексті воєнного стану це означає необхідність ретельного балансування між інтересами безпеки та правами суб'єктів, оскільки надмірне втручання може підривати довіру до держави не менше, ніж недостатнє реагування на загрози [8].

Принцип належного врядування вимагає, щоб органи державної влади діяли обґрунтовано, послідовно, передбачувано, без свавілля та з дотриманням мінімальних стандартів процедурної справедливості. Санкційне рішення не може бути легітимним лише тому, що воно політично доцільне або адміністративно зручне. Воно має бути мотивованим, внутрішньо несуперечливим і прийнятим уповноваженим суб'єктом у визначеній процедурі. Особливу вагу цей принцип має там, де санкція спирається на оцінку ризику або конфіденційну безпекову інформацію [4].

Цей принцип набуває особливого значення у випадках, коли санкційні рішення базуються на оцінці ризиків або інформації з обмеженим доступом, що потребує додаткових гарантій від свавілля [4].

Нарешті, принцип ефективного судового контролю є ключовою гарантією дотримання прав у санкційній сфері. Чим ширшими є повноваження держави у кризовий період, тим сильнішими повинні бути гарантії судового захисту. Інакше санкційний механізм ризикує перетворитися з інструменту захисту держави на інструмент надмірного владного тиску. У зв'язку з цим у судовий контроль у воєнний час повинен бути не формальним, а реальним і здатним перевіряти не лише зовнішню законність акта, а й межі розсуду, достатність мотивування, зв'язок між фактичними обставинами та обраним заходом. Така вимога узгоджується і з КАС України, і з загальноєвропейськими стандартами [4; 8].

Суд повинен виступати не лише формальним арбітром, а реальним інструментом перевірки обґрунтованості та меж державного втручання, забезпечуючи баланс між безпекою та свободою.

Отже, межі допустимої трансформації фінансових санкцій визначаються не лише потребами безпеки, а поєднанням цих потреб із незмінними принципами правової держави.

Саме збереження цього балансу є вирішальним критерієм легітимності санкційного режиму у воєнний період.

5. Міжнародний досвід та судова практика у сфері фінансових санкцій

5.1. Порівняльно-правовий аналіз регулювання фінансових санкцій в Україні, Європейському Союзі та міжнародній практиці

Порівняльно-правовий аналіз дозволяє побачити, що українська модель фінансових санкцій розвивається одночасно під впливом внутрішніх безпекових потреб, європейської інтеграції, міжнародних стандартів FATF і, опосередковано, глобальної практики targeted financial sanctions. З огляду на це її не можна адекватно оцінювати без зіставлення з моделями ЄС і США та з міжнародними підходами FATF [2; 7; 12].

Наведена модель дає змогу не лише ідентифікувати відмінності між правовими системами, а й виявити спільні тенденції розвитку санкційного права, що формують сучасну міжнародну архітектуру фінансової прозорості [7; 16].

Українська модель є гібридною. Доцільно також уточнити, що гібридність проявляється не лише у поєднанні різних видів санкцій, а й у різних правових режимах їх застосування. Частина санкцій функціонує в межах класичної фінансово-правової відповідальності, інша — у площині безпекового права, що має інші стандарти доказування, процедур і контролю. Це створює ситуацію, коли одна й та сама дія може оцінюватися через різні правові режими. Така багаторівневість ускладнює уніфікацію правозастосування. Вона поєднує класичні санкції фінансово-правової відповідальності,

регуляторно-наглядові заходи впливу та спеціальні економічні й інші обмежувальні заходи у сфері національної безпеки [9; 12; 13]. Її сильний бік — висока адаптивність до кризових умов. Її слабкий бік — фрагментарність і недостатня системність нормативної архітектури. Норми розосереджені між податковим, бюджетним, валютним, банківським, AML/CFT і санкційним законодавством, що ускладнює побудову єдиної доктринальної моделі.

У результаті правозастосувач стикається з необхідністю одночасного врахування норм різних галузей права, що підвищує ризик колізій та неоднакової практики їх застосування.

Модель ЄС є значно більш нормативно формалізованою. Окремо слід підкреслити, що правова визначеність у праві ЄС досягається не лише через формалізацію актів, а й через їх системне тлумачення Судом ЄС. Саме судова практика забезпечує однакове розуміння санкційних критеріїв, зокрема понять «контроль», «пов'язаність» та «економічна вигода». Це істотно знижує ризик різного застосування норм у державах-членах. Restrictive measures реалізуються через рішення Ради та регламенти Ради ЄС, які підлягають прямому застосуванню державами-членами. Базовим актом у контексті російської агресії залишається Council Regulation (EU) No 833/2014, що утворює системну правову рамку для секторальних і фінансових обмежень [2].

Важливою особливістю цієї моделі є високий рівень юридичної техніки та нормативної узгодженості, що забезпечує однаковість застосування санкцій у межах усіх держав-членів і мінімізує ризики довільного тлумачення.

У цій моделі санкція розглядається не як покарання у внутрішньодержавному сенсі, а як інструмент зовнішньополітичного та безпекового впливу, який підлягає суворим вимогам legal certainty, statement of reasons і judicial review [9; 10].

Стандарти FATF не встановлюють санкції у вузькому національно-правовому сенсі, але формують глобальну рамку targeted

financial sanctions, freezing mechanisms, beneficial ownership transparency та risk-based supervision [7].

Саме в межах підходу FATF фінансові санкції набувають системного характеру і розглядаються як елемент ширшої архітектури фінансової прозорості та запобігання ризикам, що виходить за межі традиційного розуміння юридичної відповідальності.

Для України це означає, що санкційна політика повинна розвиватися не ізольовано, а в тісному зв'язку з системою фінансового моніторингу та аналізу ризиків.

Американська модель OFAC демонструє один із найрозвиненіших у світі режимів targeted financial sanctions, у якому висока адміністративна ефективність поєднується з цифровізованими санкційними списками та розвиненою compliance infrastructure.

Важливою особливістю американської моделі є також широке застосування secondary sanctions, які поширюють санкційний вплив за межі юрисдикції США. Це створює глобальний ефект екстериторіальності, який змушує міжнародні фінансові установи враховувати вимоги OFAC незалежно від країни їх реєстрації. Для України цей аспект є актуальним у контексті інтеграції у світову фінансову систему.

Ключовою рисою цієї моделі є поєднання жорстких санкційних механізмів із детальною системою роз'яснень і процедур перегляду, що дозволяє зменшити правову невизначеність для бізнесу та фінансових установ.

Для українського законодавства цей досвід важливий як приклад того, що сучасний санкційний режим потребує не лише заборон, а й ефективної інституційної та цифрової інфраструктури.

Судовий контроль і стандарти пропорційності

Однією з головних відмінностей між українською та європейською моделями є інтенсивність судового контролю. У праві ЄС restrictive measures підлягають розвинутому judicial review, що підтверджено справами Kadi та Rosneft [9; 10].

У цих рішеннях сформульовано підхід, відповідно до якого навіть санкції у сфері безпеки не можуть застосовуватися без належного обґрунтування та перевірки їх пропорційності, що істотно обмежує дискрецію органів влади [9].

Практика ЄСПЛ, зокрема у справі M.S.L., TOV v. Ukraine, додатково підсилює вимогу fair balance і недопустимості свавільного втручання у майнову сферу [8].

На підставі порівняльного аналізу доцільно **запропонувати кілька напрямів імплементації**. Ці напрями мають системний характер і спрямовані не лише на вдосконалення нормативної бази, а й на трансформацію інституційної практики застосування санкцій.

По-перше, Україні потрібна систематизація законодавства про фінансові санкції — принаймні на рівні рамкового закону або комплексного пакета, який уніфікував би поняття, види санкцій, принципи їх застосування та мінімальні стандарти судового контролю [11].

По-друге, доцільно нормативно закріпити тест пропорційності для найбільш інтенсивних санкційних втручань у право власності, господарську діяльність та доступ до фінансової інфраструктури [8].

По-третє, слід створити систему офіційних санкційних роз'яснень для банків, фінансових установ і бізнесу за аналогією з європейськими FAQs та американським compliance guidance.

По-четверте, необхідно поглибити цифровізацію санкційного комплаєнсу: інтеграцію санкційних списків, даних про бенефіціарну власність, AML/CFT-індикаторів ризику та інформації про судовий статус санкційних рішень.

По-п'яте, варто розглянути створення чіткої процедури адміністративного перегляду санкційних рішень до або паралельно із судовим оскарженням, що дозволило б оперативніше виправляти помилкові чи застарілі рішення.

По-шосте, слід поглибити інтеграцію санкційної політики з AML/CFT та beneficial ownership regulation, оскільки в сучасному

правопорядку санкція вже не може бути ефективною без ризикоорієнтованого аналізу транзакційних і корпоративних зв'язків.

5.2. Системний аналіз судової практики України, Європейського Союзу та Європейського суду з прав людини у спорах щодо фінансових санкцій

Однією з ключових гарантій легітимності фінансових санкцій у сучасній правовій державі є ефективний судовий контроль. Саме судова практика визначає, чи залишаються санкції інструментом захисту публічного фінансового інтересу, чи перетворюються на форму надмірного владного втручання у майнову сферу особи. У контексті фінансових санкцій судовий контроль має особливе значення, оскільки санкційні механізми майже завжди пов'язані з втручанням у право власності, свободу підприємницької діяльності, доступ до рахунків, активів, платіжної інфраструктури або ринку капіталу. Відтак в демократичному правопорядку санкції не можуть оцінюватися виключно з точки зору доцільності чи ефективності: вони повинні витримувати перевірку на законність, належне мотивування, пропорційність, правову визначеність і наявність ефективного засобу захисту [4; 8; 9; 10]. Водночас у сучасних умовах воєнного стану ця вимога набуває підвищеного значення, оскільки інтенсивність втручання держави у фінансову сферу істотно зростає, що об'єктивно потребує більш глибокого та змістовного судового контролю.

У цьому контексті доцільно розрізняти формальний і матеріальний рівні судового контролю. Формальний контроль обмежується перевіркою компетенції органу та дотримання процедури, тоді як матеріальний охоплює оцінку обґрунтованості, пропорційності та фактичної бази рішення. Саме матеріальний контроль є визначальним для сучасних санкційних спорів.

В Україні основою судового контролю за фінансовими санкціями виступають насамперед стаття 55 Конституції України, яка гарантує

право на судовий захист, стаття 8 Конституції України, що закріплює принцип верховенства права, а також положення Кодексу адміністративного судочинства України, які забезпечують право особи оскаржити рішення, дії чи бездіяльність суб'єкта владних повноважень [3; 4]. Конституційний Суд України у своїх узагальнених правових позиціях послідовно наголошує, що принцип юридичної визначеності як складник верховенства права не виключає надання органам публічної влади дискреційних повноважень, однак у такому разі обов'язково мають існувати правові механізми запобігання зловживанню ними; крім того, обмеження прав і свобод допустимі лише тоді, коли вони є домірними, суспільно необхідними та встановленими законом. Це означає, що навіть у сфері фінансової безпеки держава не звільняється від обов'язку діяти в межах чітко визначених процедурних і матеріальних критеріїв [3; 4; 11].

Для фінансових санкцій це має пряме значення. Якщо санкція застосовується податковим органом, органом державного фінансового контролю, НБУ, Держфінмоніторингом чи іншим суб'єктом владних повноважень, вона повинна бути підконтрольною суду не лише формально, а й по суті. Інакше кажучи, суд має перевіряти не тільки наявність компетенції органу, а й чи існувала достатня правова підстава для застосування санкції, чи були належно встановлені фактичні обставини, чи відповідає вид та інтенсивність санкції поставленій меті, чи не було порушено принцип правової визначеності, а також чи не є втручання у права особи надмірним. Зазначений підхід фактично трансформує суд з органу формального контролю у повноцінний механізм матеріально-правової перевірки санкційного рішення, що відповідає сучасним стандартам верховенства права [4; 5].

Разом із тим саме українська практика демонструє одну з головних проблем у цій сфері: фінансові санкції в Україні часто перебувають на межі кількох правових режимів — фінансово-правового,

адміністративного, банківського, безпекового, санкційного. Через це не завжди є очевидним, який саме стандарт контролю має застосовувати суд: класичний стандарт перевірки адміністративного акта, більш стриманий стандарт контролю за безпековими рішеннями чи змішаний стандарт із підвищеною увагою до прав власності та економічної свободи. У результаті формується ситуація, коли судова практика може бути неоднорідною, що, у свою чергу, впливає на рівень правової визначеності та передбачуваності правозастосування [4; 12; 17]. Саме ця методологічна невизначеність є одним із чинників, що призводить до потребу надалі doctrinal refinement українського санкційного законодавства. Ця проблема ускладнюється також відсутністю єдиної класифікації фінансових санкцій у національному праві. У результаті суди змушені самостійно визначати природу санкції, що безпосередньо впливає на стандарт її перевірки.

Для розуміння сучасних стандартів судового контролю надзвичайно важливою є практика Суду Європейського Союзу. Саме в ній найпослідовніше вироблено правову модель, за якою навіть санкції у сфері зовнішньої політики та міжнародної безпеки не виводяться за межі юрисдикційного контролю. Європейський підхід демонструє, що безпековий характер санкцій не є підставою для зниження стандартів правового захисту, а навпаки — потребує їх посилення [9; 10].

У справі Kadi and Al Barakaat International Foundation v Council and Commission Суд ЄС прямо підтвердив, що акти ЄС, якими імплементуються санкційні або заморожувальні заходи, підлягають повноцінній перевірці на відповідність фундаментальним правам, зокрема праву на захист, праву бути вислуханим і праву на ефективний судовий перегляд. Суд наголосив, що навіть коли санкційний режим спрямований на цілі міжнародної безпеки, це не означає, що суд має відмовитися від перевірки його законності [9]. Ця позиція

фактично закріплює пріоритет прав людини навіть у найбільш чутливих сферах публічного управління. Таким чином, справа Kadi заклала основу доктрини автономності правового порядку ЄС, у межах якої навіть міжнародні санкційні рішення підлягають перевірці на відповідність фундаментальним правам.

Ще більш значущою для порівняльного аналізу є справа Rosneft (C-72/15). У ній Суд ЄС підтвердив, що restrictive measures, ухвалені в рамках Спільної зовнішньої та безпекової політики ЄС, підлягають судовому тлумаченню і перевірці на предмет законності. З практичної точки зору ця справа демонструє надзвичайно важливий принцип: широка дискреція інституцій у сфері санкцій не означає відсутності судового контролю; навпаки, саме ширина дискреції вимагає наявності дієвих механізмів judicial review [10]. Таким чином, дискреція і контроль у європейській моделі розглядаються як взаємодоповнюючі елементи, а не як альтернативи.

Таким чином, європейська судова практика виходить із кількох базових положень: санкційний акт має бути належно мотивований; повинна існувати достатня фактична база для включення особи до санкційного режиму; має бути забезпечене право на ефективний засіб юридичного захисту; втручання у майнову сферу має бути пропорційним [9; 10]. Ці критерії фактично формують універсальний стандарт оцінки санкційних рішень, який може бути імплементований і в національне право України. Систематизований огляд відповідної судової практики наведено у Додатку 2.

Для України ця практика має подвійне значення. Вона, з одного боку, підтверджує допустимість сильного санкційного механізму в умовах зовнішньої агресії та загроз безпеці, а з іншого — наголошує, що навіть найбільш жорсткий санкційний режим не може бути виведений за межі вимог верховенства права. Це особливо актуально в умовах воєнного стану, коли баланс між безпекою і правами людини стає найбільш вразливим.

Європейський суд з прав людини підходить до фінансових санкцій і суміжних обмежувальних заходів насамперед через призму статті 1 Першого протоколу до Конвенції, тобто через право мирного володіння майном. Саме цей підхід є особливо важливим для фінансових санкцій, оскільки більшість із них прямо або опосередковано зачіпають активи, розрахунки, комерційну діяльність або корпоративні права. Таким чином, фінансові санкції розглядаються не лише як інструмент публічного управління, а і як форма втручання у фундаментальне право, що потребує підвищеного рівня обґрунтування [8].

У справі M.S.L., TOV v. Ukraine Суд розглядав український санкційний режим у контексті замороження активів та дійшов висновку про проблематику відсутності достатніх процесуальних гарантій при такому втручанні. Це рішення має принципове значення для української правової системи, оскільки воно показує: навіть за наявності легітимної мети, пов'язаної з національною безпекою, держава повинна забезпечити достатній рівень правової процедури, зрозумілі підстави втручання та можливість ефективного оскарження [8]. Фактично йдеться про вимогу процесуальної справедливості як невід'ємного елементу санкційного механізму.

У справі S. C. Zorina International S.R.L. v. Romania Суд досліджував уже інший тип втручання — податково-санкційний [18]. Йшлося про штраф, конфіскацію виручки та тимчасове зупинення діяльності компанії. Суд розглядав справу саме крізь призму пропорційності санкції й дотримання справедливого балансу між публічним інтересом та правами суб'єкта господарювання. Це рішення є надзвичайно важливим для доктрини фінансових санкцій, оскільки демонструє: навіть якщо санкція формально передбачена законом і спрямована на захист податкової дисципліни, вона все одно повинна бути lawful, proportionate, and not excessive [18]. Це підкреслює, що формальна законність не є достатньою умовою легітимності санкції. Важливо також враховувати, що ЄСПЛ

оцінює не лише сам факт втручання, а й якість правової процедури, що йому передує. Відсутність достатніх процесуальних гарантій може сама по собі становити порушення Конвенції, незалежно від кінцевого результату втручання.

Отже, практика ЄСПЛ дозволяє сформулювати для фінансових санкцій кілька базових стандартів: будь-яке втручання в майнову сферу має бути законним; воно повинно мати на меті; має підтримуватися справедливий баланс між публічним інтересом і правами особи; у особи повинна бути реальна можливість оскаржити таке втручання. Ці стандарти утворюють універсальний правовий тест, який має застосовуватися судами незалежно від виду санкції чи галузі права.

Саме ці стандарти мають стати методологічною основою для української судової практики у спорах щодо фінансових санкцій. Їх імплементація дозволить не лише підвищити рівень захисту прав суб'єктів, а й зміцнити довіру до санкційного механізму як інструменту правової держави.

5.3. AML/CFT та санкційний комплаєнс як складник сучасного режиму фінансових санкцій

Однією з найбільш помітних тенденцій сучасного розвитку фінансового права є функціональне зближення інституту фінансових санкцій і механізмів AML/CFT. Закон України № 361-IX будує національну систему запобігання та протидії легалізації доходів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення на ризикоорієнтованому підході, обов'язках фінансових установ щодо ідентифікації клієнта, виявлення підозрілих операцій та інформування компетентних органів [14].

Формально фінансовий моніторинг і фінансові санкції не є тотожними правовими інститутами. Перший є системою контролю й виявлення ризиків, другий — формою владного впливу чи обмеження. Однак у період воєнного стану та в умовах глобальної

санкційної політики вони дедалі частіше працюють як єдиний функціональний комплекс. Результати AML/CFT-аналізу можуть стати підставою для блокування транзакцій, відмови у проведенні операції, замороження активів або передачі інформації для застосування обмежувальних заходів. При цьому важливо розмежовувати автоматичні та дискреційні рішення. Частина обмежень застосовується на підставі формалізованих індикаторів ризику, тоді як інші потребують індивідуальної оцінки комплаєнс-підрозділу. Це підвищує значення внутрішніх процедур і професійної відповідальності відповідних працівників.

Водночас важливо підкреслити, що така взаємодія не є випадковою або ситуативною: вона відображає глибинну трансформацію фінансового права, в якій акцент зміщується від реакції на вже вчинене правопорушення до раннього виявлення та нейтралізації ризиків. У цьому сенсі AML/CFT виступає своєрідною «аналітичною передумовою» санкцій, а санкції — їх інструментальною реалізацією.

Така інтеграція прямо узгоджується з логікою FATF Recommendations, де targeted financial sanctions розглядаються в контексті комплексної системи financial integrity [7]. До того, сучасна практика показує, що ефективність санкційного режиму значною мірою залежить не від суворості формальних заборон, а від здатності фінансової системи ідентифікувати ризикові зв'язки, транзакційні патерни та бенефіціарні структури, які підпадають під санкційні критерії.

FATF Recommendations у редакції, amended October 2025, прямо визначають targeted financial sanctions як один із ключових інструментів протидії терористичному фінансуванню та financing of proliferation [7]. Окремої уваги заслуговує те, що FATF розглядає ефективність санкцій не лише через наявність формального списку або норми про блокування активів, а через наявність у держави й фінансового сектору повноцінної compliance ecosystem: accurate

beneficial ownership information; timely asset freezing; suspicious transaction reporting; cross-border information exchange; supervisory enforcement; risk-based due diligence.

Зазначені елементи утворюють цілісний цикл: від ідентифікації ризику до його нейтралізації. Відсутність хоча б одного з них істотно знижує ефективність санкційного механізму.

Таким чином, санкційний комплаєнс у сучасному сенсі — це не внутрішня «технічна» функція банку, а одна з форм реалізації публічно-правового обов'язку щодо захисту фінансової системи. Саме тому в сучасній науковій доктрині виправдано говорити про санкційну комплаєнс-систему як сукупність внутрішніх процедур, політик, механізмів перевірки та управління ризиками, спрямованих на забезпечення відповідності діяльності суб'єкта вимогам санкційного, банківського та AML/CFT-законодавства.

З огляду на це особливого значення набуває ризикоорієнтований підхід (risk-based approach), який дозволяє гнучко адаптувати інтенсивність контролю до рівня загрози. Саме він забезпечує баланс між ефективністю санкційного режиму та недопущенням надмірного втручання у легальну економічну діяльність.

Крім того, FATF фактично формує універсальну «мову» санкційного комплаєнсу, що забезпечує сумісність національних систем і полегшує міжнародну координацію, особливо у справах, пов'язаних із транскордонними фінансовими потоками та складними корпоративними структурами.

У сучасних умовах банки вже не можуть розглядатися як нейтральні технічні посередники. Законодавство про банки, валютне регулювання, фінансовий моніторинг та санкції фактично покладає на них обов'язок здійснювати постійний контроль за контрагентами, транзакціями, пов'язаними особами та операційними ризиками [14; 15; 17]. У цьому контексті фінансова установа одночасно виконує приватногосподарську, регуляторно-комплаєнс-функцію та

квазіпублічну функцію з підтримання санкційного режиму. У цьому контексті постає питання меж відповідальності фінансових установ. Надмірне покладання квазіпублічних функцій може призвести до зміщення балансу між державою і приватним сектором, що потребує чіткого нормативного визначення.

Таке поєднання ролей об'єктивно змінює правову природу діяльності банків: вони стають не лише учасниками ринку, а й активними елементами механізму реалізації державної фінансової політики. Це, у свою чергу, підвищує вимоги до внутрішніх процедур контролю, прозорості прийняття рішень та документування підстав для обмежувальних заходів.

Саме така багатофункціональність і створює ризик over-compliance, коли фінансова установа внаслідок страху перед відповідальністю застосовує більш жорсткі обмеження, ніж прямо вимагає закон. Ця проблема добре відома і в міжнародній практиці, і відтак в ЄС та США велика увага приділяється роз'ясненням, FAQs, guidance notes і reconsideration procedures [2; 7]. Особливо це проявляється у відмовах від обслуговування клієнтів із підвищеним ризиком, навіть за відсутності прямих правових підстав для такого обмеження. Це створює ризики дискримінації та звуження доступу до фінансових послуг.

Крім того надмірний комплаєнс може мати негативні системні наслідки: обмеження доступу до фінансових послуг, «деризикування» (de-risking), витіснення добросовісних клієнтів з ринку. З огляду на це сучасна регуляторна політика дедалі більше орієнтується не лише на жорсткість контролю, а й на його пропорційність та обґрунтованість.

Невід'ємною рисою сучасного санкційного режиму є його цифровізація. У США OFAC підтримує Sanctions List Service, а в ЄС існує консолідований доступ до restrictive measures через EUR-Lex та пов'язані інструменти Комісії [2]. Українське законодавство

й практика також рухаються у цьому напрямі, однак науково обґрунтованою є теза про необхідність створення цілісної національної цифрової інфраструктури санкційного комплаєнсу.

Йдеться не лише про технічну інтеграцію даних, а про формування єдиного цифрового середовища, у якому санкційна інформація буде доступною, актуальною та взаємопов'язаною. Така система має забезпечувати інтеграцію санкційних списків, даних про бенефіціарну власність, AML/CFT-індикаторів ризику, судового статусу санкційних рішень і офіційних регуляторних роз'яснень у режимі, максимально наближеному до реального часу.

Додатково варто враховувати потенціал використання технологій штучного інтелекту та автоматизованого аналізу даних для виявлення складних фінансових схем, що дозволить підвищити точність санкційного комплаєнсу та зменшити залежність від формальних критеріїв.

Таким чином, цифровізація виступає не допоміжним, а структуроутворюючим елементом сучасного санкційного режиму. Вона забезпечує перехід від фрагментарного контролю до системного управління фінансовими ризиками, що критично важливо в умовах воєнного стану та глобалізованої економіки. Водночас широке впровадження технологій потребує належного врегулювання питань захисту даних, доступу до інформації та відповідальності за помилки автоматизованих систем. Без відповідної правової бази технологічна ефективність може супроводжуватися зростанням юридичних ризиків.

6. Розгорнуті пропозиції *de lege ferenda* щодо вдосконалення правового регулювання фінансових санкцій в Україні

Порівняльний, доктринальний та практичний аналіз дозволяє сформулювати розгорнуту систему пропозицій *de lege ferenda*, спрямованих на підвищення системності, передбачуваності

та легітимності фінансових санкцій в Україні. Разом із тим важливо підкреслити, що такі пропозиції не є абстрактними теоретичними конструкціями, а випливають із конкретних проблем правозастосування, виявлених як у національній практиці, так і в практиці Європейського Союзу та ЄСПЛ. З огляду на це їх реалізація має розглядатися як елемент більш широкої реформи фінансового та адміністративного права в умовах воєнного стану та євроінтеграції [3; 4; 8]. У зв'язку з цим подальший виклад пропозицій доцільно структурувати за ключовими напрямами реформування: нормативно-системним, процедурним, інституційним та технологічним.

Передусім потрібна загальна систематизація законодавства у сфері фінансових санкцій. Йдеться не обов'язково про кодифікацію у формі окремого кодексу, а щонайменше про рамковий закон або комплексний законодавчий пакет, який би: визначив поняття фінансових санкцій; класифікував їх види; розмежував фінансові санкції, заходи контролю, забезпечувальні заходи та *restrictive measures* у сфері національної безпеки; закріпив загальні принципи застосування санкцій; встановив мінімальні стандарти мотивування та перегляду рішень.

Зокрема, на рівні законодавчої техніки доцільно передбачити внесення змін до Закону України «Про санкції» з метою деталізації видів фінансових обмежень та процедур їх застосування, а також узгодження його положень із нормами Податкового кодексу України та Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [9; 12; 14]. Окремо доцільним є закріплення у Кодексі адміністративного судочинства України спеціальних процесуальних норм щодо оскарження санкційних рішень, що дозволить забезпечити єдність судової практики [4].

Важливо також передбачити уніфіковані дефініції суміжних категорій (зокрема «санкційний захід», «обмеження», «замороження активів», «ризик»), що дозволить уникнути змішування правових режимів у правозастосуванні. Окремо доцільно визначити співвідношення матеріальних і процесуальних норм у цій сфері, оскільки саме їх неузгодженість нині часто породжує колізії.

Доцільність такої систематизації зумовлена тим, що чинне регулювання є фрагментованим і розосередженим між податковим, банківським, валютним, санкційним та AML/CFT законодавством, що ускладнює як правозастосування, так і судовий контроль. У результаті одна й та сама ситуація може отримувати різну правову кваліфікацію залежно від галузевої «оптики», що підриває принцип правової визначеності [9; 12; 14; 17]. У цьому контексті особливої уваги потребує узгодження санкційних механізмів із положеннями валютного законодавства та банківського регулювання, зокрема Закону України «Про валюту і валютні операції» та Закону України «Про банки і банківську діяльність», які вже містять елементи обмежувальних фінансових заходів [15; 17]. Одним із ключових елементів подолання зазначених проблем є впровадження універсальних матеріально-правових критеріїв оцінки санкційних рішень.

Доцільно нормативно закріпити обов'язок застосовувати тест пропорційності щодо тих санкцій, які істотно втручаються у право власності, господарську діяльність або доступ до фінансової інфраструктури. У законі або в загальних процедурних нормах має бути прямо передбачено, що орган, який застосовує санкцію, повинен оцінити:

1) легітимну мету;
2) придатність заходу;
3) необхідність заходу;
4) співмірність втручання.

При цьому законодавець може деталізувати критерії оцінки пропорційності, зокрема через врахування характеру порушення, тривалості обмеження, обсягу втручання у господарську діяльність та можливості застосування альтернативних, менш обтяжливих заходів. Такий підхід дозволить перевести принцип пропорційності з рівня загальної декларації на рівень прикладного інструменту. Доцільно також передбачити, що недотримання тесту пропорційності є самостійною підставою для скасування санкційного рішення в адміністративному судочинстві, що прямо узгоджується з положеннями статті 2 Кодексу адміністративного судочинства України щодо перевірки рішень суб'єктів владних повноважень [4].

Включення такого тесту на нормативному рівні дозволить уніфікувати підходи органів публічної влади та судів, а також забезпечить імплементацію європейських стандартів захисту права власності, сформованих у практиці ЄСПЛ та Суду ЄС [8; 9; 10; 18]. Крім того, це сприятиме зниженню ризику формального або автоматичного застосування санкцій без належної індивідуалізації.

Україні доцільно запровадити постійну систему офіційних санкційних роз'яснень для банків, небанківських фінансових установ, суб'єктів фінансового моніторингу та бізнесу. Така система могла б бути побудована за аналогією з європейськими FAQs та американським OFAC guidance і суттєво зменшила б рівень правової невизначеності та *over-compliance*. Крім того, такі роз'яснення можуть виконувати функцію превентивного регулювання, оскільки дозволяють суб'єктам ринку адаптувати свою поведінку до вимог держави без необхідності застосування санкцій. Такий підхід може бути інституціоналізований через повноваження Національного банку України та інших регуляторів щодо надання обов'язкових до врахування роз'яснень, аналогічно їхнім існуючим функціям у сфері банківського нагляду [13; 15]. У цьому сенсі вони

виступають елементом «м'якого права», що доповнює формальні нормативні приписи.

Запровадження таких роз'яснень має не лише інформаційне, а й правове значення, оскільки дозволяє сформувати передбачувану практику застосування санкційних норм. У відсутності чітких орієнтирів суб'єкти господарювання змушені діяти обережніше, ніж це об'єктивно необхідно, що призводить до надмірного обмеження економічної активності та фінансових операцій.

Окремо варто передбачити чітку процедуру адміністративного перегляду санкційних рішень, не як заміну судового контролю, а як додатковий механізм оперативного виправлення помилкових, застарілих або непропорційних обмежень. З огляду на це показовою є модель 31 CFR § 501.807 у США, яка передбачає *petition for administrative reconsideration* [19]. В українських умовах така процедура може бути закріплена у Законі України «Про санкції» як окремий адміністративний механізм перегляду, із визначенням компетентного органу та процесуальних строків [12]. Поряд із процедурними гарантіями не менш важливим є функціональний зв'язок санкційного режиму з суміжними інститутами фінансового контролю.

Впровадження подібної процедури в Україні дозволить зменшити навантаження на судову систему та забезпечити більш швидке відновлення порушених прав у випадках очевидної помилки або зміни обставин. Водночас така процедура має супроводжуватися чіткими строками розгляду, вимогами до мотивування рішень та гарантіями неупередженості органу, який здійснює перегляд. Доцільно також передбачити можливість подання нових доказів або інформації, яка не була доступна на момент ухвалення первинного рішення, що підвищить ефективність такого перегляду.

Ще один напрям — поглиблення інтеграції санкційного режиму з AML/CFT і регулюванням бенефіціарної власності.

Наступним логічним етапом розвитку санкційного регулювання є його технологічна модернізація. Без належної прозорості корпоративних структур і ефективного виявлення пов'язаних осіб санкційний режим неминуче залишається неповним. Саме тому законодавче вдосконалення санкцій повинно йти паралельно з посиленням механізмів *beneficial ownership transparency* та ризик-коорієнтованого нагляду [7; 14].

Особливого значення ця інтеграція набуває в умовах використання складних транскордонних корпоративних структур, які дозволяють обходити санкційні обмеження. У цьому аспекті важливим є також забезпечення взаємодії між Держфінмоніторингом, Національним банком України та іншими органами фінансового контролю, що прямо випливає з чинного законодавства у сфері фінансового моніторингу [14]. У зв'язку з цим ефективність санкцій безпосередньо залежить від якості фінансового моніторингу та доступу до вирогідної інформації про кінцевих бенефіціарів.

Доцільно створити єдину цифрову інфраструктуру санкційного комплаєнсу, яка б дозволяла банкам, фінансовим установам і державним органам в режимі реального часу перевіряти статус особи, пов'язаність, судовий статус рішення, наявність у санкційних списках, а також отримувати офіційні роз'яснення щодо режиму застосування обмежень. Це відповідає глобальній тенденції переходу від спискового санкційного режиму до *data-driven sanctions governance*. Впровадження такої системи може бути реалізоване на базі вже існуючих державних реєстрів та інформаційних систем, зокрема реєстрів бенефіціарної власності та фінансового моніторингу, із подальшою їх інтеграцією [14]. Важливо, щоб така система була сумісною з міжнародними інформаційними платформами та забезпечувала автоматизований обмін даними з іноземними юрисдикціями, що особливо актуально для протидії обходу санкцій через транскордонні структури.

Фактично йдеться про створення інтегрованої інформаційної екосистеми, яка забезпечуватиме не лише доступ до даних, а й їх аналітичну обробку. Такий підхід дозволить підвищити точність санкційного комплаєнсу, зменшити кількість помилкових блокувань і при цьому підвищити ефективність виявлення реальних загроз [2; 16].

Необхідно також розробити на рівні доктрини та, можливо, узагальнення судової практики єдиний стандарт судового контролю для фінансових санкцій і суміжних заходів. Суд повинен мати чіткі орієнтири щодо перевірки:

— компетенції органу;

— достатності доказової бази;

— мотивування акта;

— зв'язку між фактичними обставинами та обраним обмеженням;

— пропорційності втручання.

Окремої уваги потребує питання стандарту доказування, який має застосовуватися у справах щодо фінансових санкцій, оскільки він прямо впливає на баланс між ефективністю санкційного режиму та захистом прав особи.

Уніфікація таких стандартів сприятиме підвищенню передбачуваності судової практики та зміцненню довіри до санкційного механізму загалом. Водночас вона дозволить уникнути ситуацій, коли подібні за своєю природою санкційні спори вирішуються за різними методологічними підходами, що нині є однією з ключових проблем правозастосування в Україні.

У підсумку запропоновані вектори вдосконалення свідчать про необхідність трансформації фрагментарного регулювання фінансових санкцій у цілісну та методологічно узгоджену архітектуру, що поєднує дієвість безпекових механізмів із гарантіями верховенства права. Саме такий підхід дозволить забезпечити баланс між

публічним інтересом держави та інтересами учасників фінансових відносин у сучасних умовах. Реалізація зазначених заходів має відбуватися поетапно: на першому етапі — нормативна систематизація та уніфікація понять, на другому — запровадження процедурних гарантій і механізмів перегляду, на третьому — цифровізація та інтеграція санкційного комплаєнсу. Така послідовність дозволить уникнути фрагментарності реформ і забезпечити їх практичну ефективність. Окреслені заходи реформування утворюють взаємопов'язаний комплекс змін, спрямований на одночасне зміцнення санкційного інструментарію та підвищення рівня юридичного захисту. Деталізовану структурно-функціональну модель реалізації зазначених пропозицій наведено у Додатку 3. Їх системна реалізація сприятиме розбудові виваженої правової конструкції, орієнтованої на європейські стандарти. Узагальнену нормативну модель запропонованих змін наведено у Додатку 4.

Таким чином, проведене дослідження дозволило обґрунтувати, що фінансові санкції в сучасному правопорядку України трансформуються з інструменту ретроспективної відповідальності у комплексний механізм превентивного фінансово-безпекового регулювання. Доведено, що їх ефективність залежить не лише від нормативного закріплення, а й від якості процедур, рівня судового контролю, інтеграції з AML/CFT та розвитку цифрової інфраструктури. Встановлено, що ключовими умовами легітимності санкцій є дотримання принципу пропорційності, забезпечення правової визначеності та наявність ефективних засобів юридичного захисту, що відповідає як конституційним засадам, так і практиці ЄСПЛ та Суду ЄС [3; 4; 8; 9; 10]. У сукупності це свідчить про формування нової парадигми фінансового права, орієнтованої на управління ризиками, забезпечення фінансової безпеки та узгодження публічних і приватних інтересів.

7. Висновки

Проведене дослідження дає підстави стверджувати, що інститут фінансових санкцій у сучасному правопорядку України втратив суто вузьке, традиційне розуміння як форми фінансово-правової відповідальності за вже вчинене порушення і трансформувався у значно складніший, багатофункціональний та міжгалузевий механізм державного впливу. У сучасних умовах, особливо в період дії воєнного стану, фінансові санкції функціонують не лише як засіб покарання і компенсації, так й інструмент підтримання фінансової стабільності, захисту публічних фінансів, обмеження ризикових фінансових потоків, запобігання використанню фінансової системи в підривних цілях і забезпечення економічного суверенітету держави. Така еволюція повністю корелює з конституційною моделлю допустимого втручання держави у майнову сферу особи, оскільки Конституція України одночасно гарантує захист права власності, право на судовий захист і допускає тимчасові обмеження окремих прав лише на підставі закону та в межах воєнного стану [3, 6], що додатково підкреслює необхідність системного узгодження санкційного регулювання з фундаментальними конституційними гарантіями та принципом верховенства права як матеріального критерію оцінки будь-якого втручання. Така трансформація потребує не лише опису, а й системного узагальнення ключових результатів дослідження.

Перший загальний висновок полягає в тому, що фінансові санкції доцільно розглядати як самостійний правовий інститут публічного права, що має міжгалузевий характер, але системно пов'язаний насамперед із фінансовим правом. Його самостійність обумовлюється власним предметом регулювання, специфічним суб'єктним складом, особливими процесуальними формами реалізації та чітко вираженим майново-обмежувальним характером. На відміну від інших видів юридичного примусу, фінансові санкції спрямовані

переважно на сферу коштів, активів, фінансових операцій, ліквідності, доступу до платіжної та банківської інфраструктури, а тому мають особливий зв'язок із правом власності та економічною свободою суб'єкта. Саме тому їх правова конструкція потребує одночасного урахування фінансово-правових, адміністративно-процесуальних, банківсько-регуляторних і конституційних параметрів [4; 9; 13; 15], а також узгодження з сучасними підходами до публічного управління ризиками у фінансовій сфері, що виходять за межі класичної каральної парадигми.

Другий висновок полягає в тому, що поняття фінансових санкцій не може обмежуватися лише штрафом, пенею чи іншим класичним стягненням. У сучасному сенсі фінансові санкції охоплюють ширший комплекс майнових, організаційно-обмежувальних та владно-регуляторних заходів, які прямо встановлюються законом або реалізуються в межах закону уповноваженими суб'єктами у сфері податкового, бюджетного, валютного, банківського, AML/CFT та санкційного регулювання. У зв'язку з цим запропоноване в дослідженні розуміння фінансових санкцій як заходів, спрямованих не лише на припинення правопорушень, а й на відновлення фінансового порядку, попередження ризиків і забезпечення економічного суверенітету, є більш адекватним сучасному стану законодавства та правозастосування, ніж традиційна вузька каральна модель. Конституційні рамки такого підходу визначаються поєднанням статей 8, 41, 55, 64 і 67 Конституції України, а міжнародно-правова логіка — сучасними стандартами FATF і restrictive measures ЄС [2; 3; 7], що свідчить про поступову конвергенцію національного права з глобальними стандартами фінансової безпеки та комплаєнсу.

Третій висновок стосується системоутворюючих ознак фінансових санкцій. Аналіз показує, що їх визначальними рисами є: майновий або економічно-обмежувальний характер; публічно-владна природа; спеціальна сфера функціонування; застосування лише

уповноваженими законом суб'єктами; зв'язок або з правопорушенням, або з ризиком порушення фінансового порядку; багатофункціональність; підвищений ступінь втручання у сферу права власності; наявність спеціального процесуального режиму. Саме поєднання цих ознак дає змогу відмежувати фінансові санкції від цивільноправовий штрафних механізмів, загальних адміністративних обмежень або суто контрольних процедур. У сучасній доктрині це має принципове значення, оскільки без такого розмежування правове регулювання санкцій неминуче залишається фрагментарним і суперечливим [5; 11], що ускладнює як правозастосування, так і судовий контроль за відповідними рішеннями.

Четвертий висновок полягає в необхідності чіткого розмежування фінансових санкцій, заходів фінансового контролю, забезпечувальних заходів та обмежувальних заходів у сфері національної безпеки. Податкова перевірка, фінансова ревізія, валютний нагляд або процедура фінансового моніторингу самі по собі ще не є санкціями. Вони можуть бути підготовчим, контрольним або виявлювальним етапом, але санкційного характеру набувають лише тоді, коли за їх наслідками до особи застосовується негативний владний вплив. Аналогічно, не кожен захід замороження, зупинення чи блокування автоматично тотожний фінансовій санкції у вузькому сенсі: частина таких заходів має забезпечувальну природу, а частина — безпекову. Однак у період воєнного стану між цими інститутами відбувається очевидне функціональне зближення, унаслідок чого вони все частіше утворюють єдиний механізм захисту фінансової безпеки держави, що потребує їх доктринального переосмислення як елементів єдиної системи фінансово-безпекового регулювання.

П'ятий (загальний) висновок стосується відмінності між мирним періодом і періодом воєнного стану. У мирний час фінансові санкції функціонують переважно в логіці ретроспективної

юридичної відповідальності. Їх підставою є встановлене порушення фінансового законодавства, а домінуючими функціями виступають каральна і компенсаційна. Для цього режиму характерні вищий рівень формалізації, чіткіші процедурні рамки, вужча дискреція органів державної влади та більш усталений судовий контроль. Умовно кажучи, мирна модель фінансових санкцій є моделлю реакції на порушення. Натомість воєнний стан породжує іншу модель — реакції на ризик і загрозу, в межах якої санкція дедалі більше виконує превентивну, стабілізаційну та безпекову функції, що зумовлює необхідність перегляду традиційних підходів до їх правової природи та меж допустимого втручання.

Шостий висновок полягає в тому, що в умовах воєнного стану відбувається якісна трансформація правової природи фінансових санкцій. Вони переходять від переважно реактивної моделі до моделі проактивного фінансово-безпекового регулювання. Ця трансформація проявляється у п'яти взаємопов'язаних напрямах: зміщенні акценту з покарання на захист фінансової безпеки; посиленні превентивної функції; розширенні дискреційних повноважень; зростанні ролі приватного сектору як співвиконавця санкційної політики; інтеграції фінансових санкцій з механізмами національної безпеки. У результаті санкція перестає бути лише технікою фіскального чи дисциплінарного впливу й перетворюється на елемент економічної оборони держави, що свідчить про формування нової парадигми фінансового права, орієнтованої на управління ризиками та забезпечення стійкості фінансової системи. У цьому контексті доцільно говорити про формування окремого підінституту фінансово-безпекового регулювання, який поєднує елементи фінансового права, права національної безпеки та економічного права.

Сьомий висновок пов'язаний із тим, що така трансформація, хоч і є об'єктивно виправданою, не може бути безмежною. Воєнний стан не скасовує фундаментальних засад правової держави.

Навпаки, чим інтенсивнішим стає втручання держави у майнову сферу особи, тим суворішими повинні бути вимоги до законності, правової визначеності, пропорційності, належного врядування та ефективного судового контролю. Закон України «Про правовий режим воєнного стану» не усуває вимог Конституції України, а лише дозволяє тимчасово модифікувати певні правові режими у встановлених межах [3; 6], що обумовлює необхідність підвищених стандартів обґрунтування та перевірки санкційних рішень у судовому порядку.

Восьмий висновок стосується судового контролю. Аналіз української, європейської та конвенційної практики показує, що фінансові санкції не можуть бути легітимними поза ефективним механізмом judicial review. У праві України така вимога випливає зі статті 55 Конституції України та Кодексу адміністративного судочинства України [3; 4]; у праві ЄС — із практики Суду Європейського Союзу; у конвенційному праві — зі статті 1 Першого протоколу та статті 13 Конвенції у їх матеріальному розумінні [20]. У справах Kadi and Al Barakaat та Rosneft Суд ЄС сформулював засадничий підхід, за яким навіть безпекові санкції повинні бути підконтрольні суду [9; 10], а їх мотивування та доказова база підлягають повноцінній перевірці на відповідність фундаментальним правам. У справі M.S.L., TOV v. Ukraine ЄСПЛ окремо підкреслив проблематику незаконного замороження активів за відсутності достатніх процесуальних гарантій [8], що є прямим орієнтиром для вдосконалення української практики.

Дев'ятий висновок полягає в тому, що принцип пропорційності виступає спільним методологічним ядром української, європейської та міжнародної моделей фінансових санкцій. У конституційному правовому полі України він випливає зі статей 8, 41 і 64 Конституції України та правових позицій Конституційного Суду України щодо верховенства права і юридичної визначеності. У праві

ЄС пропорційність є одним із базових критеріїв оцінки restrictive measures, а в FATF-парадигмі аналогічна логіка реалізується через risk-based approach, що забезпечує баланс між ефективністю санкцій і недопущенням надмірного втручання у права особи.

Десятий висновок стосується порівняльно-правового аналізу. Українська модель фінансових санкцій є гібридною: вона поєднує класичні інструменти фінансово-правової відповідальності, регуляторно-наглядові заходи та спеціальні обмежувальні заходи у сфері національної безпеки. Європейська модель характеризується вищим рівнем нормативної формалізації, розвитком soft law guidance та сильнішим судовим контролем. Міжнародні стандарти FATF зміщують фокус санкцій із покарання на таргетоване фінансове стримування ризиків, а американська практика OFAC демонструє високий рівень цифровізації та процедур адміністративного перегляду [7; 19], що відкриває для України можливість формування синтетичної, більш збалансованої моделі санкційного регулювання.

Одинадцятий висновок пов'язаний з AML/CFT та санкційним комплаєнсом. Сучасне санкційне право неможливо більше розглядати ізольовано від системи фінансового моніторингу. Закон України № 361-IX, вимоги FATF та сучасна банківська практика підтверджують, що фінансовий моніторинг, перевірка бенефіціарної власності, аналіз підозрілих транзакцій і санкційний режим утворюють єдиний функціональний комплекс захисту фінансової системи [7; 14], у межах якого приватний сектор фактично виступає співвиконавцем публічної санкційної політики.

Дванадцятий висновок стосується необхідності вдосконалення українського законодавства de lege ferenda. У результаті проведеного дослідження можна визнати науково та практично обґрунтованими такі напрями реформування:

— систематизація законодавства про фінансові санкції;
— нормативне закріплення тесту пропорційності;

— створення системи офіційних санкційних роз'яснень для банків, фінансових установ і бізнесу;

— запровадження більш чіткої процедури адміністративного перегляду санкційних рішень;

— інтеграція санкційного режиму з AML/CFT і beneficial ownership regulation;

— розвиток цифрової інфраструктури санкційного комплаєнсу;

— уніфікація стандартів судового контролю, що в сукупності має забезпечити підвищення правової визначеності, узгодженості та ефективності санкційного механізму без втрати його функціональної спроможності.

Отже, загальний підсумок усього розділу полягає в тому, що фінансові санкції в сучасному українському правопорядку є комплексним, багаторівневим і міжгалузевим інститутом, який поєднує риси фінансово-правової відповідальності, державного примусу, макрофінансового регулювання та економіко-безпекового управління. У мирний період вони проявляються переважно як інструмент відповідальності за порушення фінансового законодавства; в умовах воєнного стану — як механізм попередження, локалізації та нейтралізації фінансових ризиків і загроз національній безпеці. Водночас визначальним критерієм їх легітимності залишається здатність поєднувати ефективність державного впливу з дотриманням фундаментальних прав людини, що формує необхідність подальшої європеїзації та доктринальної узгодженості санкційного законодавства України. У більш широкому теоретико-правовому вимірі результати дослідження дозволяють констатувати формування в Україні нової парадигми фінансового права, яку доцільно визначити як **security-driven finance law** — моделі, в якій фінансово-правові інструменти використовуються не лише для фіскального регулювання чи забезпечення відповідальності, а передусім як засіб

управління системними ризиками, захисту фінансової стабільності та забезпечення економічної безпеки держави. У межах цієї парадигми фінансові санкції виступають ключовим функціональним елементом, що поєднує регуляторну, превентивну та безпекову складові, трансформуючи традиційні уявлення про межі та призначення фінансово-правового впливу. Подальший розвиток цього інституту має відбуватися з урахуванням не лише внутрішніх потреб держави, а й динаміки міжнародного санкційного середовища, що характеризується високим рівнем змінюваності та технологічної складності.

Таким чином, у роботі доведено, що еволюція фінансових санкцій в Україні є не фрагментарною зміною окремих правових інструментів, а проявом глибшої трансформації всієї системи фінансового права, орієнтованої на поєднання принципів верховенства права з імперативами національної та фінансової безпеки. Саме ця трансформація визначатиме подальшу логіку розвитку як санкційного законодавства, так і фінансово-правової доктрини загалом.

Список використаних джерел:

1. Кучерявенко М. П. Фінансове право : підручник. Харків : Право, 2013. 512 с.

2. Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. *Official Journal of the European Union*. 2014. L 229. Pp. 1–11. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0833

3. Конституція України : Закон України від 28 червня 1996 року № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

4. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV. *Відомості Верховної Ради України*. 2005. 30. Ст. 284. URL: https://zakon.rada.gov.ua/laws/show/2747-15

5. Орлюк О. П. Фінансове право: академічний та прикладний аспекти : підручник. Київ : Юрінком Інтер, 2020.

6. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. *Відомості Верховної Ради України*. 2015. № 28. Ст. 250. URL: https://zakon.rada.gov.ua/laws/show/389-19

7. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: FATF Recommendations. FATF, 2025. URL: www.fatf-gafi.org

8. Case of M.S.L., TOV v. Ukraine: Judgment of the European Court of Human Rights of 2025. URL: hudoc.echr.coe.int

9. Kadi and Al Barakaat International Foundation v Council and Commission: Judgment of the Court of Justice (Grand Chamber) of 3 September 2008. Joined Cases C-402/05 P and C-415/05 P. URL: eur-lex.europa.eu

10. Rosneft Case C-72/15: Judgment of the Court of Justice (Grand Chamber) of 28 March 2017. PJSC Rosneft Oil Company v Her Majesty's Treasury and Others. URL: eur-lex.europa.eu

11. Кучерявенко М. П. Фінансове право України: доктринальні основи : монографія. Харків : Право, 2019.

12. Про санкції : Закон України від 14.08.2014 № 1644-VII. *Відомості Верховної Ради України*. 2014. № 40. Ст. 2018. URL: https://zakon.rada.gov.ua/laws/show/1644-18

13. Про Національний банк України : Закон України від 20.05.1999 № 679-XIV. *Відомості Верховної Ради України*. 1999. № 24. Ст. 118. URL: https://zakon.rada.gov.ua/laws/show/679-14

14. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06 грудня 2019 року № 361-IX. *Відомості Верховної Ради України*. 2019. № 50. Ст. 472. URL: https://zakon.rada.gov.ua/laws/show/361-20

15. Про банки й банківську діяльність : Закон України від 07.12.2000 № 2121-III. *Відомості Верховної Ради України*. 2001. № 9. Ст. 66. URL: https://zakon.rada.gov.ua/laws/show/2121-14

16. Principles for Financial Market Infrastructures: Basel Committee on Banking Supervision. Bank for International Settlements. 2012. URL: www.bis.org

17. Про валюту і валютні операції : Закон України від 21.06.2018 № 2473-VIII. *Відомості Верховної Ради України*. 2018. № 38. Ст. 161. URL: https://zakon.rada.gov.ua/laws/show/2473-19

18. Case of S.C. Zorina International S.R.L. v. Romania: Judgment of the European Court of Human Rights of 20 October 2015. (Application no. 38133/05). URL: hudoc.echr.coe.int

19. 31 CFR § 501.807 — Procedures for Persons Subject to Blocking Pursuant to Executive Order 13224: Code of Federal Regulations of the United States of America. Title 31. Subtitle B. Chapter V. Part 501. URL: www.ecfr.gov

20. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), 4 November 1950. URL: https://www.echr.coe.int

References:

1. Kucheryavenko, M. P. Financial Law: Textbook. Kharkiv : Law, 2013. 512 p.

2. Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. *Official Journal of the European Union*. 2014. L 229. Pp. 1–11. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0833

3. Constitution of Ukraine: Law of Ukraine of 28 June 1996 No. 254k/96-VR. *Bulletin of the Verkhovna Rada of Ukraine*. 1996. No. 30. Art. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

4. Code of Administrative Procedure of Ukraine: Law of Ukraine dated 06.07.2005 No. 2747-IV. *Bulletin of the Verkhovna Rada of Ukraine*. 2005. No. 30. Art. 284. URL: https://zakon.rada.gov.ua/laws/show/2747-15

5. Orlyuk, O. P. Financial Law: Academic and Applied Aspects: Textbook. Kyiv: Yurinkom Inter, 2020.

6. On the Legal Regime of Martial Law: Law of Ukraine dated 12.05.2015 No. 389-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2015. No. 28. Art. 250. Retrieved from https://zakon.rada.gov.ua/laws/show/389-19

7. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: FATF Recommendations. FATF, 2025. URL: www.fatf-gafi.org

8. Case of M.S.L., TOV v. Ukraine: Judgment of the European Court of Human Rights of 2025. URL: hudoc.echr.coe.int

9. Kadi and Al Barakaat International Foundation v Council and Commission: Judgment of the Court of Justice (Grand Chamber) of 3 September 2008. Joined Cases C-402/05 P and C-415/05 P. URL: eur-lex.europa.eu

10. Rosneft Case C-72/15: Judgment of the Court of Justice (Grand Chamber) of 28 March 2017. PJSC Rosneft Oil Company v Her Majesty's Treasury and Others. URL: eur-lex.europa.eu

11. Kucheryavenko M. P. Financial Law of Ukraine: Doctrinal Foundations: Monograph. Kharkiv: Law, 2019.

12. On Sanctions: Law of Ukraine dated 14.08.2014 No. 1644-VII. *Bulletin of the Verkhovna Rada of Ukraine*. 2014. No. 40. Art. 2018. Retrieved from https://zakon.rada.gov.ua/laws/show/1644-18

13. On the National Bank of Ukraine: Law of Ukraine dated 20.05.1999 No. 679-XIV. Bulletin of the Verkhovna Rada of Ukraine. 1999. No. 24. Art. 118. Retrieved from https://zakon.rada.gov.ua/laws/show/679-14

14. On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction: Law of Ukraine dated December 6, 2019 No. 361-IX. *Bulletin of the Verkhovna Rada of Ukraine*. 2019. No. 50. Art. 472. URL: https://zakon.rada.gov.ua/laws/show/361-20

15. On Banks and Banking Activities: Law of Ukraine dated December 7, 2000 No. 2121-III. *Bulletin of the Verkhovna Rada of Ukraine*.

2001. No. 9. Art. 66. Retrieved from https://zakon.rada.gov.ua/laws/show/2121-14

16. Principles for Financial Market Infrastructures. Basel Committee on Banking Supervision. Bank for International Settlements. 2012. Retrieved from www.bis.org

17. On Currency and Currency Operations: Law of Ukraine of 21.06.2018 No. 2473-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2018. No. 38. Art. 161. Retrieved from https://zakon.rada.gov.ua/laws/show/2473-19

18. Case of S.C. Zorina International S.R.L. v. Romania: Judgment of the European Court of Human Rights of 20 October 2015 (Application no. 38133/05). Retrieved from hudoc.echr.coe.int

19. 31 CFR § 501.807 — Procedures for Persons Subject to Blocking Pursuant to Executive Order 13224: Code of Federal Regulations of the United States of America. Title 31. Subtitle B. Chapter V. Part 501. Retrieved from www.ecfr.gov

20. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), 4 November 1950. Retrieved from https://www.echr.coe.int

Додаток 1

Емпіричні та аналітичні індикатори застосування фінансових санкцій

Показник	Мирний період	Воєнний стан	Тенденція
Частка санкцій post factum	Висока	Знижується	↓
Частка санкцій risk-based	Низька	Висока	↑
Рівень дискреції органів	Обмежений	Розширений	↑
Інтенсивність втручання (активи)	Помірна	Висока (freeze / block)	↑
Роль банків / AML	Допоміжна	Ключова	↑
Судове навантаження	Стабільне	Зростає	↑
Ризик over-compliance	Низький	Високий	↑

Додаткові емпіричні висновки:

— спостерігається **зростання кількості випадків блокування активів**;

— посилюється **роль комплаєнс-рішень банків та фінансових установ**;

— відбувається **зміщення від штрафних санкцій до обмежувальних заходів** (*restrictive measures*).

Джерело: узагальнено автором на основі аналізу національної та міжнародної практики застосування фінансових санкцій.

Додаток 2

Судова практика щодо фінансових санкцій (деталізований аналіз)

№	Суд / справа	Фактичні обставини	Правове питання	Позиція суду	Значення для доктрини
1	Kadi and Al Barakaat v Council and Commission	Замороження активів особи за рішенням ООН/ЄС	Чи підлягають санкції перевірці на відповідність правам людини	Суд визнав обов'язковість повного судового контролю	Формування стандарту judicial review навіть у сфері безпеки
2	Rosneft (C-72/15)	Санкції ЄС проти іноземної компанії	Межі дискреції інститутів ЄС	Суд підтвердив можливість перевірки санкцій	Баланс між дискрецією та контролем
3	M.S.L., TOV v. Ukraine	Замороження активів української компанії	Чи забезпечено процесуальні гарантії	Виявлено порушення прав власності	Вимога fair balance + due process
4	S.C. Zorina International S.R.L. v. Romania	Податкові санкції + конфіскація	Пропорційність санкції	Санкція визнана надмірною	Стандарт proportionality test
5	Українська практика (КАС ВС)	Податкові донарахування	Межі доказування	Суд вимагає достатності доказів	Формування стандарту burden of proof

Додаток 3

У цьому додатку узагальнено практичні алгоритми застосування, перевірки та оскарження фінансових санкцій, що випливають із проведеного дослідження.

Практичні алгоритми застосування та оскарження фінансових санкцій

Алгоритм перевірки фінансової санкції судом	
Крок	Контрольне питання
1	Чи існує належна правова підстава для застосування санкції?
2	Чи встановлено факт правопорушення або наявність ризику?
3	Чи є достатня та належна доказова база?
4	Чи відповідає санкція принципу пропорційності?
5	Чи дотримано встановлену процедуру застосування?
6	Чи забезпечено право особи на захист?
Алгоритм дій юриста при оскарженні санкції	
Крок	Процесуальна дія
1	Аналіз правової підстави застосування санкції
2	Перевірка достатності та допустимості доказів
3	Оцінка пропорційності втручання
4	Виявлення процесуальних порушень
5	Підготовка та подання позовної заяви
Алгоритм санкційного комплаєнсу для банків	
Етап	Зміст дії
KYC	Ідентифікація та верифікація клієнта
Screening	Перевірка за санкційними списками
Monitoring	Аналіз фінансових операцій
Decision	Прийняття risk-based рішення
Reporting	Повідомлення уповноважених органів
Типові помилки правозастосування фінансових санкцій	
Помилка	Правовий наслідок
Недостатнє мотивування рішення	Скасування санкції судом
Надмірна дискреція	Порушення прав суб'єкта
Відсутність належних доказів	Визнання рішення незаконним
Over-compliance	Надмірне обмеження господарської діяльності

Додаток 4

Систематизована модель пропозицій *de lege ferenda*

Блок реформування	Елемент	Зміст
Нормативна структура	Розділ I	Загальні положення (поняття фінансових санкцій)
	Розділ II	Види санкцій (штрафні, обмежувальні, безпекові)
	Розділ III	Підстави застосування (порушення / ризик)
	Розділ IV	Процедура застосування
	Розділ V	Стандарти доказування
	Розділ VI	Судовий контроль
	Розділ VII	Санкційний комплаєнс
	Розділ VIII	Цифрова інфраструктура
Матеріально-правові стандарти	Пропорційність	Придатність → Необхідність → Співмірність
Стандарти доказування	Податкові санкції	balance of probabilities
	AML/CFT	risk-based suspicion
	Санкції безпеки	reasonable grounds
Процедурні гарантії	Етап 1	Адміністративний перегляд
	Етап 2	Суд першої інстанції
	Етап 3	Апеляція
	Етап 4	Перегляд за новими обставинами

Модель норми (приклад)

Стаття X. Принцип пропорційності фінансових санкцій

Фінансова санкція може бути застосована лише за умови, що вона:

— є придатною для досягнення легітимної мети;
— є необхідною (відсутні менш обтяжливі заходи);
— не створює надмірного втручання у права особи.

РОЛЬ МІЖНАРОДНИХ СТАНДАРТІВ ЩОДО ЗАХИСТУ ПІВ І ЗАДОВОЛЕННЯ СУСПІЛЬНИХ ІНТЕРЕСІВ У СФЕРІ ФАРМАЦІЇ

THE ROLE OF INTERNATIONAL STANDARDS IN PROTECTING CONSUMERS AND SERVING THE PUBLIC INTEREST IN THE PHARMACEUTICAL SECTOR

Kyryliuk A. V.,
PhD in Law, Associate Professor,
Associate Professor of the Department of Intellectual Property Law
and Patent Justice,
National University "Odesa Law Academy",
Odesa, Ukraine

Abstract. This study examines the complex impact of international standards on the legal regulation of the pharmaceutical market in the context of globalisation. The fundamental dilemma between the need for strict protection of intellectual property rights (IPR) as an incentive for scientific research and the state's duty to safeguard public interests, primarily the physical and economic accessibility of essential medicines, has been analysed.

Particular attention is paid to international standards and the TRIPS Agreement, which define the contemporary architecture of pharmaceutical law. The paper examines in detail the legal 'flexibilities' (TRIPS flexibilities), in particular the mechanisms of compulsory licensing and parallel importation, which act as safeguards against market monopolisation. It is argued that international

standards serve not only as technical quality regulations but also as the legal foundation for upholding the right to the highest attainable standard of health. It is established that the harmonisation of national legislation with international standards is a guarantee of national security and the sustainable development of the healthcare system.

It is highlighted how the harmonisation of national legislation with international requirements guarantees patient safety, the circulation of effective medicines, and fulfils the social responsibility of the pharmaceutical sector.

The necessity of improving the quality of pharmaceutical products through the implementation of international standards, which ensures the protection of consumer rights, is demonstrated.

The mechanisms by which international standards influence the fulfilment of public interests, as well as the safety and efficacy of medicines, are examined.

It is established that the implementation of international standards is a tool for enhancing the competitiveness of pharmaceutical companies and a key mechanism for realising the right to healthcare.

Keywords: intellectual property, pharmaceutical regulation, TRIPS Agreement, public health, patent monopoly, accessibility of medicines, international quality standards, pharmaceutical sector, protection of public interests, quality of medicines, patient safety, social responsibility.

Право на охорону здоров'я є одним з основних прав людини і тому є визначальним у формуванні державної політики у цьому напрямку. Реалізація і дотримання цього права залежать від багатьох факторів і не в останню чергу від балансу інтересів всіх учасників правовідносин, які при цьому виникають.

Оскільки сучасні технології відіграють у процесі реалізації права на охорону здоров'я дуже важливу роль, досягнення у біомедичній, фармакологічній науках забезпечують можливості для

розробки нових, безпечних і ефективних продуктів для охорони здоров'я населення. Права інтелектуальної власності, з одного боку, є важливим стимулом для розробки нових продуктів у сфері охорони здоров'я та водночас, є чинником серйозних суперечок між Світовою організацією торгівлі (СОТ) та Всесвітньою організацією охорони здоров'я (ВООЗ).

Основними проблемами, що виникають при зіткненні інтересів прав патентовласників і суспільством, є, зокрема, проблеми патентування лікарських препаратів та інших медичних виробів.

Справа в тому, що від 70 до 90 % (згідно з даними різних джерел) вартості фармацевтичної компанії складають права інтелектуальної власності, зокрема патентні права.

Зокрема, ВООЗ висловлює побоювання в тому, що патентний захист нових лікарських препаратів за відсутності механізму контролю над цінами може стати чинником подорожчання цих ліків.

Однак виготовлення аналогу препарату без згоди патентовласника є правопорушенням. Ці суперечки посилилися у зв'язку з прийняттям Угоди TRIPS, що діє в межах СОТ і передбачає уніфіковані правила регулювання патентів.

Проблема патентного захисту лікарських препаратів була предметом обговорення на міністерській конференції СОТ у столиці Катара Дохі. Бразилія і Індія запропонували негайно переглянути Угоду TRIPS, а саме ті її положення, що перешкоджають безоплатному копіюванню запатентованих ліків. В свою чергу, США і Швейцарія заперечували проти цього, аргументуючи свою позицію тим, що це зачіпає права розробників, що неприпустимо в умовах чесної конкуренції.

В результаті було прийнято Декларацію про Угоду TRIPS і громадську охорону здоров'я.

У ній зазначалося, що країнам, що розвиваються, надається можливість безоплатного копіювання лікарських препаратів в інтересах

захисту здоров'я населення. Так, у Декларації зазначається, що вона не перешкоджає і не повинна перешкоджати застосування членами заходів по захисту здоров'я людей. Виражаючи прихильність до Угоди по торгових аспектах прав інтелектуальної власності, Декларація акцентує увагу на тому, що Угоду TRIPS слід тлумачити і реалізовувати таким чином, щоби підтримувати права членів СОТ на захист здоров'я людей, і зокрема, на сприяння загальному доступу до лікарських засобів.

Аналіз відповідних положень Угоди TRIPS дозволяє зробити висновок про те, що у ній закладені певні можливості для запровадження гнучкої політики стосовно взаємоузгодження приватних і публічних інтересів у сфері права інтелектуальної власності.

Так, зокрема, у статтях 7 та 8 Угоди йдеться про те, що охорона і забезпечення прав інтелектуальної власності мають сприяти технічному прогресу і переданню та поширенню технологій для взаємної вигоди виробників та користувачів технічних знань, сприяючи соціально-економічному добробуту і досягненню балансу прав та обов'язків. У той же час при розробці або зміні законів і правил члени Угоди можуть вживати заходів, які є необхідними для охорони здоров'я населення і харчування і для сприяння у життєво важливих для їх соціально-економічного та технічного розвитку.

Хоча міжнародним базисом правового врегулювання питань прав інтелектуальної власності є TRIPS, різні країни імплементують положення цієї угоди до своїх законодавчих систем по-різному; тут існують два основних (протилежних) підходи.

Перший передбачає максимально повну імплементацію положень TRIPS, інколи навіть запровадження додаткових застережень, які угодою прямо не передбачені. Такий підхід відомий під назвою «ефект TRIPS-плюс» і користується найбільшою підтримкою з боку правовласників. Деякі експерти оцінюють його як надмірний. І саме такого підходу, дотепер і понині, дотримується Україна.

Другий підхід сповна використовує всі переваги так званого «гнучкого механізму TRIPS»: коли уряд запроваджує якомога помірніший рівень охорони права інтелектуальної власності з усіх, передбачених угодою, завдяки чому досягається більший рівень економічної доступності ліків для населення. Останнім часом цей підхід набуває все більшої популярності у світі.

Тоді як Україна дотримується першого («TRIPS-плюс») підходу, при проведенні загальних реформ у фармацевтичній галузі та розробці законопроектів у сфері спеціального законодавства спостерігається тенденція до застосування глобального підходу з одночасною його переорієнтацією таким чином, щоб отримати змогу скористатися важливими перевагами «гнучкого механізму TRIPS». Саме на цій межі знаходитиметься справедливий баланс між інтересами правовласників та правом населення України на отримання доступної за ціною фармакотерапії.

На сьогодні, у зв'язку з визнанням суспільного інтересу в підвищенні доступності лікарських засобів, все більше набуває актуальності необхідність ослаблення патентної монополії у сфері охорони здоров'я.

Одним із шляхів обмеження такої монополії є використання так званих «гнучких можливостей», що закріплені, зокрема, Угодою ТРІПС і передбачають існування «різних варіантів, за допомогою яких зобов'язання за Угодою ТРІПС можуть бути перенесені в національне законодавство, із тим щоб забезпечити національні інтереси, із одного боку, і при цьому не порушити положення та принципи Угоди ТРІПС, з іншого».

Інструмент «гнучкості» надає можливість вжити певних заходів з нейтралізації впливу виключних прав, заохочення конкуренції та розширення доступу до лікарських засобів».

Одним із таких інструментів є передбачена ст. 30 Угоди ТРІПС можливість надання обмежених винятків з виключних прав, що

надаються патентом, за умови, що такі винятки не будуть суттєво суперечити нормальному використанню патенту та завдавати суттєвої шкоди законним правам та інтересам його власника, із огляду на інтереси третіх осіб.

Також слід звернутися до механізму примусового ліцензування як ефективного засобу для вирішення проблем колізії інтересів.

Відповідні норми про примусове ліцензування містяться як в національному законодавстві, так і в законодавстві ЄС. Так Директивою 2001/83/ЕС «Про звід законів Співтовариства щодо лікарських засобів для людини» та Регламентом (ЄС) № 816/2006 «Про примусове ліцензування патентів, що стосуються виробництва лікарських засобів, для експорту до країн з проблемами в сфері охорони здоров'я» № 816/2006 встановлюється, що головною метою будь-яких правил, що регулюють виробництво, розподіл та використання лікарських засобів, є захист здоров'я населення (Ст. 1(2) Директиви 2001/83/ЕС) та механізмом забезпечення здоров'я населення є видача примусової ліцензії для виробництва та експорту лікарських засобів до країн із відповідними економічним показниками та проблемами в сфері забезпечення здоров'я населення (п. 5 Преамбули Регламенту (ЄС) № 816/2006).

Юридичні підстави використання державами механізму примусового ліцензування визначені також у Статті 31 Угоди ТРІПС і серед них: некомерційне використання в інтересах суспільства; використання за настання надзвичайного стану та крайньої необхідності; використання для запобігання ведення анти-конкурентної практики; взаємозалежності патентів.

Механізм примусового ліцензування був розроблений як гнучкий механізм подолання суперечностей між приватними та публічними інтересами. Але він стосується існуючих патентів. Тобто цей механізм, як зазначає О. Гургула, не може застосовуватися до заявок на патент. Отже, до моменту видачі патенту механізм

примусового ліцензування не може застосовуватись. Також під питанням є застосування примусового ліцензування до сертифікатів додаткової охорони, які є окремою формою захисту від патентів та конкретно не згадуються в ТРІПС.

Виникнення ідеї додаткової охорони було зумовлене перш за все особливостями фармацевтичної галузі та інноваційної діяльності в цій сфері. Розробка інноваційних лікарських засобів є тривалим процесом і потребує великих фінансових затрат, що часом можуть сягати сотень мільйонів доларів.

При цьому не завжди спроби розробки нового препарату здатні увінчатися успіхом — шанси на виділення речовини, що має лікувальні властивості, невеликі, їх оцінюють як 1 до 10 тисяч.

Після отримання (синтезу) молекули діючої речовини компанія-розробник проводить низку доклінічних та клінічних випробувань, метою яких є визначення ефекту від застосування відповідної речовини, виявлення побічної дії, визначення необхідної дози, підтвердження ефективності та безпечності для організму. Лише на підставі зазначених досліджень формується реєстраційне досьє і стає можливим реєстрація препарату та отримання дозволу на введення його в комерційний обіг.

У цілому цей процес може тривати до 10–13 років. До цього моменту власник патенту на інноваційну фармацевтичну розробку не може повноцінно реалізувати свої права, тобто період ефективної охорони згідно з патентом скорочується на строк, необхідний для надання дозволу регуляторного органу. Тим самим обмежується можливість отримання прибутку та повернення інвестицій, вкладених у вищезгадані дослідження.

З огляду на це виникає потреба в наданні додаткового строку охорони, який зможе компенсувати втрачений час на регуляторні процедури. Сполучені Штати Америки стали першою державою, яка запровадила механізм додаткової охорони (продовження строку дії

патенту) з метою заохочення інноваційних розробок у сфері фармації. Зокрема, у 50–70 роки минулого століття економіка США зазнала суттєвих змін: сотні дрібних фармацевтичних компаній, що існували в державі в 40-ві роки, були витіснені та замінені кількома десятками інноваційних гігантів, тобто національна фармацевтична промисловість була переорієнтована на здійснення інноваційної діяльності та передових розробок у сфері фармації.

Тому найбільші фармацевтичні корпорації почали домагатися введення в патентне законодавство США норм, які дозволяли б продовжувати строк дії патенту, виданого на фармацевтичний продукт.

Наслідком цього стало прийняття Закону про конкуренцію цін на лікарські засоби і відновлення строку дії патенту в 1984 році (The Drug Price Competition and Patent Term Restoration Act of 1984).

З огляду на наявний запит інноваційних фармацевтичних компаній у 1988 році були внесені схожі за змістом зміни до Закону про патенти в Японії, а в 1991 році аналогічно була доповнена частина друга статті 63 Європейської патентної конвенції.

Досить швидко норми, що передбачають надання додаткового періоду монополії, почали з'являтися на рівні національних законодавств окремих країн Європейського Союзу, зокрема, Італії та Франції, що викликало необхідність гармонізації законодавства. Так, у 1992 році за активної підтримки Європейської федерації фармацевтичної промисловості та асоціацій (EFPIA) був прийнятий Регламент Ради (ЄЕС) № 1768/92 (далі — Регламент № 1768/92) щодо створення сертифікатів додаткової охорони для медичних продуктів.

Відповідно до вступної частини Регламенту № 1768/92 прийняття цього акта зумовлене тим, що тривалий час, необхідний для отримання патенту та дозволу регуляторного органу на комерційний маркетинг зводить нанівець період ефективної правової

охорони винаходу, адже він є недостатнім для того, щоб забезпечити покриття інвестицій, вкладених у фармацевтичні дослідження.

Така ситуація призводить до того, що інноваційні розробки нібито караються, що у свою чергу створює ризик релокації науково-дослідницьких центрів, розміщених на території ЄС, до країн, де рівень правової охорони вищий (наприклад, США, Японія).

Важливо зазначити, що як у випадку продовження строку дії патенту в США та Японії, так і у випадку додаткової охорони за європейським підходом, ці механізми виникли у відповідь на наявні національні економічні інтереси, а саме — розвиток уже існуючої, належним чином розвиненої інноваційної фармацевтичної галузі.

Тобто додаткова охорона — це засіб підтримки і стимулювання інноваційних досліджень у фармацевтичній галузі, створений у відповідь на потребу виробника, а не механізм переорієнтації фармпромисловості чи її становлення як інноваційного сектору економіки.

Окремо варто наголосити, що метою додаткової охорони є стимулювання саме інноваційної діяльності у сфері фармації, що полягає в пошуку нових молекул та речовин і передбачає здійснення суттєво нових розробок, які потребують значних інвестицій та широких досліджень.

Водночас, як зазначається у вступній частині Регламенту № 1768/92, при вирішенні питання про надання додаткової охорони повинні бути враховані також публічні інтереси з огляду на складність та чутливість фармацевтичної галузі. Ця особливість зумовлює необхідність обмеження терміну такої охорони (до 15 років ефективної охорони, після прийняття кодифікованої версії Регламенту № 469/2009 — 15,5 років) та її обсягу (у контексті прив'язки до продукту як лікарського засобу, на який було видано дозвіл компетентного органу).

Додаткова охорона може бути надана лише винаходу, об'єктом якого є активний фармацевтичний інгредієнт лікарського засобу, процес отримання лікарського засобу або застосування лікарського засобу, засіб захисту тварин, засіб захисту рослин. Таке визначення об'єкта додаткової охорони повністю відповідає, зокрема, дефініції поняття «базовий патент», яка міститься в чинному Регламенті ЄС № 469/2009 щодо сертифікатів додаткової охорони для медичних продуктів.

Окрім того, права на додаткову охорону обмежені продуктом (активним фармацевтичним інгредієнтом або сукупністю активних фармацевтичних інгредієнтів лікарського засобу), введення в обіг якого дозволено відповідним компетентним органом згідно із законодавством, та його застосуванням відповідно як лікарського засобу, засобу захисту тварин, засобу захисту рослин у межах прав, що надавалися відповідним патентом на день подання клопотання про видачу сертифіката додаткової охорони, та є чинними за умови чинності такого дозволу.

Варто зазначити, що правова конструкція сертифіката додаткової охорони є досить складною в контексті визначення на практиці як її об'єкта, так і її обсягу.

Дуже детально цю проблематику проаналізував Ю. Капіца, зокрема щодо можливості поширення додаткової охорони на відмінні форми лікарського засобу (наприклад, у дозволі на використання вказана ін'єкційна форма, то чи поширюватиметься сертифікат на таблетовану); щодо комбінацій активних речовин, якщо вони не зазначені у формулі базового патенту; можливості додаткової охорони препаратів, які базуються на формулі Маркуша тощо.

Природа надаваних сертифікатом додаткової охорони прав суттєво відрізняється від патентних прав. Адже додаткова охорона — це не «логічне продовження» патенту, а специфічна «гібридна» правова конструкція, яка поєднує в собі як приватно-правову

(пов'язану з патентом), так і публічноправову складову (пов'язану з дозволом компетентного органу).

При цьому варто вказати, що Регламент № 469/2009 чітко встановлює, що сертифікат надає такі ж права, як і базовий патент, та має ті ж самі обмеження й зобов'язання.

Певний час (до прийняття кодифікованої версії регламенту) зберігалося «обмежувальне» тлумачення норм Регламенту № 1768/92, згідно з яким вважалося, що обсяг правової охорони, який випливає з сертифікату додаткової охорони, є не настільки широким, як обсяг правової охорони базового патенту — натомість сертифікат надає ексклюзивні права, обмежені виключно застосуванням препарату як лікарського засобу, що вказаний у відповідному дозволі.

З огляду на це наразі практика застосування положень щодо обсягу додаткової охорони може формуватися як у контексті звуженого тлумачення обсягу такої охорони, так і в більш широкому, прирівнюючи обсяг прав, що надаються сертифікатом, до обсягу прав, надаваних базовим патентом.

Як зазначає О. Літвінова, у процесі виробництва і виведення на ринок нових лікарських препаратів важливий не тільки позитивний науково-технічнии, економічнии, а й соціальний результат, оскільки фармація є соціально значущою галуззю, її діяльність впливає на рівень соціально-економічної та біологічної безпеки країни і людства в цілому.

Таким чином, додаткова охорона є більш гнучким механізмом, що може бути адаптованим до національних потреб.

З огляду на вплив Угоди ТРІПС, матеріально-правову базу патентного захисту складають Європейська патентна конвенція 2000 року [1] (ЄПК) та норми національного законодавства держав — учасниць ЄПК, які здебільшого відповідають положенням ЄПК. Обсяг правового захисту, питання, що стосуються реалізації та порушення патентних прав, регулюються нормами національного законодавства країн — членів ЄПК. Проте гармонізація патентного

законодавства ЄС частково була досягнута завдяки початковим зусиллям розробників Конвенції про європейський патент для Спільного ринку, укладеної 15 грудня 1975 року в Люксембурзі [2], яка, однак, так і не набула патентного захисту чинності. Найбільш значущими нормативно-правовими актами ЄС у сфері лікарських засобів є Директива 98/44/ЄС Європейського парламенту та Ради ЄС від 6 липня 1998 року про правовий захист біотехнологічних винаходів [3], Регламент Європейського парламенту та Ради ЄС № 469/2009 від 6 травня 2009 року про сертифікати для додаткової охорони для лікарських засобів [4] та Регламент Європейського парламенту та Ради ЄС № 1610/96 від 23 липня 1996 року про патент додаткової охорони для лікарських засобів та засобів захисту рослин [5].

Однією з причин комплексного характеру патентного законодавства ЄС є створення єдиного судового органу для розгляду та вирішення патентних спорів щодо порушення або визнання недійсними патентних прав. Варто зазначити, що наразі діє Угода про Єдиний патентний суд від 19 лютого 2013 року [6], реалізація положень якої сприяє більш ефективному функціонуванню патентної системи ЄС завдяки вищому рівню інтеграції матеріального та процесуального права Європейського Союзу.

Згідно з Угодою, Єдиний патентний суд створений для вирішення спорів, пов'язаних з європейськими патентами та єдиним європейським патентом. При цьому основою для прийняття рішень буде не лише право Європейського Союзу, ЄПК та інші міжнародні договори у сфері патентів, обов'язкові для всіх договірних держав, а й національне законодавство.

Заявку на реєстрацію патенту на фармацевтичний продукт можна подати як до європейського, так і до національного патентного відомства кожної з держав — учасниць ЄПК. Європейський патент, відповідно до ст. 64 ЄПК, починаючи з дати публікації повідомлення про його видачу в Європейському патентному бюлетені,

надає його власнику в кожній Договірній державі, де вимагається охорона, ті самі права, які надавав би національний патент, виданий у цій державі. Строк дії європейського патенту становить 20 років з дати подання заявки відповідно до ст. 63 ЄПК.

У Європейській патентній конвенції закріплено принцип відкритого доступу до неї представників будь-якої країни, незалежно від членства в Європейській патентній організації. Заявку на європейський патент може подати будь-яка особа незалежно від її громадянства чи місця проживання.

Згідно зі ст. 28 ТРІПС патент зобов'язує третіх осіб утримуватися від створення, використання, пропонування для продажу, продажу та імпорту продукту, що знаходиться під патентною охороною, без згоди правовласника. А якщо об'єктом патенту є спосіб, третім особам забороняється здійснювати аналогічні дії з продуктом, отриманим безпосередньо згаданим способом.

На практиці учасники фармацевтичного ринку подають заявку на реєстрацію патенту до уповноваженого органу ще на етапі розробки та дослідження певного лікарського засобу, коли до моменту його виходу на ринок проходить значний час, внаслідок чого фактичний строк дії 20-річної патентної охорони суттєво скорочується.

Більшість фармацевтичних компаній у ЄС подають заявки на реєстрацію патенту до Європейського або національного патентного відомства держави — учасниці ЄПК на підставі положень Договору про патентну кооперацію (PCT).

Треті особи мають право анонімно подавати заперечення проти реєстрації патенту, у свою чергу, заявник має право надати відповідь на це заперечення. У разі відхилення заявки заявник має право подати апеляцію до Великої апеляційної палати. Загалом Європейське патентне відомство реєструє патенти на винаходи, які відповідають критеріям патентоспроможності: новизни, винахідницького рівня та промислової придатності [7].

З точки зору критеріїв патентоспроможності фармацевтичних продуктів доцільно розглянути деякі практичні особливості реалізації положень європейського патентного законодавства.

У ст. 54(4) і 54(5) ЄПК встановлено вимоги до новизни та промислової придатності як умов патентоспроможності для субстанцій і композицій, які становлять основу фармацевтичних продуктів.

Важливе значення при визначенні критерію новизни у фармацевтиці має складання і тлумачення пунктів формули винаходу. Показовим прикладом може бути формула винаходу на продукт, охарактеризований способом його отримання, яка в практиці патентування фармацевтичних продуктів у ЄС [8] може бути подібною до формули винаходу без зазначення способу його виготовлення, оскільки сам продукт, як правило, не обмежується способом його отримання, зазначеним як ознака формули винаходу [9, с. 20]. Такий підхід загалом зумовлює значущість встановлення новизни винаходу шляхом визначення рівня техніки, відомого на дату пріоритету заявленого винаходу.

Водночас у фармацевтичній галузі умови патентування показань до застосування вже відомого лікарського засобу потребують особливої уваги.

Згідно зі ст. 54 ЄПК винахід вважається новим, якщо він не належить до рівня техніки. У європейському патентному законодавстві закріплено принцип, за яким зазначення певного способу або методу застосування у формулі винаходу запатентованого продукту не є обмеженням для застосування інших продуктів тим самим методом або способом. Обмеження стосується лише цільового застосування певного винаходу, що перебуває під патентною охороною [10, с. 116]. Тобто певне застосування може бути прив'язане до кількох продуктів, однак це не означає, що метод чи спосіб застосування винаходу можуть виступати фактором, що визначає новизну винаходу. Таким чином, при визначенні

критерію новизни є неприпустимим вважати додаткове застосування перевагою чи удосконаленням заявленого продукту у порівнянні з таким самим винаходом, формула якого не містить цього застосування як ознаки.

Однак для фармацевтичних продуктів, відповідно до ст. 54(4) і 54(5) ЄПК, передбачено виняток із зазначеного принципу. Нове показання до застосування відомої речовини або композиції, призначеної для використання у хірургії, терапії чи діагностиці, є вирішальним чинником при встановленні новизни винаходу. Загалом формула винаходу має оцінюватися на основі загальних норм щодо новизни як умови патентоспроможності, однак визнання специфіки фармацевтичної галузі, пов'язаної з визначенням новизни залежно від виявлення нового застосування відомого лікарського засобу як способу лікування, має суттєве значення для можливості проведення досліджень і розробок.

Однак у юридичній літературі триває дискусія про те, чи є мета винаходу правовою ознакою винаходу.

Показання до застосування має ознаку новизни, якщо воно не відоме з рівня техніки. Важливим моментом при цьому є обсяг правової охорони при виявленні терапевтичного застосування відомої речовини, яке раніше не використовувалося в медичних цілях. Так, наприклад, при розгляді Апеляційною палатою справи [11, с. 164] щодо правомірності відхилення заявки на реєстрацію патенту на продукт на підставі того, що формула винаходу не була обмежена визначеним терапевтичним застосуванням відомого хімічного з'єднання, Апеляційна палата дійшла висновку, що вказівка на певне застосування продукту як ознака формули винаходу не обмежує використання продукту тільки для заявленого застосування. Видається обґрунтованим, що на основі принципу рівноправ'я, якщо винахіднику нового хімічного з'єднання, яке потенційно може бути використане для лікування, надається абсолютна охорона,

то винахідник, який вперше створив умови для безпосереднього цільового застосування в терапії вже відомого з'єднання, не повинен бути обмежений у своєму праві на вказання в формулі винаходу його терапевтичного ефекту як сутності формули винаходу.

Зазначене рішення Апеляційної палати стало відправним у практиці Європейського патентного відомства при наданні широкого обсягу правової охорони для продуктів, які вперше використовувалися для медичного застосування [12, с. 139]. Так, наприклад, у рішенні Апеляційної палати 1984 року [13, с. 164] додатково було підтверджено, що перше встановлене показання до медичного застосування відомої субстанції або композиції, тобто перше виявлене застосування відомої речовини за медичним призначенням, визначає широку правову охорону для продукту.

Питання надмірної правової охорони фармацевтичних продуктів з встановленим показанням до медичного застосування, виявленим, дослідженим і доведеним вперше (первинне медичне застосування), вирішується в ст. 54(5) ЄПК, згідно з якою таке показання може бути підставою для реєстрації патенту на продукт. Варто зазначити, що в США застосовується більш обмежувальний підхід, відповідно до якого патент у розглянутому випадку видається лише на показання до застосування відомої речовини [14].

Умови, обсяг і рівень правової охорони, які можуть бути надані при виявленні другого або наступного нового показання до медичного застосування, можна узагальнити на основі практики розгляду справ Апеляційною палатою, яка діє на основі норм ЄПК при розгляді випадків, коли нове показання виявлено вперше відповідно до ст. 54(5) ЄПК, тобто застосування не належить до відомого рівня техніки.

У ряді рішень Великої апеляційної палати було закріплено, що всі виявлені пізніше показання до застосування відомих фармацевтичних продуктів підлягають охороні при подачі заявки в так званому

форматі формули винаходу «швейцарського типу», в рамках якого основне значення надається основному цільовому призначенню діючої речовини фармацевтичного продукту, коли «субстанція або композиція X використовується для виробництва лікарського засобу за його медичним застосуванням Y» [15]. Попри те, що в форматі «швейцарського типу» основне значення надається способу виробництва, Велика апеляційна палата визначила потенційну готовність встановлювати ознаку новизни винаходу на основі виявлення нових характеристик відомого продукту, таких як нові показання до застосування вже відомого лікарського засобу, тим самим створивши прецедент, який встановив виняток для загальних вимог, що висуваються для цілей встановлення новизни.

Для уникнення двозначності трактування в ЄПК щодо патентоспроможності нових виявлених показань до застосування вже відомих фармацевтичних продуктів у 2000 році була включена стаття 54(5), відповідно до якої загальні вимоги, що пред'являються для встановлення новизни винаходу, не можуть виключати патентоспроможність субстанції або композиції за певним показанням до застосування в хірургії, терапії чи діагностиці, за умови, якщо таке показання не випливає з відомого рівня техніки. При введенні цієї уточнюючої норми виникали питання про те, яке нове застосування можна вважати ознакою, що визначає як новизну, так і винахідницький рівень винаходу, які були вирішені в практиці розгляду спорів [16]. Так, було встановлено, що не виключаються з патентоспроможності лікарські засоби з новим способом їх застосування, хоча й у разі захворювання, лікування якого здійснювалося запатентованим лікарським препаратом з аналогічною речовиною чи композицією. Це положення також стосується і режиму дозування, якщо він є визначальною ознакою, не відомою з рівня техніки.

В національному законодавстві держав-членів ЄС є положення, ідентичні встановленим в статті 54 ЄПК. Наприклад,

в пункті 4 статті 46 Кодексу Італії про промислову власність передбачено правило, згідно з яким не виключається патентоспроможність речовини або комбінації речовин, що вже містяться в сучасному рівні техніки, але тільки для цілей їх нового використання.

Відповідно, використання відомих з рівня техніки речовини або композицій речовин для нового застосування, яке не відоме з рівня техніки, не спотворює новизну фармацевтичного продукту [17, с. 93].

В законодавстві ЄС немає кількісних обмежень для патентування показань до застосування вже відомих лікарських засобів. Однак межі дії патентних прав обмежені щодо конкретних показань до застосування певного лікарського засобу на основі грамотно складеної формули винаходу, в якій повинно бути чітко позначено нове цільове застосування лікарського засобу [18, с. 183], а не опис процесу чи механізму дії відомого показання до застосування, як, наприклад, у спорі [68] щодо застосування препарату в терапії діабету першого і другого типу, в формулі винаходу якого в якості визначальної ознаки було вказано «стимулювання розростання бета-клітин [19]» як технічного ефекту. І хоча раніше в формулі винаходу такий ефект не був описаний, він не був визнаний новим для цілей визначення патентоспроможності, оскільки розглядуваний винахід вже був запатентований як фармацевтичний продукт, що використовується в лікуванні діабету, і розглядуваний технічний ефект не був визнаний як нове застосування в терапевтичних цілях, оскільки був складовою частиною та визначальною частиною відомого терапевтичного ефекту в цій конкретній терапії.

Способи визначення наявності або відсутності винахідницького рівня винаходів, особливо для лікарських препаратів, загалом мають достатньо суб'єктивний характер, оскільки при такому визначенні використовується за загальним правилом критерій очевидності

винаходу для фахівця середнього рівня, що має стандартний набір знань у певній галузі.

В практиці правового регулювання патентування в ЄС підходи до визначення винахідницького рівня винаходу були узагальнені Апеляційною палатою [20, с. 162] наступним чином:

— спочатку встановлюється винахід, відомий з рівня техніки, за своїми ознаками схожими з винаходом, що заявляється для реєстрації;

— потім оцінюється технічний результат, що досягається внаслідок застосування винаходів, які порівнюються;

— далі визначається технічне завдання, яке вирішується при застосуванні заявленого для реєстрації винаходу;

— на завершення визначається, чи встановив би фахівець можливість досягнення заявленого в формулі технічного результату і вирішення технічного завдання шляхом реалізації технічних характеристик, зазначених у заявці, для визначення неочевидності винаходу з існуючого рівня техніки.

Введення останньої вимоги щодо необхідності оцінки умов патентоспроможності винаходу на основі врахування вказаних у формулі винаходу технічних характеристик, які є невід'ємною умовою досягнення заявленого технічного результату, є важливим обставиною щодо патентування лікарських засобів, особливо може застосовуватись до біотехнологій, оскільки при аналізі винахідницького рівня застосування стандартних технічних параметрів не завжди може призвести до вирішення задачі, поставленої заявником. Тому при оцінці винахідницького рівня слід виходити з принципів розумності, зокрема, коли є розумне підґрунтя очікувати досягнення успіху, що проявляється в заявленому технічному результаті, що не можна плутати з «надією на успіх» [21], тобто низькою ймовірністю вирішення технічної задачі, наприклад, при використанні стандартних аналітичних методів, не актуальних і не підходящих у конкретному

випадку. Застосування цього підходу не виключає використання стандартних підходів у оцінці винахідницького рівня, застосування яких може бути достатнім [22], а вимагає врахування специфічних характеристик винаходу в кожному конкретному випадку, виходячи з об'єктивних даних, що містяться в описі винаходу.

На відміну від розглянутих ознак патентоспроможності фармацевтичних продуктів, в ЄС критерій промислової застосовності в більшості випадків не розглядається як умова, що є складною для визначення.

Згідно зі статтею 57 ЄПК, винахід вважається промислово застосовним, якщо він може бути виготовлений або використаний у будь-якій галузі промисловості, в тому числі в сільському господарстві. Разом з тим, наприклад, умови абстрактного промислового використання винаходу знайшли своє відображення в Директиві про біотехнології [23]. Згідно з Директивою, промислове застосування послідовності генів, включаючи їх функції (призначення), повинно бути в описі винаходу.

Одночасно, виходячи з практики [24] Апеляційної палати патентного відомства, можна зробити висновок, що фармацевтичний продукт як об'єкт винаходу не просто повинен бути цікавим з точки зору дослідницького потенціалу, а й повинен містити реальний терапевтичний механізм дії для цілей лікування певного захворювання або підтримання якості життя пацієнта. У разі недостатності розуміння функції діючої речовини за медичним призначенням можна зробити висновок про невідповідність фармацевтичного продукту умові патентоспроможності «промислова застосовність».

Навіть якщо пряме функціональне призначення в лікуванні захворювання виявити важко, однак речовина має певні терапевтичні характеристики, наприклад, протизапальний ефект або впливає на відновлення і оздоровлення тканин, внаслідок чого має потенціал для створення та вдосконалення нових лікарських засобів, як

у рішенні щодо оцінки дії синтетичного білка [25], то може бути визнано відповідність винаходу умові «промислова застосовність». При цьому належна увага повинна бути приділена опису цільового призначення винаходу, умовам і методам його промислового застосування для вирішення поставленої технічної задачі [26], а також доказам дії заявленого об'єкта, який отримано експериментальним шляхом [27], незважаючи на те, що окремі ознаки препарату можуть вимагати окремої оцінки та вивчення [28].

Зважаючи на розгляд критеріїв оцінки умов патентоспроможності фармацевтичних продуктів, що склалися в рамках правозастосовної практики в ЄС, необхідно відзначити, що додатковою невід'ємною умовою розгляду особливостей патентоспроможності лікарських засобів є питання про виключення з патентоспроможності для фармацевтичних продуктів.

Забезпечення балансу прав та інтересів правоволодільця і суспільства досягається введенням виключень щодо деяких об'єктів правової охорони в законодавстві ЄС. Згідно зі статтею 53(c) ЄПК, європейські патенти не видаються на способи лікування людей або тварин за допомогою хірургії чи терапії та методи діагностики, що застосовуються в медицині або ветеринарії. Це положення відповідає Угоді ТРІПС, в якій зазначається, що держави можуть виключати з області патентування діагностичні, терапевтичні та хірургічні методи лікування людей або тварин. Разом з тим, як встановлено в статті 53(c) ЄПК, вказане виключення не поширюється на продукти, зокрема речовини (субстанції) або склад речовин (композиції), які використовуються в цих способах або методах, а саме: в хірургії, терапії та діагностиці. Таким чином, лікарські препарати, вакцини та інші фармацевтичні продукти, що використовуються в медицині, є об'єктами патентної охорони.

Більш глибокого аналізу потребує розгляд можливості патентування фармацевтичних продуктів у випадках, що стосуються

публічного порядку, наприклад, повя'заних з технологією застосування ембріональних стовбурових клітин при розробці інноваційних лікарських препаратів. Сучасний рівень розвитку фармацевтичної галузі безсумнівно пов'язаний з біотехнологіями та науковими досягненнями, зокрема в галузі генетичної терапії.

У зв'язку з цим важливо проаналізувати випадки комерційного використання фармацевтичних продуктів, використання яких може суперечити публічному порядку згідно зі ст. 53(а) ЄПК. Згідно зі ст. 27(2) ТРІПС, держави-члени можуть виключати з області запатентованих винаходів ті, комерційному використання яких необхідно запобігти на їхніх територіях для охорони суспільного порядку або моралі. Однак умови застосування таких виключень досить вузькі.

Умови застосування принципу публічного порядку мають надзвичайно важливе значення з метою підтримки подальшого розвитку технологій і усунення можливих зловживань, які ставлять під загрозу такий розвиток. Для забезпечення балансу між принципом публічного порядку і необхідністю розвитку технологій у ЄПК встановлено, що комерційне використання винаходу не може розглядатися як таке, що суперечить суспільному порядку або моралі тільки тому, що воно заборонене законодавчими або нормативними положеннями у всіх або деяких Договірних державах. Тобто якщо винахід заборонено для обігу, це не означає, що він не підлягає патентуванню.

Принцип публічного порядку не може застосовуватися лише через те, що використання винаходу є неправильним або нецільовим. Так, наприклад, зброя та інші технології, використання яких пов'язане з небезпекою, визнаються об'єктами патентування. Щодо обмежень у патентуванні відповідно до ст. 53 ЄПК, позиція Європейського Союзу була сформульована так, що ці обмеження не допускаються і, як наслідок, вимагають надання більш широких правових норм для патентування в галузі біологічних винаходів.

Питання про співвідношення забезпечення необхідного рівня захисту прав і гідності людини та використання останніх досягнень у розвитку біотехнологій, генної інженерії і технологій у сфері репродукції людини є неоднозначним. З метою визначення деяких меж для можливого використання біотехнологій у Директиві про біотехнології в ст. 6(2) [29] був закріплений відкритий перелік прикладів, які підпадають під виключення з патентоспроможності. Вказаний перелік був імплементований також у Правило 28 ЄПК, згідно з яким не підлягають патентуванню такі види винаходів у галузі біотехнологій: способи клонування людини; способи модифікації зародкової генетичної ідентичності людини; використання людського ембріона в промислових або комерційних цілях; способи модифікації генетичної ідентичності тварин, ризик шкоди від застосування яких перевищує користь від їх застосування в медичних або ветеринарних цілях, а також тварин, які виникають в результаті застосування таких способів.

Заборона на використання ембріона людини в промислових або комерційних цілях викликає суперечки, оскільки це може перешкоджати вдосконаленню технологій у галузі вивчення ембріональних стовбурових клітин та їх можливого використання у фармацевтичній галузі для лікування важких захворювань [30, с. 43].

У рішенні Великої апеляційної палати [31] було підкреслено, що, згідно з правилом 28(c) ЄПК, не допускається патентування біотехнологічних винаходів, розробка, отримання або виробництво яких пов'язані з використанням методу знищення ембріона людини, навіть якщо цей метод не є складовою частиною формули винаходу. Тобто встановлена заборона не поширюється на можливість патентування аналогічних винаходів, створення яких не пов'язане з використанням згаданого методу.

Позиція Великої апеляційної палати була пізніше підтверджена Європейським судом [32] в рамках тлумачення ст. 6(2)(c)

Директиви про біотехнологій. Європейський суд встановив, що не підлягає патентуванню винахід, спосіб виробництва якого неминуче призводить до знищення людського ембріона або заснований на його використанні як на вихідному матеріалі для виробництва. У випадках, коли опис процесу виробництва продукту не включає жодних відомостей про характер використання ембріона в ньому, такий продукт також не підлягає патентній охороні.

Вказане розя'снення було остаточно підтверджено Великою Палатою Європейського суду з прав людини в рішенні від 18 жовтня 2011 [33] року. Використання ембріона людини було додатково обмежено науково-дослідницькими цілями, в додаток до промислових і комерційних, з умовою, що патентування допускається лише за умови використання ембріона в терапевтичних (лікувальних) і діагностичних цілях.

Отже, спосіб виробництва фармацевтичного продукту не завжди є ознакою, що визначає новизну винаходу, оскільки сам продукт, як загальне правило, не обмежується способом його виробництва. Проте для деяких фармацевтичних продуктів, особливо біологічних, як об'єктів патентного захисту, зазначена ознака може мати суттєве значення для визначення новизни винаходу, оскільки спосіб виробництва біологічного препарату може впливати на його терапевтичні властивості.

Нове застосування відомої речовини або композиції як спосіб лікування є визначальним критерієм при встановленні новизни фармацевтичного продукту. Обсяг правової охорони у випадку виявлення нового застосування відомої речовини або композиції, які раніше не застосовувалися як фармацевтичний продукт у медичних цілях, поширюється на продукт у цілому. Однак при встановленні нових показань до застосування вже відомого фармацевтичного продукту обсяг правової охорони поширюється виключно на такі нові показання.

Для відповідності фармацевтичного продукту критерію промислової придатності повинні бути надані докази того, що цей продукт має реальний терапевтичний механізм дії.

Публічний порядок при патентуванні фармацевтичних продуктів, пов'язаних із технологією застосування ембріональних стовбурових клітин, не поширюється на випадки, не пов'язані із використанням методу знищення ембріона людини.

Відповідно до параграфа 101 розділу 35 Зводу законів США будь-хто, хто винаходить або робить відкриття будь-якого нового та корисного способу, пристрою, способу виробництва або складу речовини, або будь-якого нового та корисного їхнього вдосконалення, може отримати на них патент відповідно до умов та вимог розділу 35 Зводу законів США, положення якого поширюються на відносини, суб'єктом яких є будь-яка особа незалежно від громадянства. У США — державі, яка є членом Паризької конвенції з 1887 року, щодо охорони промислової власності діє національний режим.

У Розділі 35 частини 2 Зводу законів США встановлено норми правового регулювання щодо визначення патентоспроможності винаходів та процедури видачі патентів. Для більш комплексного аналізу умов патентування та здійснення патентних прав на фармацевтичні продукти доцільно розглянути практичні аспекти застосування законодавства США, згідно з яким для задоволення вимог патентоспроможності винахід як об'єкт патентного захисту, так само як і в європейському патентному законодавстві, повинен відповідати критеріям новизни, неочевидності, під якою розуміється винахідницький рівень, та промислової застосовності.

Як у ЄПК, так і в Зводі законів США встановлено критерії патентоспроможності винаходу, що включають загальний перелік об'єктів, які підлягають патентуванню. Однак у межах встановлених вимог є відмінності.

Згідно з параграфом 101 розділу 35 Зводу законів США патентоспроможні об'єкти включають п'ять категорій, а саме: спосіб, пристрій, спосіб виробництва, речовину або композицію речовин, а також їхнє нове та корисне вдосконалення. До непатентоспроможного класу об'єктів включені закони та продукти природи, природні явища, теоретичні абстрактні ідеї та концепції, розумові процеси, що є, по суті, суспільним надбанням у сфері отримання нових знань та розвитку науки [34]. Для порівняння, в ЄПК немає вичерпного переліку об'єктів, що є винаходами, проте є перелік об'єктів, які не визнаються винаходами. Згідно зі ст. 52(2) ЄПК винаходами не визнаються відкриття, наукові теорії та математичні методи; естетичні рішення; схеми, правила та методи інтелектуальної або господарської діяльності, а також програми для ЕОМ; просте подання інформації.

Визначення критерію новизни як умови патентоспроможності об'єкта в США ґрунтується на тому, що винахід визнається новим, якщо він відрізняється від уже існуючого винаходу, відомого громадськості. При цьому, згідно зі ст. 102 Посібника з проведення патентної експертизи в США [35], враховується інформація про відомий винахід, опублікована або іншим чином розголошена за межами США, тобто встановлюється критерій світової новизни, як у ЄС, однак у США винахідник або третя особа за згодою винахідника мають право протягом року з моменту розголошення інформації про винахід подати заявку на реєстрацію патентних прав. В ЄПК встановлено вимогу абсолютної новизни, згідно з якою будь-яке публічне розкриття інформації про винахід не тільки винахідником, але й будь-якою третьою особою означатиме, що новизна відсутня.

Хоча у ст. 55 ЄПК визначено шестимісячний пільговий період, протягом якого розкриття винаходу не порушує його новизну, він діє у виняткових випадках: у випадках очевидного зловживання, вчиненого стосовно заявника, або експонування заявником свого винаходу на офіційно визнаних виставках. Таким чином, при

розголошенні інформації про винахід поза встановленими випадками у США, ЄС або РФ новизна втрачається в ЄС, однак зберігає свою дію протягом року у США — з моменту публічного розкриття інформації про винахід самим винахідником або іншою особою за згодою винахідника.

Зазначений річний пільговий період може створювати обмеження для третіх осіб, які першими подали заявку на реєстрацію патенту. Однак вважаємо, що для фармацевтичних продуктів такий підхід видається необхідним, оскільки компенсує не тільки витрати, пов'язані з процесом їх розробки та досліджень до моменту становлення як потенційного предмета пропозиції до продажу, але й є стимулом до наукових досліджень у пошуку нових технічних рішень третіми особами, які мають намір надалі вдосконалювати винахід, інформація про який була розкрита винахідником. Зазначений позитивний ефект пільгового періоду, що діє в США, підтверджується думкою судді Верховного суду США Стівена Брейєра: «Патентне право передбачає досягнення досить непростого компромісу, тому що воно прагне просувати науку та інновації, надаючи винахіднику тимчасову монополію на прибуток від використання його винаходу».

Характерною ознакою фармацевтичних продуктів є наявність у їхньому складі компонентів, які можуть бути запатентовані або самі по собі окремо втратили новизну. Як зазначається в юридичному середовищі, про втрату новизни можна говорити тоді, коли стали відомі абсолютно всі відомості або коли повністю розкрита істотна інформація про лікарський засіб, що описує його невід'ємні ключові ознаки. Таким чином, якщо комбінація речовин, що представляє собою відомі істотні ознаки фармацевтичного продукту, є унікальною, розроблена та розкрита вперше, заявлений об'єкт має бути визнаний таким, що відповідає критерію «новизни». Це положення випливає з параграфа 102 розділу 35 Зводу законів США [36], як і зі ст. 54 ЄПК,

розглянутої в параграфі 2 цієї глави. Наприклад, якщо фармацевтичний продукт являє собою унікальну композицію елементів «А», «Б» і «В», він буде вважатися новим, навіть якщо один або два із зазначених елементів у будь-якій їхній комбінації вже є складовими іншого продукту. Однак якщо існує продукт, у якому міститься така композиція з додатковим невідомим четвертим елементом «Г», вона втратить свою унікальність, оскільки для задоволення вимоги новизни фармацевтичний продукт не повинен містити всі елементи та ознаки іншого відомого винаходу.

Особливістю, якою визначається новизна винаходу для фармацевтичного продукту, є виявлення нових показань щодо його медичного застосування. У США закріплено підхід, відмінний від ЄС, до встановлення новизни винаходу в галузі фармацевтики у разі виявлення медичного застосування відомого сполучення речовин. Якщо в ЄС при вперше виявленому показанні щодо медичного застосування відомого сполучення речовин патент надається на фармацевтичний продукт, то в США стосовно патентування показань до застосування відомої речовини або сполучення речовин, виявлених вперше для використання в терапевтичних медичних цілях, патент видається не на продукт, а лише на його застосування.

Дійсно, згідно зі ст. 1 Угоди ТРІПС держави-члени СОТ мають свободу у визначенні належного методу виконання положень зазначеної Угоди в рамках своїх правових систем. Відповідно, держава-член СОТ має свободу у визначенні патентоспроможності продукту в цілому при виявленні його медичного застосування, виявленого вперше, як це встановлено в ЄС. Однак така широка правова охорона видається на перший погляд надмірною, оскільки речовина або сполука речовин у такому випадку вже відома. Разом з тим, з огляду на те, що застосування в медичних цілях такої відомої речовини або сполуки виявлено вперше і створено умови для такого застосування у фармакотерапії, подібний підхід видається

обґрунтованим. Незважаючи на те, що в США застосовується обмежувальний підхід при вперше виявленому медичному застосуванні відомого сполучення речовини, правовий захист надається лише щодо показань до застосування, а не на продукт загалом, така можливість виправдана з огляду на збільшення кількості дженериків на ринку, які можуть бути застосовні за іншим незапатентованим показанням. З огляду на те, що досягається терапевтичний ефект як новий технічний результат використання відомої речовини, патентування показань щодо застосування фармацевтичного продукту є доцільним.

Водночас у законодавстві США не встановлено обмежень щодо призначення лікарського препарату, що перебуває під патентним захистом, за певним показанням. Згідно з параграфом 287(c) [37] розділу 35 Зводу законів США лікар під час здійснення своєї професійної діяльності не несе відповідальності за можливе призначення дженерика за запатентованим показанням до застосування.

Згідно зі Зводом законів США фармацевтична компанія несе відповідальність у разі, якщо стимулює призначення лікарем лікарського препарату з порушенням патентних прав патентовласника, наприклад призначення дженерика за запатентованим показанням до застосування. Таке порушення характеризується, згідно із законодавством США, як непряме порушення. До категорії непрямих порушень належать випадки, коли особа сприяє або підштовхує третю особу до порушення патентних прав. Відповідальність при цьому несе особа, яка спонукає до вчинення порушення, оскільки саме вона мала намір [38]. Хоча в ряді випадків непряме порушення може випливати з прямого, оскільки до обігу на ринку допускаються лише зареєстровані лікарські засоби, а виведення препарату на ринок з порушенням чинного патенту на підставі отримання дозволу уповноваженого органу є прямим порушенням.

При прямому порушенні особа без згоди правовласника створює, використовує, пропонує до продажу, продає на території США або імпортує на територію США запатентований продукт протягом терміну дії правової охорони. При цьому наявність наміру порушити або навіть обізнаність про наявність чинних патентних прав не вимагається.

Питання про можливе порушення патентних прав може бути вирішене і під час реєстрації відтвореного лікарського препарату в FDA. Наприклад, під час розгляду судом спору щодо реєстрації в FDA відтвореного перорального протизаплідного засобу за запатентованим показанням щодо застосування [39] не було визнано порушення патенту в частині реєстрації одного із запатентованих показань щодо застосування. Обґрунтуванням у даному випадку було те, що дія патенту поширювалася на одночасне застосування за трьома зареєстрованими показаннями, включаючи такі показання застосування, як контрацепція та антиандрогенний ефект. Однак, оскільки виробник дженерика запитував у FDA реєстрацію лише на одне показання — контрацепцію, суд не визнав факт порушення патенту.

На підставі наведеного прикладу можна зробити висновок, що при патентуванні єдиного вперше виявленого показання щодо застосування відомої сполуки ступінь правової охорони фармацевтичного продукту в частині його застосування за певним призначенням є більш стійкою, ніж при одночасному патентуванні декількох показань. Оскільки застосування дженерика за одним із показань, що становить частину запатентованого комплексу показань щодо медичного застосування, не є порушенням патенту. Порушенням патенту буде реєстрація в FDA та застосування копії оригінального препарату в цілому одночасно за всіма показаннями, що складають єдність винаходу.

Незважаючи на те, що патентування продукту в ЄС при виявленні вперше показань щодо застосування у терапії відомої сполуки

видається найбільш надійним ступенем правової охорони для фармацевтичних продуктів, патентний захист способу, що характеризує застосування відомої сполуки за новим призначенням, також видається обґрунтованим, оскільки не обмежує інших господарюючих суб'єктів у розробці дженериків за іншим показанням, що не охоплюється патентом.

При встановленні винахідницького рівня винаходу, що патентується, у судовій практиці США за основу беруться такі умови, сформульовані Верховним судом [40]: обсяг правової охорони та зміст опису відомого винаходу, середній рівень компетентності фахівця у певній галузі техніки, відмінності заявленого винаходу від уже відомого, об'єктивні докази неочевидності винаходу для фахівця. Верховний суд також встановив вторинні критерії визначення винахідницького рівня, такі як: комерційна ефективність з точки зору реальної доступності винаходу на ринку та давно назріла потреба в ньому. Згодом у 2007 році Бюро з патентів і товарних знаків США, ґрунтуючись на рішенні Верховного суду, яке підтвердило необхідність застосування зазначених умов, встановило вимогу, згідно з яким суд повинен оцінити, чи перевершує, за очікуванням фахівця у певній галузі, заявлене вдосконалення у відомому винаході передбачуваний та очевидний результат використання винаходу, відомого з рівня техніки відповідно до його призначення [41] Рішення Верховного суду, в якому зазначена вимога була закріплена, стосувалося констатації очевидності винаходу, що відноситься до системи механізму дії педалі гальма транспортного засобу. Верховним судом було встановлено очевидність заявленого об'єкта на підставі того, що педаль залишатиметься у фіксованому положенні незалежно від наявності нової ознаки у складі винаходу, зокрема, чи буде закріплений датчик на опорному елементі педалі чи ні, з огляду на те, що всі елементи та ознаки винаходу є очевидними з рівня техніки. Тобто

функціональне призначення педалі не зміниться, а залишиться очевидним для фахівця, який застосовує базові відомі методи оцінки винаходу, що є відомим для нього.

Застосування подібного методу встановлення винахідницького рівня для фармацевтичних продуктів не завжди є прийнятним, оскільки доповнення до складної молекулярної структури лікарського препарату на перший погляд незначною складовою у вигляді зміни лікарської форми або дозування може бути підставою для досягнення нового терапевтичного ефекту відомого фармацевтичного продукту.

Удосконалення підходів у застосуванні вимоги, встановленої Верховним судом, для оцінки критерію очевидності винаходу для лікарських засобів було надалі проведено на практиці.

Для лікарських препаратів зі складною структурою, особливо щодо біотерапевтичних препаратів, встановлення очевидності винаходу, що включає ознаки відомого винаходу, має здійснюватися на основі заявлених в описі винаходу особливостей. Такі препарати, незважаючи на наявні в них подібні ознаки, відомі з рівня техніки, можуть мати різний технічний результат, а саме, різні функціональні характеристики фармацевтичного продукту внаслідок іншого способу виробництва і, можливо, як наслідок, іншого механізму взаємодії речовин у ньому.

Копіювати біологічні препарати набагато складніше [42]. Так, наприклад, біологічні препарати «Епоген» та «Епрекс» для лікування анемії [43] з однаковою амінокислотною послідовністю, вироблені з використанням однієї технології рекомбінантних ДНК [44, с. 613.], через невеликі відмінності в лікарській формі мали різну дію. При прийомі препаратів «Епрекс» вироблялася значно більша кількість антитіл, що призводило не просто до відсутності будь-якої реакції, але також і до погіршення стану пацієнта.

У зв'язку з цим варто зазначити, що процес затвердження біологічних препаратів займає набагато більше часу і вимагає значних витрат,

що, безсумнівно, відбивається на їхній вартості. Річна вартість препарату «Авастин» для лікування раку становить близько 60 тис. дол. США, а 300 тис. дол. США на рік становить вартість препарату «Церезим», що застосовується в терапії хвороби Гоше [45].

При патентуванні біотерапевтичних препаратів на практиці виявляються стратегії, що застосовуються фармацевтичними компаніями, які не завжди реалізуються добросовісними методами. Так, наприклад, так звана стратегія оновлення патенту передбачає охорону винаходу при реєстрації патентних прав на окремі ознаки цього винаходу. Особливо часто цей спосіб продовження терміну дії патенту застосовується у сфері виробництва біологічних лікарських препаратів. Так, наприклад, якщо заявка на реєстрацію патенту на діючу речовину була подана у 2005 р., а згодом — на спосіб виробництва цієї речовини у 2010 р., то компанія, яка розробила дженерик, виготовлений за тією ж технологією, не зможе випустити його в обіг до 2030 р., хоча термін дії патенту на речовину закінчиться у 2025 р.

Класичним прикладом оновлення патенту стало патентування продукту обміну, що утворюється при вживанні запатентованого антигістамінного препарату «Кларитин» [46], термін охорони якого закінчувався на два роки раніше, ніж термін патенту на продукт обміну, заснованого на ньому. Однак патент на продукт обміну (вторинний патент з пізнішою датою видачі) було скасовано [47] на тій підставі, що даний продукт утворюється при кожному прийомі препарату людиною і, відповідно, має відомий терапевтичний ефект, як і раніше запатентований фармацевтичний продукт. В одному з досліджень, що стосується трьох запатентованих продуктів, які використовують метод оновлення патенту, було зроблено висновок про те, що використання такого методу призвело до втрати 1,5 млрд дол. США дохідної частини бюджету, які могли бути використані для цілей реалізації

програми безкоштовної медичної допомоги при продажу відтворених препаратів.

Однак варто визнати, що з урахуванням умов патентоспроможності винаходів, коли певні зміни у відомому винаході можуть призвести до раніше не виявленого результату, заборона на оновлення патенту є необґрунтованою в тій мірі, в якій не стосується зловживання виключними правами.

У той час як при оновленні патенту вторинні патенти ґрунтуються на первинному, виникає проблема при патентуванні змін лікарського препарату, на який було зареєстровано первинний патент. Такі зміни можуть бути визнані очевидними в ряді випадків. Так, наприклад, у міру наближення дати закінчення терміну дії патенту на фармацевтичний продукт омепразол компанія зареєструвала патент на езомепразол. Однак суд визнав вторинний патент недійсним, оскільки відмінності в якісних характеристиках препарату були незначними порівняно з препаратом, на який було видано первинний патент [48]. Дійсно, у науковій літературі зазначається, що на сьогоднішній день немає доказів того, що зазначені препарати, незважаючи на деякі відмінності, що існують між ними, мають помітно різний ступінь ефективності при терапії кислотозалежних захворювань.

Однак у практиці оновлення патенту представлено приклади сумлінних дій виробників фармацевтичних продуктів, коли винахід із внесеними змінами визнавався таким, що відповідає критерію «винахідничого рівня».

Наприклад, у спорі щодо порушення патентних прав на антибіотик кларитроміцин [49], відповідач — виробник дженерика заявив зустрічну вимогу про невідповідність винаходу винахідницькому рівню. Відповідач стверджував, що для досягнення поліпшення дії антибіотика, заявленого патентовласником як досягнення технічного результату, фахівець середнього рівня у відповідній галузі знань міг би здійснити аналогічні поліпшення, що, у свою чергу,

могло призвести до заявлених фармакологічних властивостей шляхом використання пролонгованого вивільнення діючої речовини, тобто застосування рутинного дослідження та доступного експериментального методу. При цьому відповідач не довів, що фармакологічні властивості заявленого винаходу випливають із рівня техніки у порівнянні з лікарськими засобами, складові ознаки яких відомі з рівня техніки та містяться у заявленому винаході.

Проте правовласник довів, що фармакологічні властивості заявленого винаходу не випливають із рівня техніки, оскільки екстраполяція очевидних для фахівця середнього рівня результатів експерименту "in vitro" 190 на терапевтичну дію препарату, яку можна довести в дослідженні "in vivo", є неприпустимою, оскільки на підставі такої екстраполяції може скластися недостовірне уявлення про терапевтичні властивості препарату. Доведений правовласником факт іншої дії препарату на живому організмі, у порівнянні з його очевидною дією в пробірці, став підставою для твердження, що очевидність лікарського препарату, яка може констатуватися на підставі даних, отриманих у дослідженні "in vitro", може бути відсутньою в результаті проведення досліджень "in vivo".

Крім того, у розглянутому рішенні суд вказав, що при встановленні Верховним судом підходу щодо виявлення винахідницького рівня на підставі стандартних оцінок, прийнятних для відомих винаходів, не було закріплено, що очевидність винаходу презумптується у випадку, якщо ознаки заявленого об'єкта або їх сукупність відомі з рівня техніки. Видається, що оцінка винахідницького рівня для лікарських засобів повинна проводитися з урахуванням усіх описаних у заявці особливостей та технічних характеристик, спрямованих на досягнення заявленого результату та заснованих на застосуванні нестандартних для відомих винаходів методів оцінки їх функцій.

Аналіз проблеми вибору права, що застосовується до відносин щодо охорони патентних прав на фармацевтичні продукти, показав,

що висока технологічність виробництва фармацевтичних продуктів, а також процес розробки та виробництва фармацевтичних продуктів, який може одночасно зачіпати багато держав, зокрема, коли використання виключного права пов'язане з подальшими вдосконаленнями щодо лікарського препарату, можуть впливати на колізійно-правове регулювання договірних відносин, пов'язаних з використанням запатентованого продукту ліцензіатом.

Формула lex loci protectionis — закон держави, щодо якої робиться запит відносно охорони, є стійкою колізійною прив'язкою при визначенні деліктного та інтелектуального статутів до відносин, пов'язаних з використанням запатентованого лікарського засобу, виходячи з принципу територіальності. Однак у договірних зобов'язаннях, наприклад, у разі внесення зусиллями ліцензіата певних поліпшень фармацевтичного продукту, або коли згідно з договором ліцензіат зобов'язується провести подальші дослідження та розробку запатентованого лікарського препарату та/або підтримувати чинність патенту, доцільно прийняти рішення яке право має застосовуватися за формулою характерного виконання. Вибір права має ґрунтуватися на законі держави, де фармацевтичний продукт буде використовуватися у випадку, якщо право передається за ліцензійним договором на територію однієї держави.

Такий вибір права вважається прийнятним, зокрема тому, що зазначені дії ліцензіата можуть безпосередньо впливати на ринкові відносини тієї держави, на території якої знаходиться його основне місце здійснення діяльності. У разі якщо виключне право передається або відчужується одночасно на території кількох держав, доцільним є застосування права держави місця проживання або основного місця діяльності ліцензіара / правовласника.

Аналіз особливостей патентування фармацевтичних продуктів, алгоритму оцінки їх патентоспроможності та корисних удосконалень лікарських препаратів, за допомогою яких досягається нова

терапевтична дія, показав, що рішення проблеми балансу інтересів правовласників та доступності лікарських засобів для населення може бути знайдено в рамках застосування норм патентного права, пов'язаного з експертизою патентних заявок без однозначного та виключного застосування механізму примусового ліцензування.

На підставі проведеного аналізу міжнародно-правових норм слід зробити висновок, що застосування механізму примусового ліцензування щодо фармацевтичних продуктів може бути запроваджено за умови дотримання таких умов: підстава використання повинна становити надзвичайну ситуацію або інші обставини крайньої необхідності, пов'язані з охороною здоров'я населення в певній державі-учасниці Угоди ТРІПС та Декларації Дохи. Цілі такого використання повинні відповідати зазначеним підставам використання, необхідна оцінка можливості виробництва фармацевтичного продукту третіми особами, обов'язковість попередніх переговорів з правовласником, у тому числі щодо дослідження характеру та складності виробничого процесу для оцінки перспективної можливості виробництва аналогічного продукту з урахуванням вимог щодо його безпеки та якості; патентовласнику має бути виплачена винагорода (роялті), пропорційна обсягу та строку використання запатентованого винаходу. Загалом обмеження, встановлені в рамках примусової ліцензії, не повинні суперечити нормальному використанню патенту та обмежувати законні інтереси патентовласника.

Список використаних джерел:

1. Конвенція про видачу європейських патентів (European Patent Convention) від 5 жовтня 1973 р. URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1976:017:0001:0028:EN:PDF

2. Конвенція про європейський патент для спільного ринку (Community Patent Convention) 76/76/EEC. *Official Journal of the*

European Communities. URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1976:017:0001:0028:EN:PDF

3. Директива 98/44/ЄС Європейського парламенту та Ради від 6 липня 1998 р. про правову охорону біотехнологічних винаходів. OJ EC L 213, 30 July 1998.

4. Регламент (ЄС) № 469/2009 Європейського парламенту та Ради від 6 травня 2009 р. щодо додаткового сертифіката захисту лікарських засобів.

5. Регламент (ЄС) № 1610/96 Європейського парламенту та Ради від 23 липня 1996 р. щодо створення додаткового сертифіката захисту продуктів захисту рослин.

6. Угода про Єдиний патентний суд (2013/C175/01). *Official Journal of the European Union*. 20.06.2013. URL: https://www.epo.org/law-practice/unitary/patent-court.html

7. Річний звіт Європейського патентного відомства за 2006 рік. URL: http://www.epo.org/about-us/office/annual-reports.html

8. Рішення Палати лордів від 21 жовтня 2004 р. — Kirin-Amgen Inc. v. Hoechst Marion Roussel Ltd.

9. Young R. J. The construction of product-by-process claims — A study in enlightened compromise. OJ EPO, Special Edition 2, 2003. P. 20.

10. Moufang R. Use and purpose indications in patent claims. OJ EPO, Special edition, 1, 2011. P. 116.

11. Рішення від 12 січня 1984 р., OJ EPO 1984, 164 — Pyrrolidine-Derivatives/Hoffmann-La Roche. T 128/82 OJ EPO 1984 ("T 128/82 Pyrrolidine-Derivatives"). P. 164.

12. SOU 2006:70 Oinskränkt produktskydd för patent på genteknikområdet. P. 139.

13. Рішення G 2/08 від 12 січня 1984 р., OJ EPO 1984, 164 — Pyrrolidine-Derivatives/HOFFMANN-LA ROCHE. T 128/82 OJ EPO 1984 ("T 128/82 Pyrrolidine-Derivatives"). P. 164.

14. Merges R. Patent law and policy. Cases and materials. Contemporary Legal Educational Series, Boston, 1992.

15. Рішення Розширеної апеляційної палати G 1/83, G 5/83, G 6/83 від 5 грудня 1984 р. (OJ EPO 1985, 60, 64, 67). Cockbain J. S. Streckx (2011), 'Is the Enlarged Board of Appeal of the European Patent Office Authorized to Extend the Bounds of the Patentable?' — The G 5/8 Second Medical Indication /Eisai and G-2/08 Dosage Regime/ ABBOTT RESPIRATORY Cases', IIC, 42, 257. URL: http://www.epo.org/law-practice/legal-texts/html/caselaw/2016/e/clr_i_c_7_2_3.htm

16. Рішення Розширеної апеляційної палати G 2/08, OJ EPO 2010, 456 — Dosage regime/ABBOTT RESPIRATORY.

17. Gervais B. L. Life Sciences and Chemical Patent Practice in Canada: A Practical Guide. Borden Ladner Gervais LLP, 2011. P. 93.

18. Domeij. Pharmaceutical patents in Europe. Kluwer Law International/Norstedts Juridik, 2000. P. 183.

19. Рішення від 16 січня 2008 р. — Stimulation of beta cell proliferation/Novo Nordisk.

20. Case Law of the Boards of Appeal of the European Patent Office. 6th edition, Munich, 2010. P. 162.

21. Рішення Апеляційної палати T 296/93 від 28 липня 1994 р. — HBV antigen production/BIOGEN INC. URL: https://www.epo.org/law-practice/case-law-appeals/recent/t980091eu1.html

22. Рішення Апеляційної палати T 91/98 від 29 травня 2001 р. — Antiviral nucleoside/Wellcome.

23. Стаття 5(3) та преамбули 22–24 Директиви 98/44/ЄС Європейського парламенту та Ради від 6 липня 1998 р. про правову охорону біотехнологічних винаходів. URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0044:EN:HTML

24. Рішення Апеляційної палати T 870/04 від 11 травня 2005 р. — BDPI Phospharase/MAX-PLANCK.

25. Рішення Апеляційної палати T 604/04 від 16 березня 2006 р. — PF4A receptors/Genentech.

26. Рішення Апеляційної палати T 898/05 від 7 липня 2006 р. — Hematopoietic receptor/Zymogenetics.

27. Рішення Апеляційної палати Т 1452/06 від 10 травня 2007 р. — Serine Protease/Bayer.

28. Рішення Апеляційної палати Т 18/09 від 21 жовтня 2009 р. — Neutrokine/Human Genome Sciences.

29. Директива 98/44/ЄС Європейського парламенту та Ради від 6 липня 1998 р. про правову охорону біотехнологічних винаходів.

30. Schuster M. The Court of Justice of the European Union's Ruling on the Patentability of Human Embryonic Stem-Cell Related Inventions, 2012. P. 43.

31. Рішення G 2/06 Розширеної апеляційної палати від 25 листопада 2008 р., OJ EPO 2009, 306 — Use of embryos/WARF.

32. Рішення від 17 грудня 2009 р., GPUR Int. 2009, 236 — Neurale Vorläuferzellen = 41 IIC 853 (2010) — Neural precursor cells/ Brüstle's patent (Greenpeace v. Oliver Brüstle).

33. Справа Суду Європейського Союзу C-34/10, Oliver Brüstle v Greenpeace e.v. Official Unpublished. Reported in IIC, 43, 711 (2012). URL: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-34/10

34. Funk Brothers Seed Co. v. Kalo Inoculant Co., 333 U.S. 127, 1948.

35. Manual of Patent Examining Procedure. 9th Edition, March 2014. Official Website of the United States Patent and Trademark Office. URL: http://www.uspto.gov/web/offices/pac/mpep/index.htm

36. Звід законів Сполучених Штатів Америки, TITLE 35 / CHAPTER 10 / PART II / § 102. URL: http://uscode.house.gov/

37. Звід законів Сполучених Штатів Америки, TITLE 35 / CHAPTER 10. URL: http://uscode.house.gov/

38. Апеляційний суд США федерального округу, Warner-Lambert Co. v. Apotex Corp., 394 F.3d 1348 (Fed. Cir. 2003). URL: https://casetext.com/case/warner-lambert-co-v-apotex-corp

39. Апеляційний суд США федерального округу, Bayer Schering Pharma AG v Lupin, 676 F.3d 1316, 1328 (Fed. Cir. 2012). URL: https://casetext.com/case/warner-lambert-co-v-apotex-corp

40. Верховний суд США, Graham et al. v. John Deere Co. of Kansas City et al., 383 U.S. 1, 1966. URL: https://supreme.justia.com/cases/federal/us/383/1/case.html

41. United States Patent and Trademark Office. Examination guidelines for determining obviousness under 35 U.S.C. 103 in view of the Supreme Court Decision in KSR International Co. v. Teleflex Inc. *Federal Register*, Vol. 72, No. 195, Oct. 10, 2007.

42. Singer N. In pursuit of a pipeline of biological treatments. New York : New York Times, 27 January 2009.

43. Benett C. L. et al. Long-term outcome of individuals with pure red cell aplasia and antierythropoietin antibodies in patients treated with recombinant epoetin: a follow-up report from the research on adverse drug events and reports (RADAR). Project, 106 BLOOD 3343, 2005.

44. Schellekens H., Jiskoot W. Letter to the editor, eprex-associated pure red cell aplasia and leachtes. *Nature Biotechnol*, 24, 2006. P. 613–614.

45. Generic Drug Savings in the U.S. Fourth Annual Edition. The Generic Pharmaceutical Association, 2012.

46. Апеляційний суд США федерального округу. Shering v Geneva Pharmaceutical, 339 F.3d 1373, FCCA, 2003.

47. NIHCM Foundation. Prescription drugs and intellectual property protection, issue brief, August 2000. URL: https://www.nihcm.org/pdf/prescription.pdf

48. Рішення Федерального суду Канади, AstraZeneca Canada Inc. v. Apotex Inc., 2010, FC 714. URL: http://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/58357/index.do

49. Апеляційний суд США федерального округу, Abbott Laboratories v. Sandoz, Inc. 544 F.3d 1341, Fed. Cir. 2008.

References:

1. Convention on the Grant of European Patents (European Patent Convention). (1973, October 5). Retrieved from http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1976:017:0001:0028:EN:PDF

2. Convention for the European Patent for the Common Market (Community Patent Convention) 76/76/EEC. (n.d.). Official Journal of the European Communities NoL\17/1. Retrieved from http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1976:017:0001:0028:EN:PDF

3. Directive 98/44/EC of the European Parliament and the Council. (1998, July 6). on the legal protection of biotechnological Inventions. OJ EC L 2013, 30 July 1998, 13 = OJ EPO 1999, 101.

4. Regulation (EC) No. 469/2009 of the European Parliament and the Council. (2009, May 6). concerning the supplementary certificate for medicinal products.

5. Regulation (EC) No. 1610/96 of the European Parliament and the Council. (1996, July 23). concerning the creation of a supplementary certificate for plant protection products.

6. Agreement on a Unified Patent Court (2013/C175/01) // Official Journal of the European Union. 20.06.2013 URL: https://www.epo.org/law-practice/unitary/patent-court.html

7. European Patent Office Annual Report 2006. URL: http://www.epo.org/about-us/office/annual-reports.html

8. House of Lords decision of 21 October 2004 — Kirin-Amgen Inc. v. Hoechst Marion Roussel Ltd.

9. Young R. J. The construction of product-by-process calims — A study in enlightened compromise. OJ EPO, Special Edition 2, 2003. P. 20.

10. Moufang R. Use and purpose indications in patent claims. OJ EPO, Special edition, 1, 2011. P. 116.

11. Decision of 12 January 1984, OJ EPO 1984, 164 — Pyrrolidine-Derivatives/Hoffmann-La Roche. T 128/82 OJ EPO 1984 ("T 128/82 Pyrrolidine-Derivatives"). P. 164.

12. SOU 2006:70 Oinskränkt produktskydd för patent på genteknikområdet. P. 139.

13. Decision G 2/08 of 12 January 1984, OJ EPO 1984, 164 — Pyrrolidine-Derivatives/HOFFMANN-LA ROCHE. T 128/82 OJ EPO 1984 ("T 128/82 Pyrrolidine-Derivatives"). P. 164.

14. Merges R. Patent law and policy. Cases and materials, Contemporary Legal Educational Series, Boston, 1992.

15. Enlarged Board of Appeal Decisions G 1/83, G 5/83, G 6/83 of 5 December 1984 (OJ EPO 1985, 60, 64, 67). Cockbain, J. S. Streckx (2011), 'Is the Enlarged Board of Appeal of the European Patent Office Authorized to Extend the Bounds of the Patentable?' — The G 5/8 Second Medical Indication /Eisai and G-2/08 Dosage Regime/ ABBOTT RESPIRATIRY Cases',IIC, 42, 257. URL: http://www.epo.org/law-practice/legal-texts/html/caselaw/2016/e/clr_i_c_7_2_3.htm

16. Enlarged Board of Appeal Decision G 2/08, OJ EPO 2010, 456 — Dosage regime/ABBOTT RESPIRATORY.

17. Gervais B. L. Life Sciences and Chemical Patent Practice in Canada: A Practical Guide. Borden Ladner Gervais LLP, 2011. P. 93.

18. Domeij Pharmaceutical patents in Europe, Kluwer Law International/Norstedts Juridik, 2000. P. 183.

19. Decision of 16 January 2008 — Stimulation of beta cell proliferation /Novo Nordisk.

20. Case Law of the Boards of Appeal of the European Patent Office, 6 th edition, Munich 2010. P. 162.

21. Board of Appeal Decision T 296/93 of 28 July 1994 — HBV antigen production/BGIOGEN INC. URL: https://www.epo.org/law-practice/case-law-appeals/recent/t980091eu1.html

22. Board of Appeal Decision T 91/98 of 29 May 2001 — Antiviral nucleoside/Wellcome.

23. Article 5(3) and Recitals 22 to 24 DIRECTIVE 98/44/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 1998 on the legal protection of biotechnological inventions URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0044:EN:HTML

24. Board of Appeal Decision T 870/04 of 11 May 2005 — BDPI Phospharase/MAX-PLANCK.

25. Board of Appeal Decision T 604/04 of 16 March 2006 — PF4A receptors/Genentech.

26. Board of Appeal Decision T 898/05 of 7 July 2006 — Hematopoietic receptor/Zymogenetics.

27. Board of Appeal Decision T 1452/06 of 10 May 2007 — Serine Protease / Bayer.

28. Board of Appeal Decision T 18/09 of 21 October 2009 — Neutrokine/Human Genome Sciences.

29. Directive 98/44/EC of the European Parliament and the Coucnil of 6 July 1998 on the legal protection of biotechnological Inventions.

30. Schuster M. The Court of Justice of the European Union's Ruling on the Patentability of Human Embryonic Stem-CellRelated Inventions, 2012, P. 43.

31. Decision G 2/06 of the Enlarged Board of Appeal of 25 November 2008, OJ EPO 2009, 306 — Use of embryos/WARF.

32. Decision of 17 December 2009, GPUR Int. 2009, 236 — Neurale Vorläuferzellen = 41 IIC 853 (2010) — Neural precursor cells / Brüstle's patent (Greenpeace v. Oliver Brüstle).

33. European Court of Justice Case C-34/10, Oliver Brüstle v Greenpeace e.v., Official Unpublished. Reportes in IIC, 43, 711 (2012). URL: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-34/10

34. Funk Prothers Seed Co. v. Kalo Inoculant Co., 333 U.S. 127, 1948.

35. Manual of Patent Examining Procedure. 9th Edition, March 2014. The official Website of the United States Patent and Trademark Office. URL: http://www.uspto.gov/web/offices/pac/mpep/index.htm

36. The Code of Laws of the United States of America, TITLE 35 / CHAPTER 10 / PART II / § 102 URL: http://uscode.house.gov/

37. The Code of Laws of the United States of America, TITLE 35 / CHAPTER 10 URL: http://uscode.house.gov/

38. United States Court of Appeals, Federal Circuit, Warner-Lambert Co. v. Apotex Corp., 394 F. 3d 1348 (Fed. Cir. 2003). URL: https://casetext.com/case/warner-lambert-co-v-apotex-corp

39. United States Court of Appeals, Federal Circuit, Bayer Schering Pharma AG v Lupin, 676 F. 3d 1316, 1328 (Fed.Cir. 2012). URL: https://casetext.com/case/warner-lambert-co-v-apotex-corp

40. U.S. Supreme Court, Graham et al. v. John Deere Co. of Kansas City et al, 383 U.S 1, 1966. URL: https://supreme.justia.com/cases/federal/us/383/1/case.html

41. United States Patent and Trademark office. Examination guidelines for determining obviousness under 35 U.S.C. 103 in view of the Supreme Court Decision in KSR International Co. v. Teleflex Inc. *Federal register*, Vol. 72, No. 195 oct 10, 2007.

42. Singer N. In pursuit of a pipeline of biological treatments. New York: New York Times; 27 січня 2009 р.

43. Benett CL. et al. Longterm outcome of individuals with pure red cell aplasia and antierythropoietin antibodies in patients treated with recombinant epoetin: a follow-up report from the research on adverse drug events and reports (RADAR). Project, 106 BLOOD 3343, 2005.

44. Schellekens H., Jiskoot W. Letter to the editor, eprex-associated pure red cell aplasia and leachtes. 24 Nature Biotechnol, 2006. P. 613–614.

45. Generic Drug Savings in the U.S. Fourth Annual Edition, The Generic Pharmaceutical Association. 2012.

46. United States Court of Appeals, Federal Circuit. Aug. 1, 2003, Shering v Geneva pharmaceutical, 339 F3d 1373, FCCA, 2003.

47. NIHCM Foundation. Prescription drugs and intellectual property protection, issue brief, August 2000. URL: https://www.nihcm.org/pdf/prescription.pdf

48. Canadian Federal Court Decision, AstraZeneca Canada Inc. v. Apotex Inc., 2010, FC 714. URL: http://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/58357/index.do

49. United States Court of Appeals, Federal Circuit, Abbott Laboratories v. Sandoz, Inc. 544 F.3d 1341, Fed. Cir. 2008.

ЗАБЕЗПЕЧЕННЯ ПРОДОВОЛЬЧОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ НАЦІОНАЛЬНОГО КРИЗОВОГО АДМІНІСТРУВАННЯ ТА ГЛОБАЛЬНОЇ НЕСТАБІЛЬНОСТІ

ENSURING FOOD SECURITY IN UKRAINE IN THE CONDITIONS OF NATIONAL CRISIS MANAGEMENT AND GLOBAL INSTABILITY

Kivalov S. V.,
Academician, Doctor of Law, Professor,
Senior lecturer of the Department of Administrative and Financial Law,
National University "Odesa Law Academy",
Odesa, Ukraine

Abstract. The study identifies the state of regulation of food security under martial law as a component of the crisis administration system in Ukraine. Crisis administration is proposed to be considered as a special type of public administration, which is formed at the intersection of law, security policy and public administration. Its essence lies in the ability of state institutions to ensure the continuity of the functioning of key systems in situations where traditional regulatory mechanisms are insufficient. On the one hand, the state of food security depends on the level of development of related sectors, primarily energy and logistics. On the other hand, violations in the field of food security can generate risks for other components of national security, in particular through the destabilization of the socio-economic situation. Food security is a relatively stable indicator of the state of national security, which during the period of the legal regime of

martial law requires effective regulation through a combination of legal, organizational and technological instruments that function as a single integrated system. Its provision involves not only responding to existing threats, but also forming mechanisms to prevent future risks, which is a necessary condition for ensuring the national security of Ukraine in the context of global instability. Attention is paid to the analysis of the experience of the European Union and other states. It has been established that the EU Common Agricultural Policy ensures a high level of stability of the food system through a combination of financial support, market regulation and a system of strategic reserves. The generalization of international experience has made it possible to formulate a number of practical recommendations for Ukraine. It is advisable to: 1) create an effective system of strategic food reserves; 2) implement digital systems for monitoring food resources; 3) develop logistics infrastructure and diversify export routes; 4) strengthen Ukraine's integration into international food security mechanisms. In addition, the need to create a single coordination center that will ensure the consistency of actions of various authorities, as well as expand the range of management entities by involving scientific institutions and the private sector, is substantiated.

Keywords: Food Security, National Crisis Management, Global Instability, State Security Policy, Sustainable Food Supply, National Security of Ukraine.

1. Вступ

В умовах докорінних трансформацій державності України, спричинених збройною агресією та тривалою безпековою нестабільністю, питання забезпечення національної безпеки набуває комплексного, багатовимірного та міжгалузевого характеру. Йдеться вже не лише про захист суверенітету чи територіальної цілісності, а про забезпечення здатності держави функціонувати в умовах

тривалих кризових викликів, що охоплюють економічну, соціальну, енергетичну та гуманітарну сфери. У цьому контексті продовольча безпека поступово виходить за межі традиційного економічного розуміння та трансформується у фундаментальний елемент національної стійкості, без якого неможливе підтримання життєдіяльності суспільства та ефективного функціонування державних інституцій [1; 2]. Це означає, що продовольча безпека виходить за межі секторальної політики та інтегрується у стратегічне планування національної безпеки.

Сучасна війна продемонструвала, що здатність держави гарантувати безперервність виробництва, зберігання, транспортування та доступу до продуктів харчування є критично важливою не лише для забезпечення добробуту населення, а й для підтримання соціальної стабільності, економічної рівноваги та обороноздатності держави [2; 3; 4]. Руйнування аграрної інфраструктури, блокування логістичних маршрутів, обмеження доступу до ресурсів і порушення глобальних ланцюгів постачання засвідчили вразливість традиційних моделей забезпечення продовольством [5]. У таких умовах постає необхідність переосмислення підходів до публічного управління, яке дедалі більше набуває ознак кризового адміністрування як специфічного режиму функціонування держави. Йдеться насамперед про перехід від стабілізаційних моделей управління до адаптивних механізмів, орієнтованих на функціонування в умовах невизначеності.

Попри значну кількість наукових напрацювань у сфері національної та продовольчої безпеки, у сучасній доктрині відчувається брак комплексного бачення зазначеної категорії саме як об'єкта кризового адміністрування, що потребує ґрунтовного теоретичного переосмислення. Подібна концептуальна обмеженість суттєво ускладнює розробку цілісної державної політики, здатної органічно поєднати превентивні механізми та реактивні інструменти

управління. Зазначені чинники зумовлюють нагальну наукову потребу у проведенні дослідження, спрямованого на формування інтегрованої моделі управління продовольчою стійкістю в умовах правового режиму воєнного стану [6].

Метою дослідження є комплексне теоретико-правове обґрунтування та розроблення науково-практичних засад впорядкування продовольчої безпеки в умовах воєнного стану як складової системи кризового адміністрування в Україні. Досягнення поставленої мети передбачає вирішення комплексу взаємопов'язаних завдань, що охоплюють: аналіз теоретико-методологічних засад кризового адміністрування; дослідження сучасного стану публічного управління у сфері національної безпеки; визначення особливостей правового регулювання продовольчої безпеки в умовах воєнного стану; виявлення системних проблем функціонування аграрного сектору та логістичних ланцюгів; а також узагальнення міжнародного досвіду і розроблення практичних рекомендацій щодо вдосконалення державної політики.

Методологічну основу дослідження становить сукупність загальнонаукових і спеціально-юридичних методів, що забезпечують комплексний характер аналізу. Використання системного підходу дозволило розглядати продовольчу безпеку як складову інтегрованої системи національної безпеки [7]. Порівняльно-правовий метод застосовано для дослідження міжнародного досвіду, формально-юридичний — для аналізу нормативно-правової бази, а методи аналізу та синтезу — для узагальнення результатів і формування наукових висновків. Додатково застосовано інституційний підхід, що дав змогу оцінити роль різних суб'єктів у забезпеченні продовольчої безпеки [8; 9]. Запропоновані висновки можуть бути застосовані у діяльності органів державної влади для підвищення ефективності управлінських рішень в умовах воєнного стану, а також у процесі формування стратегій відновлення аграрного сектору [6]. Крім

того, результати дослідження можуть бути використані у науково-дослідній та освітній діяльності при підготовці фахівців у сфері публічного управління та права. У ширшому контексті запропоновані підходи сприяють формуванню довгострокової моделі національної стійкості, орієнтованої на функціонування держави в умовах тривалих кризових процесів і глобальної нестабільності.

2. Стан кризового адміністрування в Україні

Національна безпека в сучасних умовах розвитку державності України набуває не лише статусу однієї з ключових функцій держави, а й трансформується у комплексну сферу суспільних відносин, що потребує якісно нових підходів до публічного управління. Її багатовимірний характер обумовлює необхідність поєднання правових, організаційних та інституційних механізмів, здатних забезпечити стійкість держави в умовах високої невизначеності та постійних загроз. У сучасній юридичній науці відсутній єдиний підхід до розуміння національної безпеки як об'єкта саме кризового адміністрування. Переважна частина досліджень зосереджена на її змістовному наповненні або інституційному забезпеченні, тоді як управлінський аспект у кризових умовах розкритий фрагментарно. У межах новітньої наукової доктрини кризове адміністрування дедалі частіше розглядається крізь призму теорії складних адаптивних систем, де держава виступає динамічним утворенням, здатним до ефективної саморегуляції в умовах високої волатильності середовища [10; 11].

Подібна інтерпретація передбачає рішучу відмову від застарілих лінійних моделей на користь стратегічного сценарного планування та ризик-орієнтованого підходу. Це, своєю чергою, зумовлює гостру потребу в інституційній гнучкості та здатності до оперативної модифікації управлінських алгоритмів залежно від вектору та інтенсивності виникаючих загроз [12].

Різке загострення безпекового середовища внаслідок повномасштабної збройної агресії Російської Федерації проти України зумовило нагальну потребу в радикальному перегляді традиційних моделей публічного управління. Запровадження правового режиму воєнного стану виступило не лише юридичною констатацією нових реалій, а й потужним інституційним каталізатором глибинних системних зрушень [13].

В умовах воєнних дій державний апарат змушений функціонувати в режимі перманентної мобілізації ресурсів, що диктує перехід від класичних бюрократичних процедур до гнучких та інваріантних управлінських стратегій. Така еволюція свідчить про фундаментальну зміну парадигми: від жорстко регламентованого адміністративного процесу до домінування дискреційних повноважень, де критична маса рішень приймається в умовах часового дефіциту та інформаційної асиметрії. Подібна специфіка об'єктивно підвищує рівень управлінських ризиків і потребує якісного посилення інтелектуально-аналітичної підтримки кожного владного кроку.

Зазначені тенденції неминуче посилюють роль виконавчої гілки влади, водночас загострюючи проблему дотримання балансу між оперативною ефективністю та непохитністю принципу верховенства права. У таких екстремальних обставинах особливої ваги набувають процесуальні гарантії нагляду за реалізацією широких дискреційних повноважень. Зокрема, йдеться про судовий контроль як ключовий запобіжник від управлінських зловживань, посилення парламентської підзвітності уряду, а також впровадження спеціальних механізмів прозорості, які дозволяють зберігати публічний характер влади навіть за умов виправданого обмеження доступу до стратегічної інформації.

У таких умовах особливої ваги набуває інституційна спроможність держави, яка визначається не лише формальними

повноваженнями органів влади, а й ефективністю їх взаємодії та швидкістю прийняття рішень. Вирішальним чинником стає також якість горизонтальної координації між органами влади. Саме ця спроможність стає критерієм оцінки ефективності кризового адміністрування.

З огляду на це кризове адміністрування доцільно розглядати як особливий тип державного управління, який формується на перетині права, безпекової політики та публічної адміністрації. Його сутність полягає у здатності державних інституцій забезпечувати безперервність функціонування ключових систем у ситуаціях, коли традиційні механізми регулювання виявляються недостатніми. Воно включає не лише реагування на кризові явища, але й формування передумов для запобігання їх ескалації, що свідчить про необхідність переходу до проактивної моделі управління. При цьому кризове адміністрування не може ототожнюватися виключно з антикризовим реагуванням. Його сутність полягає у формуванні стійких управлінських механізмів, здатних функціонувати в умовах постійної загрози, що відрізняє його від класичних моделей управління надзвичайними ситуаціями.

Правовою основою зазначених трансформацій виступає комплекс нормативно-правових актів у сфері національної безпеки, які детермінують межі повноважень органів державної влади та встановлюють специфічні особливості реалізації прав і свобод громадян у кризовий період. Аналіз даних актів наочно демонструє поступову еволюцію та зміщення акцентів у бік домінування безпекової компоненти в усіх сферах державної політики. При цьому засадничі документи стратегічного планування, зокрема Указ Президента України № 392/2020, остаточно закріплюють антропоцентричний підхід до ідентифікації національних інтересів [14]. Відповідно до положень цього акта, людина, її життя, здоров'я, честь, гідність, а також недоторканність і безпека визнаються

фундаментальними цінностями, що визначають вектор розвитку всієї держави. Такий ціннісний орієнтир є принципово важливим для демократичного суспільства, оскільки він підтверджує: навіть у надзвичайних умовах воєнного часу держава не нівелює базові громадянські цінності, а, навпаки, перетворює їх на головний об'єкт захисту та основу національної стійкості.

Водночас закріплення такого підходу на рівні стратегічних документів свідчить про інституціоналізацію людиноцентризму як базового принципу державного управління в умовах кризи.

Логічним продовженням реалізації цієї антропоцентричної доктрини стало виокремлення продовольчого компонента як критичного елемента виживання нації. В умовах національного кризового адміністрування забезпечення фізичної та економічної доступності продуктів харчування трансформувалося з суто економічної категорії у фундаментальний безпековий чинник. Це знайшло своє відображення у стратегічному плануванні уряду, спрямованому на мінімізацію ризиків, спричинених руйнуванням логістичних ланцюгів та дестабілізацією аграрного сектору.

Ключовим інструментом відповідно виступає Про затвердження Стратегії продовольчої безпеки України на період до 2027 року [7]. Даний документ не лише визначає пріоритетні напрями державної політики в аграрній сфері, а й створює інституційний каркас для міжвідомчої координації. Стратегія закладає основу для переходу від фрагментарних заходів підтримки ринку до цілісної системи моніторингу та оперативного реагування на загрози продовольчій стабільності. У цьому контексті доцільно враховувати й зарубіжний досвід забезпечення продовольчої безпеки. Як зазначають L. Melnyk, V. Kepko та O. Nikonenko [15], ефективні моделі продовольчої політики базуються на поєднанні державного регулювання, ринкових механізмів та цифрових технологій моніторингу. Зокрема, у розвинених країнах значна увага приділяється формуванню

стратегічних продовольчих резервів, диверсифікації логістичних маршрутів, а також використанню цифрових платформ для управління продовольчими потоками. Такий підхід може бути адаптований до українських умов з урахуванням воєнних ризиків.

Отже, інтеграція зазначеної Стратегії у загальну систему національної безпеки свідчить про формування комплексного підходу до захисту національних інтересів, де кожна ланка (від енергетики до продовольства) розглядається через призму стійкості держави та добробуту її громадян в умовах глобальної турбулентності.

Таким чином, продовольча безпека виступає не ізольованим елементом, а системоутворюючою складовою національної безпеки, що інтегрується з іншими її секторами [16]. У науковій літературі такий підхід відповідає концепції "human security", сформульованій у доповіді Програми розвитку ООН (UNDP, 1994) [17], де продовольча безпека визначається як одна з ключових складових безпеки людини. Окремий акцент державної політики спрямований на забезпечення продовольчої безпеки [7]. Порушення логістичних ланцюгів, знищення сільськогосподарської інфраструктури та мінування територій суттєво впливають на здатність держави гарантувати стабільне постачання продовольства. Це, у свою чергу, трансформує продовольчу безпеку з питання економічної політики у сферу національної безпеки, де ключове значення мають не лише обсяги виробництва, а й здатність держави забезпечити безперервність постачання в умовах воєнних ризиків. З огляду на це кризове адміністрування повинно забезпечувати не лише відновлення порушених процесів, а й формування нових механізмів їх функціонування.

У цьому зв'язку доцільно розглядати продовольчу безпеку у взаємодії з іншими критичними секторами, оскільки їх функціонування є взаємозалежним. Так, систематичні атаки на енергетичну інфраструктуру створюють загрозу не лише економічній стабільності, а й базовим умовам існування населення. Законодавство

підкреслює необхідність забезпечення доступу до надійних, сталих та безпечних джерел енергії як у звичайних, так і в кризових умовах [18]. Відповідно енергетична безпека виступає базовою умовою функціонування інших секторів, що підтверджує її системоутворюючу роль у структурі національної безпеки, оскільки порушення енергопостачання безпосередньо впливає на виробництво, зберігання та транспортування продовольства, що підсилює системний характер сучасних загроз. Додатково слід враховувати ризики фізичного руйнування критичної інфраструктури. Дослідження N. Zuievska та співавторів [19] демонструють, що енергетичні об'єкти є вразливими до вибухових впливів, що може спричинити каскадні ефекти для інших секторів, зокрема продовольчого. А саме: пошкодження енергосистеми порушує процеси зберігання продукції, ускладнює транспортування та логістику, а також створює ризики техногенних аварій, які можуть впливати на якість продовольства. Це підтверджує необхідність інтегрованого підходу до захисту критичної інфраструктури.

Попри наявність розгалуженої системи нормативно-правових актів, нинішня архітектура публічного управління виявила низку критичних структурних обмежень. Спостерігається суттєвий теоретико-методологічний та прагматичний розрив, оскільки класичні управлінські підходи виявляються неспроможними повною мірою релевантно відповідати викликам високоінтенсивного збройного конфлікту [20]. Ключовою детермінантою такої невідповідності є апріорна орієнтація звичних моделей адміністрування на стабільне середовище, що нівелює потребу в перманентній адаптації до динамічних змін безпекового ландшафту.

Варто наголосити, що застарілі підходи не враховують тривалу природу сучасних кризових явищ. Сучасна доктрина публічного управління традиційно розглядала надзвичайні стани як короткострокові аномалії або тимчасові відхилення від норми, однак

досвід повномасштабної війни диктує необхідність формування принципово нової функціональної специфіки. У цих умовах межа між класичним цивільним управлінням і стратегічною військовою доцільністю стає дедалі більш розмитою, що вимагає переосмислення ролі державних інституцій у забезпеченні життєдіяльності суспільства [10]. Це означає перехід кризового адміністрування від інструменту реагування до постійного стратегічного режиму функціонування держави. Така трансформація потребує не лише точкових рішень, а й глибоких інституційних змін, закріплених на рівні стратегічного планування [14].

У відповідь на ці екзистенційні виклики в Україні формується нова управлінська парадигма, яка передбачає відхід від галузевого підходу на користь інтегрованої моделі управління. Специфіка сучасного адміністрування полягає у переході від ієрархічної структури до об'єктно-орієнтованої моделі [10]. У межах цієї моделі продовольча, енергетична та інформаційна безпека більше не розглядаються як ізольовані напрями, а інтегруються через складні міжвідомчі інституційні механізми. Це сприяє формуванню єдиної архітектури безпеки, у межах якої взаємозв'язок секторів набуває системного характеру.

Важливою складовою цієї інтеграції є цифровізація публічного адміністрування. Як зазначається у монографії авторського колективу: С. В. Ківалов, Л. Р. Біла-Тіунова, Т. А. Латковська та ін. [21], цифрові технології створюють можливість формування єдиного інформаційного простору управління, що забезпечує синхронізацію дій різних органів влади. Цифровізація підвищує швидкість обміну інформацією, сприяє прозорості управлінських процесів та дозволяє впроваджувати інструменти прогнозування й аналітики. Така інтеграція забезпечує ефект синергії, коли взаємодія різних секторів безпеки підвищує загальну стійкість системи, що є принципово важливим в умовах гібридних загроз. Особливо це

стосується швидкості прийняття рішень та узгодженості дій різних суб'єктів управління. Такий підхід дозволяє суттєво підвищити загальну ефективність державного апарату за рахунок концентрації обмежених ресурсів на критичних об'єктах безпеки та забезпечення їхнього ешелонованого захисту від гібридних загроз.

Зазначені процеси свідчать про те, що державне управління поступово виходить за межі класичних адміністративних моделей і набуває рис складної адаптивної системи. Система кризового адміністрування поступово набуває ознак цілісної, багаторівневої та адаптивної моделі управління, яка поєднує елементи централізації, гнучкості та міжсекторальної інтеграції.

У даному контексті особливої актуальності набуває впровадження ризик-орієнтованого підходу у кризовому адмініструванні, сутність якого полягає у системному виявленні, оцінці та управлінні загрозами, які можуть впливати на функціонування ключових секторів національної безпеки. При цьому важливо враховувати їх взаємопов'язаний характер, що зумовлює ефект взаємного посилення загроз. Такий підхід дозволяє перейти від ситуативного реагування до прогнозованого управління, що є принципово важливим в умовах тривалої невизначеності.

По-перше, доцільно виокремлювати воєнні ризики, пов'язані з безпосереднім впливом бойових дій, руйнуванням інфраструктури та загрозами для безпеки населення. По-друге, логістичні ризики, що проявляються у порушенні транспортних маршрутів, блокуванні портів та ускладненні внутрішнього і зовнішнього переміщення товарів. По-третє, економічні ризики, зумовлені коливанням цін, зниженням платоспроможності населення та обмеженням доступу до фінансових ресурсів. По-четверте, інфраструктурні ризики, які охоплюють пошкодження енергетичних об'єктів, систем зберігання та переробки продукції, що безпосередньо впливає на стабільність продовольчого забезпечення.

Отже, кризове адміністрування в Україні перебуває на етапі фундаментальної трансформації. У зазначених умовах доцільно звернутися до категорії стійкості (resilience), яка дедалі активніше використовується у сучасній безпековій та управлінській доктрині. По-перше, стійкість означає здатність державної системи зберігати функціональність навіть за умов інтенсивного зовнішнього впливу та кризових навантажень. По-друге, вона передбачає спроможність до швидкого відновлення порушених процесів після деструктивних подій. По-третє, важливою характеристикою є адаптивність, тобто здатність трансформувати внутрішні механізми управління відповідно до нових умов функціонування.

У площині кризового адміністрування стійкість набуває системного значення, оскільки охоплює не лише інституційну спроможність органів державної влади, але й взаємодію між різними секторами безпеки. Вона забезпечує узгодженість управлінських рішень, сприяє мінімізації наслідків кризових явищ та формує довгострокову здатність держави протистояти гібридним загрозам.

Відбувається перехід від пасивних реактивних моделей до проактивного стратегічного управління, що базується на інтеграції різних секторів безпеки та створенні нових інституційних алгоритмів. Така еволюція системи управління створює необхідні теоретичні та практичні передумови для подальшого поглибленого дослідження продовольчої безпеки не лише як галузевого питання, а як стратегічного елементу забезпечення національної стійкості (resilience), від якого безпосередньо залежить здатність держави функціонувати в умовах довготривалої глобальної нестабільності [7]. Саме така триєдина характеристика формує сучасне розуміння стійкості як базового елементу забезпечення національної безпеки.

3. Впорядкування продовольчої безпеки в умовах воєнного стану

Очевидно, що сектор національної безпеки охоплює значну кількість ключових сфер суспільних відносин, які прямо або опосередковано впливають на її стан. У цьому контексті продовольча безпека виступає не ізольованим елементом, а інтегрованою складовою системи національної безпеки, яка взаємодіє з економічною, соціальною, енергетичною та екологічною безпекою. При цьому доцільно враховувати, що в умовах війни така взаємодія набуває ознак системної взаємозалежності, коли порушення в одному секторі здатне спричинити каскадні ефекти в інших сферах національної безпеки. Зазначена взаємодія має двосторонній характер. З одного боку, стан продовольчої безпеки залежить від рівня розвитку суміжних секторів, передусім енергетики та логістики. З іншого боку, порушення у сфері продовольчого забезпечення здатні генерувати ризики для інших складових національної безпеки, зокрема через дестабілізацію соціально-економічної ситуації.

По-перше, рівень продовольчої забезпеченості прямо впливає на соціальну стабільність, оскільки дефіцит або недоступність продуктів харчування можуть спричинити зростання соціальної напруги. По-друге, відповідна сфера визначає економічну стійкість держави через функціонування аграрного сектору як одного з базових елементів національної економіки. З огляду на це показовими є підходи Food and Agriculture Organization (FAO) [2], яка визначає продовольчу безпеку через чотири виміри: доступність, доступ, використання та стабільність. Такий підхід дозволяє розглядати продовольчу безпеку не лише як результат функціонування аграрного сектору, а як комплексну характеристику ефективності соціально-економічної політики держави. По-третє, вона має безпосередній зв'язок із обороноздатністю, адже забезпечення продовольством населення та Збройних Сил України є необхідною

умовою підтримання державної спроможності в умовах воєнного стану. Відповідно продовольче забезпечення слід розглядати також як елемент оборонної логістики, що інтегрується у загальну систему забезпечення сектору безпеки і оборони.

Продовольча безпека є відносно стабільним індикатором стану національної безпеки, однак у період дії правового режиму воєнного стану її значення істотно зростає у зв'язку з появою нових загроз і ризиків. Це зростання уваги має не лише декларативний, а й практичний характер, що проявляється у прийнятті низки управлінських рішень (запровадження державного регулювання цін на соціально значущі продукти, формування державних інтервенційних фондів, а також використання механізмів публічних закупівель для забезпечення стабільного постачання продовольства тощо [22]).

Такі заходи свідчать про поступовий перехід від реактивної моделі управління до проактивної, тобто від реагування на наслідки до управління ризиками, що передбачає системне прогнозування

Водночас, згідно з даними Глобального індексу продовольчої безпеки, Україна наразі посідає останнє місце за станом національного забезпечення продовольчої стабільності серед країн Європейського регіону. Проте слід зауважити, що методологія Global Food Security Index (GFSI) [23] переважно орієнтована на стабільні економічні системи й не враховує в повному обсязі деструктивні чинники воєнного впливу, що спричиняє певні викривлення у підсумковій рейтинговій оцінці. Також важливим чинником є те, що в обставинах збройного конфлікту об'єктивна картина продовольчої безпеки може бути висвітлена в міжнародних звітах лише частково через ускладнений доступ до верифікованих даних та надвисоку динаміку подій.

Попри методологічні нюанси, сам факт зниження рейтингових позицій сигналізує про наявність глибоких структурних проблем у функціонуванні продовольчих ланцюгів, що вимагає системного

вирішення на рівні державної політики. Це актуалізує потребу в ревізії існуючих механізмів публічного адміністрування та підвищенні їхньої адаптивності до екстремальних умов.

Зокрема, у Стратегії продовольчої безпеки України на період до 2027 року [7] та затвердження операційного плану заходів з її реалізації (2024) виокремлюються такі ключові проблеми: а) порушено цілісність ланцюгів постачання сільськогосподарської продукції господарства та харчових продуктів, а також діяльності із створення доданої вартості в агропромисловому комплексі, пов'язаної з виробництвом, переробленням, розподілом, споживанням і утилізацією (знищенням) харчових продуктів; б) ускладнено проведення посівних кампаній, особливо на територіях, які були деокуповані, на яких відбувалися бойові дії, у зв'язку із значними площами забруднених земель, а також нестачею пального та високими світовими цінами на пальне, агрохімікати, засоби захисту рослин; в) наявною обмеженістю можливостей вітчизняних аграріїв вільно продавати вирощену сільськогосподарську продукцію через блокування Російською Федерацією морських портів України та ускладнену логістику експорту аграрної продукції; ускладнено забезпечення базових продовольчих потреб у найбільш постраждалих регіонах країни.

Отже, окреслені проблеми мають системний характер і охоплюють усі етапи продовольчого ланцюга — від виробництва до споживання. У кризовий період вразливість кожного з етапів суттєво зростає, оскільки навіть незначні збої у функціонуванні окремих елементів системи можуть мати кумулятивний ефект для всього продовольчого забезпечення. Вказане обґрунтовує провадження концепції системної вразливості (systemic vulnerability), яка дає змогу ідентифікувати критичні вузли логістичних та виробничих ланцюгів для визначення пріоритетних напрямів державного втручання. Застосування цього інструментарію забезпечує перехід

від стратегії реактивного реагування до глибокого структурного аналізу слабких місць системи, що є фундаментальним для формування довгострокового безпекового курсу.

Паралельно з цим, наукового обґрунтування потребує категорія "resilience" (стійкість). У сучасній доктрині публічного адміністрування цей термін детермінує здатність складної системи не лише протистояти зовнішнім шокам, а й зберігати базову функціональність та демонструвати високі темпи ревіталізації після масштабних деструктивних впливів. Інтеграція зазначених підходів у державну політику дозволить створити адаптивну архітектуру управління, здатну витримувати тривалі кризи.

Показовим прикладом деструктивного впливу на продовольчу стійкість є пошкодження об'єктів енергосистеми, що неминуче дестабілізує технологічні процеси зберігання продукції, критично ускладнює логістику та провокує ризики техногенних інцидентів, які безпосередньо погіршують якість продуктів харчування. Системна дезорганізація цієї сфери проявляється у декількох площинах. По-перше, блокування або руйнування транспортних сполучень гальмує не лише експортні операції, а й внутрішній розподіл товарних потоків. По-друге, суттєве зниження виробничих потужностей аграрного сектору призводить до скорочення сукупної пропозиції на ринку. По-третє, дефіцит енергетичних та паливних ресурсів провокує стрімке здорожчання собівартості виробництва, що за ланцюговою реакцією зумовлює зростання кінцевих цін для споживача. Сукупність цих чинників потребує впровадження інтегрованих заходів захисту критичної інфраструктури для запобігання поглибленню продовольчої кризи.

Особливого значення набуває формування та ефективне управління державними продовольчими резервами як інструменту стабілізації ринку. Наявність стратегічних запасів дозволяє оперативно реагувати на дефіцити, згладжувати цінові коливання

та забезпечувати мінімальні соціальні стандарти. Ефективність цього механізму залежить від прозорості процедур, належного нормативного регулювання та координації між органами влади. Доцільним є також нормативне закріплення мінімальних обсягів стратегічних продовольчих резервів та механізмів їх ротації з метою недопущення втрати якості продукції.

У цих умовах важливу роль відіграють міжнародні гуманітарні механізми, зокрема діяльність Всесвітньої продовольчої програми ООН (World Food Programme), які доповнюють національні системи постачання. Вони дозволяють компенсувати дефіцити та підтримувати найбільш вразливі групи населення, особливо в зонах бойових дій [2]. При цьому ефективність використання такої допомоги значною мірою залежить від належної координації між державними органами та міжнародними організаціями, а також від прозорості механізмів її розподілу. Разом з тим надмірна залежність від зовнішньої допомоги може створювати ризики для продовольчого суверенітету держави, що потребує збалансування між міжнародною підтримкою та розвитком внутрішнього виробництва.

Повертаючись до дослідження продовольчої безпеки, зазначимо, що у науковій літературі дане поняття розглядається як складне багаторівневе явище. Зокрема, Голікова К. П. визначає її через систему показників, що охоплюють рівень самозабезпеченості держави продовольством, обсяги резервів, а також відповідність структури споживання фізіологічним нормам [24]. Такий підхід дозволяє розглядати продовольчу безпеку не лише як факт наявності ресурсів, а як збалансовану систему їх розподілу та споживання. Наведений підхід також дає підстави зробити висновок про необхідність використання комплексної системи індикаторів продовольчої безпеки, яка враховує не лише кількісні, але й якісні характеристики — показники доступності, стабільності постачання, якості продуктів

харчування та їх відповідності санітарним і безпековим стандартам. Саме багатовимірність оцінки продовольчої безпеки гарантує можливість формування ефективної державної політики у цій сфері. Саме тому особливого значення набуває створення єдиної системи збору та обробки даних щодо стану продовольчої безпеки, яка дозволяє забезпечити узгодженість управлінських рішень на різних рівнях публічного адміністрування.

У цьому контексті Тригуб А. акцентує увагу на адміністративно-правовому аспекті, визначаючи мету державного впливу як гарантування безперешкодного економічного доступу до продуктів харчування [25]. Це підкреслює, що відповідна сфера безпосередньо пов'язана з соціальною стабільністю та економічною стійкістю держави, а її забезпечення є одним із ключових завдань публічного адміністрування. Важливо підкреслити, що адміністративно-правовий вплив у сфері продовольчої безпеки має не лише регулятивний, але й гарантійний характер. По-перше, держава виступає гарантом мінімальних стандартів забезпечення населення продуктами харчування. По-друге, вона забезпечує баланс між інтересами виробників, споживачів та держави. По-третє, створює умови для стабільного функціонування ринку продовольства навіть у кризових умовах. Це дозволяє розглядати продовольчу безпеку як одну з ключових функцій сучасної держави та публічне благо, забезпечення якого не може бути повністю делеговане ринковим механізмам і потребує активної участі держави, особливо в умовах кризових явищ.

Нормативне закріплення дефініції «продовольча безпека» наразі зведено до захищеності життєвих інтересів особи, що реалізується через державні гарантії безперешкодного економічного доступу людини до харчових продуктів задля підтримання її належної життєдіяльності [22]. Отже, у вузькому розумінні ця категорія відображає захист правовідносин, що виникають у процесі забезпечення споживчих потреб населення.

Водночас у сучасних реаліях зазначене трактування потребує суттєвого розширення. Зокрема, поряд із фінансовою спроможністю споживачів, критичного значення набуває фізична доступність продовольства, яка безпосередньо детермінована станом критичної інфраструктури, поточною безпековою ситуацією та ефективністю логістичних ланцюгів. Невід'ємним чинником стає стабільність постачання, що передбачає здатність державних інституцій гарантувати безперебійність харчового забезпечення навіть в умовах дії правового режиму воєнного стану. Подібні виклики актуалізують потребу в інтенсивному розвитку систем стратегічного резервування, модернізації транспортно-складської мережі та вдосконаленні інструментарію публічного управління цими процесами. Одним із напрямів удосконалення забезпечення продовольчої безпеки є використання: а) SMART-технології; б) Інтернет речей (IoT) — використання сучасних цифрових технологій для моніторингу та управління виробництвом, контролю за здоров'ям сільськогосподарських тварин та раціональним використанням ресурсів; впровадження систем автоматизації та віддаленого контролю у галузі тваринництва, простежуваності ресурсів вздовж ланцюга постачання, а також моніторингу забруднення від підприємства; в) застосування сучасних методів генетичного відбору для створення сільськогосподарських тварин з покращеними продуктивними якостями та стійкістю до захворювань [26].

Впровадження зазначених технологій сприяє не лише зростанню виробничої ефективності, а й гарантуванню прозорості логістичних ланцюгів. По-перше, інноваційні рішення дають змогу здійснювати безперервний моніторинг стану ресурсів та виробничих циклів. По-друге, вони створюють можливості для оперативного реагування на динамічні ризики. По-третє, автоматизація процесів прискорює інтеграцію національного аграрного сектору у глобальні ринки. З огляду на це критично важливим є врахування досвіду

Європейського Союзу, зокрема стратегії "Farm to Fork" [27], яка детермінує сталість продовольчих систем та їхню резистентність до зовнішніх шоків. Імплементація цих підходів в Україні дозволить гармонізувати вітчизняну політику з європейськими стандартами та підвищити її дієвість.

У результаті цифрова трансформація стає одним із фундаментальних інструментів зміцнення національної стійкості. Зокрема, у країнах ЄС активно впроваджуються спеціалізовані платформи аграрного моніторингу (AgriTech), системи супутникового контролю та Big Data-аналітика для предиктивного моделювання продовольчих загроз. Крім того, перехід на електронні формати взаємодії створює передумови для посилення довіри між суб'єктами ринку, оскільки гарантує відкритість інформаційних потоків і нівелює ризики зловживань у сфері обігу продукції. Окремої ваги набуває кіберзахист систем управління ресурсами, адже їхня вразливість може бути використана як дієвий інструмент гібридного впливу на державу.

Водночас існує специфіка інституційного забезпечення продовольчої безпеки. Відповідно до Операційно плану заходів з реалізації Стратегії продовольчої безпеки на період до 2027 року [7], до публічного адміністрування в цій сфері має бути залучено наукові та дослідні установи. Наприклад, щодо розроблення та подання Кабінетові Міністрів України пропозицій з внесення змін до законодавства стосовно розширення державної підтримки сільського господарства; розроблення та затвердження програм науково-технічних розробок у галузі аквакультури; розроблення механізмів ефективного регулювання внутрішнього ринку сільськогосподарської продукції та продуктів її переробки і тому подібне, — має бути залучено Національну академію аграрних наук. Крім того, Національний інститут стратегічних досліджень може взяти участь у діяльності з: забезпечення функціонування системи державних

резервів; визначення системи критеріїв та індикаторів продовольчої безпеки, актуалізація методики розрахунків індикаторів продовольчої безпеки; підтримка функціонування систем національного та регіонального моніторингу продовольчої безпеки тощо [7]. Важливо, що в цьому контексті зроблено вказівку на наявність згоди у науково-дослідних установ на участь у заходах з впорядкування продовольчої безпеки. Одночасно, нормативна вказівка на конкретних суб'єктів є свідченням зміни підходу до системи суб'єктів, що здійснюють публічне адміністрування в сфері продовольчої безпеки.

Фактично йдеться про перехід від вузько відомчої моделі управління до мережевої, у якій взаємодія між державними органами, науковими установами та іншими суб'єктами набуває системного характеру. Такий підхід відповідає концепції "network governance", у межах якої публічне управління здійснюється через горизонтальні зв'язки між державою, наукою та приватним сектором. Це дозволяє підвищити ефективність управління за рахунок залучення експертного середовища та зменшення інституційної фрагментації.

Такий підхід свідчить про формування нової моделі публічного адміністрування, що базується на принципах міжсекторальної взаємодії та наукового супроводу управлінських рішень. По-перше, залучення наукових установ гарантує обґрунтованість державної політики. По-друге, сприяє впровадженню інноваційних рішень у практику державного управління. По-третє, дозволяє формувати довгострокові стратегії розвитку продовольчої системи. У свою чергу, це підвищує стійкість держави до кризових викликів.

Узагальнюючи викладене, слід зазначити, що ефективне впорядкування продовольчої безпеки можливе лише за умови поєднання правових, організаційних та технологічних інструментів, що функціонують як єдина інтегрована система.

Таким чином, продовольча безпека в умовах воєнного стану трансформується у складний об'єкт кризового публічного

адміністрування, який потребує системного, міжгалузевого та інституційно узгодженого підходу. Її забезпечення передбачає не лише реагування на наявні загрози, але й формування механізмів запобігання майбутнім ризикам, що є необхідною умовою забезпечення національної безпеки України в умовах глобальної нестабільності. Отже, цей сектор за умов збройної агресії набуває ознак стратегічного публічного блага, забезпечення якого є ключовою передумовою не лише виживання держави, але й збереження її соціальної стабільності та суверенітету. Ключовим завданням у цьому контексті є інституційна імплементація зазначених підходів у національну систему публічного управління.

4. Міжнародні інструменти забезпечення продовольчої безпеки

Міжнародні інструменти гарантування продовольчої безпеки формують багаторівневу систему регулювання, що поєднує норми міжнародного права, діяльність спеціалізованих інституцій та практику реагування на кризові ситуації, включаючи збройні конфлікти. У сучасних умовах продовольча безпека перестає бути виключно внутрішньою справою держави і набуває характеру глобального публічного блага, реалізація якого залежить від узгоджених дій міжнародної спільноти [2]. У науковій доктрині продовольча безпека дедалі частіше розглядається крізь призму концепції глобального врядування (global governance), що передбачає координацію дій не лише держав, але й міжнародних організацій, транснаціональних корпорацій та недержавних акторів [12]. Такий підхід відображає зміну природи продовольчих ризиків, які виходять за межі національних юрисдикцій і потребують комплексних багаторівневих механізмів реагування.

Така трансформація обумовлена не лише економічною взаємозалежністю держав, але й зростанням ролі продовольства як інструменту геополітичного впливу, що особливо чітко проявляється

в умовах воєнних конфліктів. Зокрема, це виражається у використанні блокування експорту, руйнування аграрної інфраструктури та обмеження доступу до продовольства як інструментів впливу на державу. При цьому у науковій доктрині дедалі частіше підкреслюється, що продовольство трансформується у елемент так званої "weaponized interdependence" (інструменталізованої взаємозалежності), коли контроль над критичними ресурсами використовується як засіб політичного та економічного тиску [28; 29].

Нормативною основою регулювання продовольчої безпеки виступає комплекс універсальних і спеціалізованих міжнародних актів. Базове значення має Міжнародний пакт про економічні, соціальні і культурні права, який закріплює право кожної людини на достатній життєвий рівень, включаючи достатнє харчування [1]. У Загальному коментарі № 12 Комітету ООН з економічних, соціальних і культурних прав це право конкретизується через категорії фізичної та економічної доступності, якості та безпечності харчових продуктів [30]. При цьому зазначений підхід передбачає також позитивні зобов'язання держав щодо створення умов для реалізації права на харчування, включаючи розвиток інфраструктури, забезпечення функціонування ринків та недопущення дискримінаційного доступу до продовольства. Це фактично формує обов'язок держав не лише утримуватися від порушень, але й активно забезпечувати реалізацію цього права.

Важливим є також Римська декларація про всесвітню продовольчу безпеку 1996 року, яка визначає обов'язок держав забезпечувати стабільний доступ населення до продовольства [31].

Додатково загальновизнані міжнародні стандарти деталізуються у добровільних керівних принципах щодо права на харчування, які формують прикладні орієнтири для розробки національної державної політики. Варто зауважити, що значний масив регуляторного інструментарію у цій царині має характер «м'якого права»

(soft law). Хоча такі акти не створюють формально обов'язкових юридичних зобов'язань, вони відіграють фундаментальну роль у гармонізації внутрішніх стратегій, утвердженні стандартів належного врядування (good governance) та поширенні кращих світових практик. Водночас дієвість подібних механізмів критично залежить від наявності політичної волі суб'єктів владних повноважень та якості їхньої імплементації на рівні вітчизняного законодавства.

Визначальне значення у цьому контексті мають Добровільні керівні принципи ФАО щодо відповідального управління земельними, рибними та лісовими ресурсами. Зазначений документ безпосередньо корелює сталий доступ до природних багатств із гарантуванням продовольчої безпеки, пропонуючи комплексний підхід до захисту прав землекористувачів як основи національної стійкості [2].

Окреме місце посідають норми міжнародного гуманітарного права, зокрема Женевські конвенції 1949 року та Додатковий протокол I 1977 року, які прямо забороняють використання голоду як методу ведення війни та зобов'язують сторони конфлікту утримуватися від знищення об'єктів, необхідних для виживання цивільного населення [5]. За умов збройних конфліктів ці норми набувають практичного значення, оскільки порушення продовольчої інфраструктури використовується як елемент тиску на державу та населення. Це свідчить про трансформацію продовольчої безпеки з економічної категорії у складову міжнародної безпеки. У цьому контексті відповідні дії можуть кваліфікуватися як порушення міжнародного гуманітарного права та воєнні злочини, що передбачає міжнародно-правову відповідальність. Важливо, що сучасна практика міжнародних судових інституцій поступово розширює тлумачення цих норм, визнаючи атаки на продовольчу інфраструктуру складовою ширшої категорії заборонених методів ведення війни. Це створює підґрунтя для притягнення винних осіб до міжнародної кримінальної відповідальності.

Подальший розвиток міжнародних стандартів відображено у Цілях сталого розвитку ООН, зокрема Цілі 2 «Подолання голоду», яка передбачає забезпечення продовольчої безпеки, поліпшення харчування та розвиток сталого сільського господарства [2]. Зазначена ціль також інтегрує показники моніторингу, що дозволяють здійснювати кількісну оцінку стану продовольчої безпеки, включаючи рівень недоїдання, доступ до продовольства та стабільність аграрного виробництва. Ця ціль тісно пов'язана з іншими напрямами розвитку, зокрема подоланням бідності та забезпеченням доступу до ресурсів, що підкреслює міжгалузевий характер продовольчої безпеки. Таким чином, міжнародно-правова база формує системне бачення продовольчої безпеки як інтегрованої категорії, що поєднує правові, економічні та безпекові аспекти.

Інституційне забезпечення реалізації продовольчої безпеки здійснюється системою міжнародних організацій. Провідну роль відіграє Food and Agriculture Organization, яка забезпечує формування глобальної політики у сфері продовольства, здійснює аналітичну діяльність та розробляє рекомендації для держав [2]. Ключовим елементом є World Food Programme, що забезпечує оперативне реагування на гуманітарні кризи шляхом надання продовольчої допомоги [3]. Аналітичну та координаційну функцію виконує Committee on World Food Security, який формує стратегічні підходи до забезпечення продовольчої безпеки [2]. Суттєву функцію виконують міжнародні фінансові інституції, зокрема World Bank, який фінансує проєкти відновлення аграрного сектору [4], а також Міжнародний фонд сільськогосподарського розвитку, спрямований на підтримку малих виробників [32]. Також задіяні регіональні механізми координації, зокрема в межах Європейського Союзу, які забезпечують узгодження політик держав-членів у сфері продовольчої безпеки.

Взаємодія між цими інституціями здійснюється на основі принципу багаторівневого глобального врядування (multi-level

governance), що забезпечує координацію між глобальним, регіональним та національним рівнями прийняття рішень. Це дозволяє забезпечити узгодженість політик та уникнути фрагментації управлінських рішень. Разом з тим ефективність діяльності зазначених інституцій нерідко обмежується проблемами координації, дублювання функцій та залежністю від політичної кон'юнктури, що може знижувати оперативність реагування на кризові ситуації, а також створювати ризики дублювання ресурсів та неефективного розподілу допомоги.

Практика міжнародного реагування на продовольчі кризи демонструє їх системний характер. Характерною ознакою сучасних продовольчих криз є їх каскадний характер, коли первинні шоки (війна, кліматичні зміни) спричиняють вторинні ефекти у вигляді інфляції, порушення логістики та соціальної нестабільності. За оцінками міжнародних організацій, сотні мільйонів людей у світі перебувають у стані хронічної продовольчої нестабільності [2], причому значна частина цих випадків припадає саме на країни, що перебувають у стані збройного конфлікту або постконфліктного відновлення. Збройні конфлікти є одним із ключових чинників гострої продовольчої небезпеки [3]. При цьому взаємозв'язок між конфліктами та продовольчою нестабільністю має циклічний характер: продовольчі кризи можуть не лише бути наслідком війни, але й виступати фактором її ескалації, посилюючи соціальну напругу та політичну нестабільність. Це підтверджується ситуаціями у Сирії, Ємені, Ефіопії, де руйнування аграрної інфраструктури, блокування логістики та переміщення населення призвели до масштабних гуманітарних криз [33].

Досвід Сирії свідчить, що тривале руйнування систем водопостачання та іригації призводить до деградації аграрного виробництва та залежності від гуманітарної допомоги [34]. При цьому надмірна залежність від зовнішньої допомоги створює ризики її

політизації та формування довгострокової економічної залежності, що ускладнює відновлення національних продовольчих систем. У Ємені тривала блокада ключових морських портів та атаки на об'єкти продовольчої інфраструктури фактично паралізували імпорт життєво необхідних товарів, що спричинило масовий голод та колапс продовольчої системи [35]. Особливо критичною є ситуація в Ефіопії (зокрема в регіоні Тиграй), де навмисне обмеження доступу до продовольства та ресурсів використовувалося як інструмент політичного тиску, що спровокувало одну з наймасштабніших продовольчих криз останніх років та поставило мільйони людей на межу виживання [36]. Ці приклади демонструють, що в умовах війни ключовими ризиками є не лише знищення виробництва, а й порушення доступу до харчових ресурсів. Це означає, що навіть за наявності внутрішнього виробництва держава може втратити продовольчу стабільність через логістичні та інституційні збої.

Окремої уваги заслуговує практика функціонування «зернових коридорів», яка стала унікальним прикладом динамічної міжнародної координації в умовах глобальної нестабільності. Гарантування експорту української агропродукції через морські та річкові порти дозволило не лише підтримати економічну стійкість держави, а й суттєво стабілізувати світові ринки продовольства, запобігаючи стрибкам цін на базові продукти [4; 10]. Водночас інституційна крихкість цього механізму продемонструвала його критичну залежність від кон'юнктурних домовленостей, що актуалізує пошук більш стабільних логістичних та безпекових альтернатив. Разом з тим, зазначений механізм виявив обмеженість класичних міжнародно-правових інструментів, оскільки його функціонування значною мірою залежало від політичних домовленостей, а не від стабільних юридичних гарантій.

Досвід Європейського Союзу у цьому контексті є одним із найбільш релевантних для розбудови вітчизняної системи кризового

адміністрування. Спільна аграрна політика ЄС передбачає не лише пряму фінансову підтримку виробників, а й функціонування складних стабілізаційних механізмів, систем стратегічного резервування та превентивного прогнозування ризиків [15]. Зокрема, інституційна архітектура ЄС включає механізми кризового резерву, здатні оперативно нівелювати різкі коливання цін та дефіцит продовольчих ресурсів [27]. У період ескалації воєнних дій ЄС продемонстрував високу адаптивність, ініціювавши створення «Шляхів солідарності» (Solidarity Lanes) — альтернативних логістичних маршрутів для безперебійного українського експорту [37]. Це свідчить про критичну важливість гнучких управлінських інструментів та міждержавної інтеграції у сфері безпеки. Крім того, важливим елементом є функціонування єдиної системи аграрної статистики та прогнозування, яка дозволяє здійснювати раннє виявлення ризиків та оперативне коригування політики. Це забезпечує високий рівень адаптивності аграрної політики до кризових викликів. Окремо слід враховувати вплив кліматичних змін, які дедалі більше посилюють нестабільність продовольчих систем, зокрема через зростання частоти посух, деградацію ґрунтів та зниження врожайності.

Особливий інтерес становить досвід Ізраїлю, який десятиліттями успішно функціонує в умовах перманентних безпекових загроз. У цій країні стійкість продовольчої системи гарантується через випереджальний розвиток високотехнологічного аграрного сектору, впровадження інноваційних іригаційних рішень, суцільного цифрового моніторингу та жорсткого державного стратегічного планування [15]. Ключовим є концептуальний підхід, за якого національна безпека забезпечується через глибоку інтеграцію агротехнологій, адаптивного управління та багаторівневого системного аналізу ризиків [12]. Зокрема, масове впровадження систем крапельного зрошення та автоматизованих комплексів

управління виробництвом дозволяє мінімізувати деструктивний вплив природних факторів і гарантувати стабільність постачання навіть у пікові моменти воєнно-політичних криз. Такий підхід демонструє ефективність поєднання технологічної модернізації та централізованого стратегічного планування у забезпеченні стійкості продовольчих систем.

Для України, з огляду на масштаби воєнних руйнувань, надзвичайно цінним є також досвід постконфліктного відновлення Хорватії та Боснії і Герцеговини. Ці держави після завершення активних бойових дій здійснили успішну ревіталізацію аграрного сектору через залучення цільової міжнародної допомоги, масштабне гуманітарне розмінування територій та розробку спеціалізованих програм підтримки малих фермерів [4]. Практика цих країн беззаперечно підтверджує, що відновлення продовольчої безпеки — це тривалий стратегічний процес, який вимагає органічного поєднання глибоких внутрішніх реформ та системної зовнішньої підтримки. При цьому критичним і першочерговим етапом стає розмінування сільськогосподарських угідь, без завершення якого повноцінне відновлення аграрного циклу та інвестиційна привабливість галузі залишаються фактично неможливими. Це підкреслює критичну роль безпекового компоненту у відновленні аграрного сектору. Важливим висновком є також те, що міжнародна допомога є ефективною лише за умови наявності внутрішньої інституційної спроможності держави до її адміністрування.

Аналіз міжнародного досвіду дозволяє визначити конкретні напрями вдосконалення політики України. Насамперед доцільним є створення ефективної системи стратегічних резервів продовольства, здатної забезпечити автономність держави у кризових умовах. Важливим є впровадження цифрових систем моніторингу продовольчих ресурсів, що дозволить оперативно реагувати на зміни ситуації. Окрему увагу слід приділити розвитку логістичної

інфраструктури та диверсифікації експортних маршрутів. Не менш суттєвим є створення механізмів страхування воєнних ризиків для аграрного бізнесу, що дозволить підтримати виробництво в умовах нестабільності. Водночас важливим є посилення взаємодії з міжнародними організаціями, що дозволить залучати фінансові та технічні ресурси для відновлення аграрного сектору.

Таким чином, міжнародні інструменти забезпечення продовольчої безпеки формують комплексну систему, яка поєднує правові, інституційні та практичні механізми. Для України їх значення полягає не лише у подоланні наслідків війни, а й у формуванні довгострокової моделі стійкого розвитку, здатної гарантувати функціонування держави навіть в умовах тривалих кризових викликів. При цьому ключовим завданням є інституційна імплементація міжнародних стандартів у національну правову систему, що передбачає їх адаптацію з урахуванням специфіки воєнного стану. Без інтеграції міжнародних інструментів у національну систему управління досягнення стабільної продовольчої безпеки в умовах війни є практично неможливим. У цьому контексті вирішального значення набуває не лише імплементація міжнародних стандартів, але й формування інституційної спроможності держави до їх ефективного застосування, що включає розвиток адміністративних, фінансових та аналітичних механізмів управління продовольчими ризиками.

5. Висновки

Результати проведеного дослідження дозволяють розкрити зміст фундаментальних зрушень у механізмах гарантування продовольчої безпеки України під час війни та довести необхідність її переосмислення як базису національної безпеки. Аналіз теоретичних концептів, ревізія нормативного масиву та компаративний розгляд світових практик фіксують появу нової управлінської логіки. У цій системі координат продовольчий сектор виходить за межі суто

соціально-економічної сфери, трансформуючись у ключовий чинник стратегічної стійкості держави.

Дослідження підтверджує, що в умовах збройної агресії продовольча безпека як об'єкт публічного управління набуває принципово нових характеристик. Це відображається у її закріпленні в засадничих документах стратегічного планування та докорінній зміні пріоритетів державної політики [14; 16]. У підсумку, продовольча сфера перетворюється з суто галузевого питання на критичний вузол національної стійкості.

Дослідження підтверджує, що традиційні моделі публічного управління, орієнтовані на стабільні умови функціонування, виявляються недостатньо ефективними у ситуаціях високої невизначеності. У зв'язку з цим обґрунтовано необхідність переходу до кризового адміністрування як окремого функціонального режиму діяльності держави. Його сутність полягає у забезпеченні безперервності функціонування ключових систем, оперативності прийняття рішень та адаптивності управлінських механізмів до динамічних змін середовища. Зокрема, йдеться про застосування механізмів швидкого перерозподілу ресурсів, спрощення регуляторних процедур та використання цифрових платформ управління. Встановлено, що кризове адміністрування у сфері продовольчої безпеки повинно поєднувати елементи правового регулювання, інституційної координації та стратегічного планування, що забезпечує комплексний характер державної політики.

У ході дослідження доведено, що сучасна система нормативно-правового забезпечення продовольчої безпеки України перебуває на етапі активної трансформації. Це зумовлено прийняттям спеціальних нормативних актів у період воєнного стану та посиленням ролі виконавчої влади у прийнятті оперативних рішень [6; 13]. Вона характеризується зростанням ролі підзаконного регулювання, підвищенням рівня централізації управлінських рішень та

одночасною необхідністю забезпечення балансу між ефективністю державного управління і дотриманням принципу верховенства права. Встановлено, що правовий режим воєнного стану виступає ключовим фактором, який визначає особливості функціонування системи публічного адміністрування, зокрема у сфері продовольчого забезпечення.

Результати дослідження підтверджують, що продовольча безпека є невід'ємною частиною загальної системи національної безпеки, яка перебуває у тісній зв'язці з енергетичним, економічним та інформаційним секторами. Будь-який збій в одному з них запускає ланцюгову реакцію, що розбалансовує всю систему. Наочним прикладом стали події 2022–2024 років, коли удари по енергосистемі миттєво вдарили по зберіганню та переробці врожаю. По суті, без стабільної електрики неможливе сучасне агровиробництво, а через інформаційні атаки чи фейки на ринку легко спровокувати паніку та дефіцит. Тому захист продовольства сьогодні неможливий без одночасного захисту енергомереж та інформаційного простору.

Важливим результатом дослідження є визначення ключових проблем, що перешкоджають ефективному забезпеченню продовольчої безпеки в Україні. До них віднесено: недостатню диверсифікацію логістичних маршрутів, обмеженість стратегічних резервів продовольства, низький рівень цифровізації аграрного сектору, а також недостатню інтеграцію національної системи управління у міжнародні механізми реагування на кризові ситуації. Окремо підкреслено проблему забруднення та мінування сільськогосподарських земель, що суттєво обмежує виробничий потенціал аграрного сектору. У сукупності ці фактори свідчать про структурну вразливість національної продовольчої системи.

Аналіз міжнародно-правових інструментів засвідчив, що продовольча безпека визнається на глобальному рівні як складова прав людини та міжнародної безпеки. Зокрема, Міжнародний пакт

про економічні, соціальні і культурні права закріплює право на достатнє харчування, що покладає на держави відповідні зобов'язання [1]. Норми міжнародного гуманітарного права, зокрема Женевські конвенції 1949 року та Додатковий протокол I 1977 року, встановлюють заборону використання голоду як методу ведення війни [5]. Це підтверджує, що продовольча безпека має не лише економічний, а й чітко виражений правовий і безпековий вимір.

Дослідження діяльності міжнародних інституцій показало, що їх роль у забезпеченні продовольчої безпеки є визначальною, особливо в умовах криз. Організація Об'єднаних Націй з питань продовольства і сільського господарства здійснює моніторинг та аналітичне забезпечення [2], Всесвітня продовольча програма забезпечує гуманітарну допомогу [33], а Світовий банк фінансує проєкти відновлення аграрного сектору [4]. Встановлено, що ефективність міжнародних інструментів значною мірою залежить від рівня координації між державами та міжнародними організаціями.

Практика міжнародного реагування на продовольчі кризи, зокрема в умовах збройних конфліктів, свідчить про системний характер загроз. Досвід Сирії, Ємену та Ефіопії демонструє, що ключовими факторами продовольчої нестабільності є не лише знищення виробництва, а й порушення доступу до продовольства через блокування логістики та переміщення населення [34; 35; 36]. У цьому контексті особливого значення набувають механізми міжнародної координації, які дозволяють частково компенсувати негативні наслідки війни.

Окремо проаналізовано приклад функціонування «зернових коридорів», який довів ефективність багатосторонніх механізмів співпраці. Забезпечення експорту українського зерна дозволило стабілізувати глобальні ринки продовольства та запобігти загостренню світової продовольчої кризи. Цей досвід підтверджує, що навіть у складних геополітичних умовах можлива

реалізація ефективних міжнародних інструментів за умови належної координації.

Значну увагу приділено аналізу досвіду Європейського Союзу та інших держав. Встановлено, що Спільна аграрна політика ЄС забезпечує високий рівень стабільності продовольчої системи завдяки поєднанню фінансової підтримки, регулювання ринку та системи стратегічних резервів [27]. Досвід Ізраїлю свідчить про ефективність інтеграції технологічних інновацій у аграрний сектор, що дозволяє забезпечувати продовольчу безпеку навіть в умовах постійних безпекових загроз [38]. Практика Хорватії та Боснії і Герцеговини демонструє важливість післявоєнного відновлення аграрного сектору через розмінування територій та підтримку фермерів [39].

Узагальнення міжнародного досвіду дозволило сформулювати низку практичних рекомендацій для України. По-перше, доцільним є створення ефективної системи стратегічних резервів продовольства, що забезпечить автономність держави у кризових умовах. По-друге, необхідно впроваджувати цифрові системи моніторингу продовольчих ресурсів, які дозволять оперативно реагувати на зміни ситуації. По-третє, важливим є розвиток логістичної інфраструктури та диверсифікація експортних маршрутів. По-четверте, слід посилити інтеграцію України у міжнародні механізми забезпечення продовольчої безпеки.

Крім того, обґрунтовано необхідність розвитку інституційної спроможності держави у сфері кризового адміністрування. Йдеться про створення єдиного координаційного центру, який забезпечуватиме узгодженість дій різних органів влади, а також про розширення кола суб'єктів управління за рахунок залучення наукових установ та приватного сектору. Встановлено, що ефективність державної політики значною мірою залежить від рівня взаємодії між державними та недержавними інституціями.

Узагальнюючи результати дослідження, слід констатувати, що система забезпечення продовольчої безпеки України перебуває на етапі глибокої трансформації. Вона поступово переходить від реактивної моделі управління до проактивної, що базується на принципах інтеграції, адаптивності та стратегічного планування. Така трансформація відповідає сучасним викликам і створює передумови для формування ефективної системи кризового адміністрування.

Отже, продовольча безпека під час війни перетворюється на фундамент національної стійкості. Від неї напряму залежить, чи зможе держава та суспільство вистояти під тиском тривалих криз. Щоб ця система працювала, мало просто мати запаси зерна — потрібен «союз» законів, чіткої роботи держорганів та активної допомоги світу. Якщо впровадити підходи, запропоновані в роботі, Україна зможе не лише залікувати рани війни, а й стати сильнішою у майбутньому. Це дасть змогу нашій країні остаточно закріпитися у світовій системі продовольчої безпеки як впливовому та надійному гравцю.

Список використаних джерел:

1. Міжнародний пакт про економічні, соціальні і культурні права : прийнятий 16.12.1966 року Генеральною Асамблеєю ООН. URL: https://zakon.rada.gov.ua/laws/show/995_042#Text

2. Food and Agriculture Organization of the United Nations. (2024). The State of Food Security and Nutrition in the World. Rome : FAO. URL: https://www.fao.org

3. Global Network Against Food Crises. (2024). Global Report on Food Crises 2024. URL: https://www.fsinplatform.org

4. World Bank. (2025). Food Security Update. Washington, DC : World Bank. URL: https://www.worldbank.org

5. Женевські конвенції про захист жертв війни від 12.08.1949 р.; Додатковий протокол I від 08.06.1977 р. : міжнародні договори. URL: https://zakon.rada.gov.ua/laws/show/995_151#Text

6. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

7. Стратегія продовольчої безпеки України до 2027 року : розпорядження Кабінету Міністрів України від 23.07.2024 р. № 684-р. URL: https://zakon.rada.gov.ua/laws/show/684-2024-%D1%80#Text

8. Organisation for Economic Co-operation and Development. (2023). Global Food Security Challenges. Paris : OECD Publishing. URL: https://www.oecd.org

9. International Food Policy Research Institute. (2024). Global Food Policy Report. Washington, DC: IFPRI. URL: https://www.ifpri.org

10. Kostruba, A. (2025). Managing foreign business operations in Ukraine in the context of war. *Business Horizons*, 68(1), 67–81. DOI: https://doi.org/10.1016/j.bushor.2024.01.003.

11. Mitchell, M. (2009). Complexity: A Guided Tour. Oxford : Oxford University Press.

12. Renn, O. (2008). Risk Governance: Coping with Uncertainty in a Complex World. London : Earthscan.

13. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 р. № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text

14. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

15. Melnyk, L., Kepko, V., & Nikonenko, O. (2024). Foreign experience of ensuring the country's food security — challenges for Ukraine. *The Institute of Accounting, Control and Analysis in the Globalization Circumstances*, 1(2). DOI: https://doi.org/10.35774/ibo2024.01-02.045.

16. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

17. UNDP. (1994). Human Development Report 1994. Oxford : Oxford University Press.

18. Про затвердження Енергетичної стратегії України на період до 2050 року : розпорядження Кабінету Міністрів України від 21.04.2023 р. № 373-р. URL: https://zakon.rada.gov.ua/laws/show/373-2023-р#Text

19. Zuievska N., Serhiienko S., Tkachuk S. (2023). Assessment of the vulnerability of energy infrastructure objects to explosive impacts. *Mining of Mineral Deposits*, 17(2), 45–56.

20. Kostruba, A. V., & Kulynych, P. F. (2020). Improvement of public control over the use of land resources as an important aspect of modernisation of the Ukrainian state in the XXI century. *International Journal of Criminology and Sociology*, 9, 3095–3103. DOI: https://doi.org/10.6000/1929-4409.2020.09.376.

21. Ківалов С. В., Біла-Тіунова Л. Р., Латковська Т. А. та ін. (2022). Адміністративістика в умовах цифровізації: теорія, правове регулювання, практика. Одеса : Видавничий дім «Гельветика». DOI: https://doi.org/10.32837/11300.21108.

22. Про державну підтримку сільського господарства України : Закон України від 24.06.2004 р. № 1877-IV. URL: https://zakon.rada.gov.ua/laws/show/1877-15#Text

23. Economist Impact. (2024). Global Food Security Index. URL: https://www.economist.com

24. Голікова К. П. Продовольча безпека держави: сутність, структура та особливості її забезпечення. *Наукові праці Кіровоградського національного технічного університету. Серія: Економічні науки*. 2012. Вип. 22(2). 1–5.

25. Тригуб А. Адміністративно-правове забезпечення продовольчої безпеки України : дис. канд. юрид. наук. Київ, 2012. 206 с.

26. Про схвалення Концепції Державної цільової економічної програми розвитку тваринництва на період до 2033 року: розпорядження

Кабінету Міністрів України від 31.01.2025 р. № 76-р. URL: https://zakon.rada.gov.ua/laws/show/76-2025-%D1%80#Text

27. European Commission. Farm to Fork Strategy. 2020. URL: https://ec.europa.eu

28. Farrell H., Newman A. L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*. 2019. 44(1). 42–79. DOI: https://doi.org/10.1162/isec_a_00351.

29. Kemmerling B., Schetter C., & Wirkus L. The logics of war and food (in)security. *World Development*. 2025. 152. 105791. DOI: 10.1016/j.gfs.2022.100634.

30. UN Committee on Economic, Social and Cultural Rights. General Comment No. 12. 1999. URL: https://www.refworld.org

31. Rome Declaration on World Food Security. 1996. URL: https://www.fao.org

32. International Fund for Agricultural Development. Investing in rural people for food security. Rome: IFAD. 2024. URL: https://www.ifad.org

33. World Food Programme. WFP Global Operational Response Plan 2024. Rome : WFP, 2024. URL: https://www.wfp.org

34. Food and Agriculture Organization. Drought Alert: The Syrian Arab Republic. Rome : FAO, 2025. URL: https://openknowledge.fao.org/handle/20.500.14283/cd5629en

35. Human Rights Watch. World Report 2024: Yemen. 2024. URL: https://www.hrw.org/world-report/2024/country-chapters/yemen

36. OCHA. Ethiopia — Situation Report, 13 December 2024. 2024. URL: https://www.unocha.org/publications/report/ethiopia/ethiopia-situation-report-13-december-2024

37. European Commission. An action plan for EU–Ukraine Solidarity Lanes to facilitate Ukraine's agricultural export and bilateral trade with the EU. Brussels : EC, 2022. URL: https://ec.europa.eu

38. FAO. Digital excellence in agriculture in Europe and Central Asia. Rome : FAO, 2023. URL: https://www.fao.org

39. World Bank. Bosnia and Herzegovina — Emergency Farm Reconstruction Project. 1996.

References:

1. International Covenant on Economic, Social and Cultural Rights: adopted on 16.12.1966 by the UN General Assembly. Retrieved from https://zakon.rada.gov.ua/laws/show/995_042#Text

2. Food and Agriculture Organization of the United Nations. (2024). The State of Food Security and Nutrition in the World. Rome : FAO. Retrieved from https://www.fao.org

3. Global Network Against Food Crises. (2024). Global Report on Food Crises 2024. Retrieved from https://www.fsinplatform.org

4. World Bank. (2025). Food Security Update. Washington, DC: World Bank. Retrieved from https://www.worldbank.org

5. Geneva Conventions for the Protection of War Victims of 12.08.1949; Additional Protocol I of 08.06.1977: international treaties. Retrieved from https://zakon.rada.gov.ua/laws/show/995_151#Text

6. On the legal regime of martial law: Law of Ukraine dated 12.05.2015 No. 389-VIII. Retrieved from https://zakon.rada.gov.ua/laws/show/389-19#Text

7. Food Security Strategy of Ukraine until 2027: Order of the Cabinet of Ministers of Ukraine dated 23.07.2024 No. 684-p. Retrieved from https://zakon.rada.gov.ua/laws/show/684-2024-%D1%80#Text

8. Organisation for Economic Co-operation and Development. (2023). Global Food Security Challenges. Paris: OECD Publishing. Retrieved from https://www.oecd.org

9. International Food Policy Research Institute. (2024). Global Food Policy Report. Washington, DC: IFPRI. Retrieved from https://www.ifpri.org

10. Kostruba, A. (2025). Managing foreign business operations in Ukraine in the context of war. *Business Horizons*, 68(1), 67–81. https://doi.org/10.1016/j.bushor.2024.01.003

11. Mitchell, M. (2009). Complexity: A Guided Tour. Oxford: Oxford University Press.

12. Renn, O. (2008). Risk Governance: Coping with Uncertainty in a Complex World. London: Earthscan.

13. On the introduction of martial law in Ukraine: Decree of the President of Ukraine of 24.02.2022 No. 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text

14. On the National Security Strategy of Ukraine: Decree of the President of Ukraine dated 14.09.2020 No. 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

15. Melnyk, L., Kepko, V., & Nikonenko, O. (2024). Foreign experience of ensuring the country's food security — challenges for Ukraine. *The Institute of Accounting, Control and Analysis in the Globalization Circumstances*, 1(2). https://doi.org/10.35774/ibo2024.01-02.045.

16. On the National Security of Ukraine: Law of Ukraine dated 21.06.2018 No. 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

17. UNDP. (1994). Human Development Report 1994. Oxford: Oxford University Press.

18. On approval of the Energy Strategy of Ukraine for the period until 2050: Order of the Cabinet of Ministers of Ukraine dated 21.04.2023 No. 373-p. URL: https://zakon.rada.gov.ua/laws/show/373-2023-p#Text

19. Zuievska, N., Serhiienko, S., & Tkachuk, S. (2023). Assessment of the vulnerability of energy infrastructure objects to explosive impacts. Mining of Mineral Deposits, 17(2), 45–56.

20. Kostruba, A. V., & Kulynych, P. F. (2020). Improvement of public control over the use of land resources as an important aspect of modernization of the Ukrainian state in the XXI century. *International Journal of Criminology and Sociology*, 9, 3095–3103. https://doi.org/10.6000/1929-4409.2020.09.376.

21. Kivalov S. V., Bila-Tiunova L. R., Latkovska T. A. et al. (2022). Administrative science in the context of digitalization: theory, legal regulation, practice. Odesa: Helvetica Publishing House. https://doi.org/10.32837/11300.21108

22. On state support for agriculture in Ukraine: Law of Ukraine of 24.06.2004 No. 1877-IV. URL: https://zakon.rada.gov.ua/laws/show/1877-15#Text

23. Economist Impact. (2024). Global Food Security Index. URL: https://www.economist.com

24. Golikova, K. P. (2012). Food security of the state: essence, structure and features of its provision. Scientific works of Kirovohrad National Technical University. *Economic Sciences*, vol. 22(2), 1–5.

25. Trygub, A. (2012). Administrative and legal provision of food security of Ukraine: dissertation of candidate of legal sciences. Kyiv, 206 p.

26. On approval of the Concept of the State Targeted Economic Program for the Development of Livestock for the Period up to 2033: Order of the Cabinet of Ministers of Ukraine dated 31.01.2025 No. 76-p. Retrieved from https://zakon.rada.gov.ua/laws/show/76-2025-%D1%80#Text

27. European Commission. (2020). Farm to Fork Strategy. URL: https://ec.europa.eu

28. Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 44(1), 42–79. DOI: https://doi.org/10.1162/isec_a_00351.

29. Kemmerling, B., Schetter, C., & Wirkus, L. (2025). The logics of war and food (in)security. *World Development*, 152, 105791. DOI: 10.1016/j.gfs.2022.100634.

30. UN Committee on Economic, Social and Cultural Rights. (1999). General Comment No. 12. URL: https://www.refworld.org

31. Rome Declaration on World Food Security. (1996). URL: https://www.fao.org

32. International Fund for Agricultural Development. (2024). Investing in rural people for food security. Rome: IFAD. URL: https://www.ifad.org

33. World Food Programme. (2024). WFP Global Operational Response Plan 2024. Rome: WFP. URL: https://www.wfp.org

34. Food and Agriculture Organization. (2025). Drought Alert: The Syrian Arab Republic. Rome: FAO. URL: https://openknowledge.fao.org/handle/20.500.14283/cd5629en

35. Human Rights Watch. (2024). World Report 2024: Yemen. URL: https://www.hrw.org/world-report/2024/country-chapters/yemen

36. OCHA. (2024). Ethiopia — Situation Report, 13 December 2024. URL: https://www.unocha.org/publications/report/ethiopia/ethiopia-situation-report-13-december-2024

37. European Commission. (2022). An action plan for EU–Ukraine Solidarity Lanes to facilitate Ukraine's agricultural export and bilateral trade with the EU. Brussels: EC. URL: https://ec.europa.eu

38. FAO. (2023). Digital excellence in agriculture in Europe and Central Asia. Rome: FAO. URL: https://www.fao.org

39. World Bank. (1996). Bosnia and Herzegovina — Emergency Farm Reconstruction Project.

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВОСУДДІ: ЗАБЕЗПЕЧЕННЯ БАЛАНСУ ПУБЛІЧНОГО І ПРИВАТНОГО ІНТЕРЕСУ

THEORETICAL AND LEGAL FOUNDATIONS FOR THE USE OF ARTIFICIAL INTELLIGENCE IN THE ADMINISTRATION OF JUSTICE: ENSURING THE BALANCE BETWEEN PUBLIC AND PRIVATE INTERESTS

Kopytova O. S.,
Doctor of Law, Senior Researcher, Retired Judge,
Associate Professor at the Department of Economic
and Legal Disciplines, Educational and Scientific Institute of Law
and Psychology,
National Academy of Internal Affairs,
Kjyv, Ukraine

Abstract. In this section,a comprehensive theoretical and legal analysis of the use of artificial intelligence in the administration of justice through the prism of balancing public and private interests. It substantiates that the integration of artificial intelligence technologies into judicial activity transforms not only procedural mechanisms but also the very nature of adjudication, raising fundamental questions about the limits of automation in law. Particular attention is paid to the correlation between the technocratic approach, focused on efficiency and optimization of judicial processes, and the humanistic foundations of justice, which require the preservation

of judicial discretion, individual assessment of cases, and respect for fundamental rights.

The study argues that the balance between public and private interests serves as a key criterion for determining the admissibility and limits of artificial intelligence application in judicial proceedings. Public interest is manifested in ensuring the efficiency, accessibility, and predictability of justice, while private interest is reflected in the protection of individual rights, procedural fairness, and the right to a reasoned judicial decision. The paper proposes a conceptual model of "graduated automation" in justice, distinguishing between zones of automation, decision-support, and exclusive human adjudication.

It is concluded that the use of artificial intelligence in the judiciary is acceptable only under conditions of preserving human primacy in decision-making, ensuring algorithmic transparency and accountability, and maintaining proportionality between technological efficiency and the protection of human rights.

Keywords: artificial intelligence, administration of justice, public interest, private interest, balance of interests, judicial discretion, algorithmic decision-making, transparency, human-centered justice, digitalization of justice.

1. Цифрова трансформація правосуддя як передумова використання штучного інтелекту

Сучасний етап розвитку цивілізації характеризується глибинними трансформаціями інституційного устрою держав під впливом технологічного прогресу. Феномен інформаційного суспільства, теоретичні підвалини якого були закладені у працях Д. Белла, М. Кастельса, Е. Тоффлера та інших дослідників постіндустріальних трансформацій, передбачає якісну зміну не лише економічних і соціальних відносин, але й механізмів здійснення

державної влади, зокрема — судової. Концепція інформаційного суспільства, розроблена Д. Беллом у фундаментальній праці «Прийдешнє постіндустріальне суспільство» (1973), виходила з того, що головним ресурсом суспільного розвитку стає інформація, а провідними агентами соціальної організації — суб'єкти, здатні ефективно її опрацьовувати [16]. М. Кастельс розвинув цю ідею у теорії мережевого суспільства, стверджуючи, що влада в умовах цифровізації реалізується через контроль над інформаційними потоками [19]. Ці теоретичні побудови мають безпосереднє значення для розуміння трансформацій судової влади: в умовах, коли інформаційне середовище стає основним простором соціальних взаємодій, судова система не може залишатися ізольованою від технологічних зрушень.

Поняття «цифровізація» (digitalization) у контексті державного управління означає не просте переведення документообігу в електронну форму, а системну переорієнтацію логіки функціонування публічних інститутів відповідно до принципів цифрової економіки — прозорості, ефективності, орієнтованості на користувача та опрацювання великих масивів даних [25]. У судовій сфері цифровізація набуває особливого значення з огляду на специфічну природу правосуддя як виду державної діяльності, пов'язаного з вирішенням правових конфліктів і захистом суб'єктивних прав.

Слід розрізняти кілька концептуально різних стадій технологічного освоєння судової діяльності. Перша — автоматизація (automation) — полягає у заміні ручних операцій комп'ютерними засобами без суттєвої зміни логіки процесу. Друга — цифровізація у вузькому значенні (digitization) — означає конвертацію аналогових даних у цифровий формат. Третя — власне цифрова трансформація (digital transformation) — передбачає фундаментальну реінженерію процесів з метою використання технологічних можливостей для досягнення якісно нових результатів [62, с. 26]. Саме

остання стадія є теоретично найбільш значущою для предмета даного дослідження.

Передумови цифрової трансформації судової влади мають декілька вимірів. Нормативний вимір пов'язаний із формуванням міжнародно-правових та національних стандартів електронного урядування, що поступово поширилися на судову сферу. Важливу роль у формуванні глобальної політики цифровізації публічного управління відіграють документи Організації Об'єднаних Націй, присвячені розвитку інформаційно-комунікаційних технологій. Зокрема, Резолюція Генеральної Асамблеї ООН 57/238 "Information and communication technologies for development" (2002) підкреслює значення використання цифрових технологій для підвищення ефективності державного управління, розвитку електронного урядування та забезпечення доступу громадян до публічних послуг [55]. На рівні Ради Європи важливе значення для формування стандартів функціонування судової влади мають рекомендації Комітету Міністрів, зокрема Recommendation CM/Rec(2010)12 щодо незалежності, ефективності та відповідальності суддів. Питання впливу технологічних змін на здійснення правосуддя також розглядаються у документах Консультативної ради європейських суддів (CCJE), зокрема у Висновку № 14 (2011) «правосуддя та інформаційні технології (IT)», де підкреслюється, що використання цифрових технологій має сприяти підвищенню ефективності судочинства, не підриваючи при цьому незалежності суддів та принципу справедливого суду [52].

Соціальний вимір цифрової трансформації правосуддя зумовлений змінами очікувань суспільства щодо якості та доступності публічних послуг. Дослідження Організації економічного співробітництва та розвитку свідчать, що рівень довіри громадян до інституцій значною мірою залежить від їхньої здатності діяти прозоро, справедливо та ефективно, забезпечуючи своєчасне і передбачуване

вирішення суспільно значущих питань, зокрема у сфері правосуддя [44]. Цифрові технології розглядаються як інструмент подолання структурних вад традиційного судочинства — надмірної тривалості процесів, географічної нерівності в доступі до правосуддя та інституційної непрозорості.

Технологічний вимір визначається конвергенцією низки ключових технологій — хмарних обчислень, великих даних (big data), блокчейну, інтернету речей та штучного інтелекту, — що у своїй сукупності формують технічний субстрат цифрового правосуддя. Особливо важливим є феномен «великих даних» у судовій сфері: масиви судових рішень, правових текстів і процесуальних документів, нагромаджені впродовж десятиліть, набувають нової цінності в умовах, коли алгоритми машинного навчання здатні виявляти в них статистично значущі закономірності [57].

Доктрина електронного правосуддя (e-justice) формувалася поступово. Починаючи з 1990-х років, у США, Австралії та низці держав-членів Євросоюзу запроваджувалися системи електронного подання документів (e-filing), електронного оповіщення сторін, онлайн-доступу до судових реєстрів. Ці заходи, однак, стосувалися переважно адміністративно-процесуальних аспектів діяльності судів, не торкаючись суті правосудної функції [56]. Якісний стрибок відбувся з початком широкого впровадження алгоритмічних систем, здатних аналізувати правову інформацію та надавати рекомендації щодо вирішення справ. Цей процес поставив принципово нові запитання: чи сумісне алгоритмічне прийняття рішень із концепцією незалежного судді? Яким чином технологічні засоби можуть сприяти реалізації конституційних гарантій правосуддя, не підриваючи їх?

Варто звернути увагу на особливу специфіку судової влади порівняно з іншими гілками влади в контексті цифровізації. Якщо виконавча влада може адаптувати технологічні рішення відносно

гнучко, а законодавча — регулювати темп власної цифровізації нормативними засобами, то судова влада пов'язана жорсткими конституційно-правовими та процесуальними стандартами, що обмежують допустимі форми технологічної модернізації. Конституційний принцип незалежності суддів, гарантії права на справедливий суд, вимоги обґрунтованості та умотивованості судових рішень — усе це формує своєрідний нормативний «каркас», в межах якого можлива цифрова трансформація судової діяльності.

Показовим є досвід Китайської Народної Республіки, де починаючи з 2017 року функціонують «Інтернет-суди», що розглядають значну частину справ у повністю онлайн-режимі [63]. Вочевидь, цей досвід не може бути механічно перенесений у правові системи, засновані на принципах верховенства права та незалежності судової влади в ліберально-демократичному розумінні, проте він виразно ілюструє технологічний потенціал цифрового правосуддя.

Щодо вітчизняного правового розвитку цифровізація судової системи України здійснюється в руслі загальних євроінтеграційних перетворень. Закон України «Про судоустрій і статус суддів» 2016 року [6] та процесуальна реформа 2017 року заклали нормативні основи для запровадження елементів електронного судочинства. Система «Електронний суд» та Єдиний державний реєстр судових рішень є початковими, але важливими кроками на шляху до повноцінної цифрової трансформації. Водночас впровадження штучного інтелекту у вітчизняну судову систему залишається перспективним завданням, реалізація якого потребує ґрунтовного теоретико-правового опрацювання.

Таким чином, цифровізація судової влади є не локальним технічним явищем, а проявом глибинних трансформацій інформаційного суспільства, що зачіпають фундаментальні засади організації публічної влади. Вона створює як нові можливості для підвищення ефективності правосуддя, так і нові виклики для правових

гарантій, покликаних захищати права людини в судовому процесі. Осмислення цих трансформацій є вихідним пунктом для теоретичного аналізу проблеми застосування штучного інтелекту у правосудді [8].

Визначення поняття штучного інтелекту є завданням, що перебуває на перетині комп'ютерних наук, філософії та права. Відсутність єдиного загальновизнаного підходу в науковій літературі зумовлена, з одного боку, динамічним характером самої технології, а з іншого — різними методологічними позиціями дослідників щодо критеріїв «інтелектуальності» машинних систем. З точки зору права принципове значення має розмежування між вузьким (narrow AI) та загальним (general AI, або AGI) штучним інтелектом. Вузький штучний інтелект, що є єдиним практично реалізованим типом на сьогодні, вирішує конкретні завдання у чітко визначених предметних областях — розпізнавання образів, обробка природної мови, прогнозування — не виявляючи здатності до узагальнення за межами тренувального домену. Загальний штучний інтелект, здатний до людиноподібного гнучкого мислення, залишається гіпотетичним конструктом, що не має практичного значення для нинішнього правового регулювання [47].

Регуляторне визначення штучного інтелекту, закріплене у Регламенті Європейського Союзу про штучний інтелект (AI Act, Regulation (EU) 2024/1689), характеризує його як «машинну систему, розроблену для роботи з різними ступенями автономності, яка може після розгортання адаптуватися та яка на основі отриманих входів генерує виходи, такі як прогнози, рекомендації, рішення або контент, що впливають на реальні або віртуальні середовища» [54]. Ця дефініція, будучи технологічно нейтральною, охоплює широкий спектр алгоритмічних систем — від простих систем правил (rule-based systems) до складних нейронних мереж глибокого навчання.

Для цілей правового аналізу застосування ШІ у правосудді доцільно виокремити кілька ключових функціональних характеристик, що відрізняють системи штучного інтелекту від традиційних автоматизованих систем:

1. *Здатність до навчання (machine learning).* На відміну від детерміністичних алгоритмів, поведінка яких цілком визначається програмним кодом, системи машинного навчання виробляють власні поведінкові моделі на основі статистичного аналізу великих масивів даних. У судовому контексті це означає, що система може «виводити» правові закономірності з масивів судових рішень без явного кодування правових правил розробниками [37].

2. *Опрацювання природної мови (natural language processing, NLP).* Правова діяльність пов'язана із текстами за своєю природою — вона оперує нормативними текстами, судовими рішеннями, процесуальними документами, доказами у текстовій формі. Здатність систем ШІ аналізувати, класифікувати та генерувати природномовні тексти є критично важливою умовою їх застосовності у правосудді [21].

3. *Розпізнавання образів* (*pattern recognition*). Алгоритми машинного навчання здатні виявляти статистичні закономірності у великих масивах правової інформації, що є основою для прогностичних застосувань у судовій сфері [13].

4. *Прийняття рішень в умовах невизначеності.* Судове правозастосування, як правило, здійснюється в умовах інформаційної та правової невизначеності. Сучасні системи ШІ, на відміну від традиційних експертних систем, здатні функціонувати в умовах неповноти та суперечливості інформації [17].

У системі електронного правосуддя штучний інтелект виконує функції, що можуть бути систематизовані за кількома критеріями. *За предметним критерієм* виокремлюються: системи правового дослідження, системи аналізу документів, системи прогнозування

результатів справ, системи оцінки ризиків та системи автоматизованого прийняття рішень. *За ступенем автономності* доцільно розрізняти: системи підтримки прийняття рішень, що надають інформацію та рекомендації, залишаючи остаточне рішення за людиною; автоматизовані системи, що приймають рішення без участі людини у кожному конкретному випадку, однак у межах, встановлених людиною; та гіпотетичні повністю автономні системи, що приймають рішення самостійно [20].

Функціональний потенціал ШІ у правосудді є надзвичайно широким. У сфері управління судовими справами алгоритмічні системи здатні автоматизувати розподіл справ між суддями, планування судових засідань, контроль строків, пошук і структурування судової практики. У сфері аналізу доказів ШІ застосовується для опрацювання великих масивів документальних матеріалів у рамках процедури e-discovery, автоматичного розпізнавання аудіо- та відеозаписів, верифікації цифрових доказів [38]. Системи обробки природної мови (NLP) дозволяють здійснювати семантичний аналіз документів, виявляючи суперечності та ключові факти, що може суттєво скорочувати витрати на підготовку справи до розгляду [46].

У сфері правового дослідження (legal research) такі системи, як ROSS Intelligence (побудований на базі IBM Watson), Westlaw Edge та LexisNexis Analytics, використовують алгоритми NLP для пошуку та класифікації релевантних правових джерел, виявлення правових прецедентів та відстеження змін у законодавстві. Найбільш дискусійними є застосування ШІ у сфері прогнозування судових рішень та оцінки ризиків. Системи COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) та PSA (Public Safety Assessment) використовуються у США для оцінки ризику рецидивізму при вирішенні питань про запобіжні заходи та умовно-дострокове звільнення [33, с. 224].

Важливим напрямом є використання ШІ для онлайн-вирішення спорів (Online Dispute Resolution, ODR). Платформи ODR, що застосовують алгоритмічні процедури для медіації та арбітражу функціонують у системах eBay (нині Modria), Cyberjustice Laboratory (Канада), а також на рівні ЄС в рамках Директиви 2013/11/EU про альтернативне вирішення спорів [26].

Слід підкреслити, що жодна з перелічених функцій не є технологічно нейтральною з точки зору права. Кожне застосування ШІ у судовій діяльності несе в собі потенційні наслідки для правових гарантій, що є серцевиною конституційного та міжнародно-правового стандарту правосуддя.

Теоретична систематизація моделей використання алгоритмічних систем у судовій діяльності є необхідним кроком для побудови коректної правової концепції цифрового правосуддя. Без чіткого розмежування різних типів алгоритмічного втручання в правосудну діяльність неможливо виробити диференційований правовий підхід до їх регулювання. В юридичній літературі пропонуються різні класифікаційні схеми. Р. Саттон виокремлює «реактивні» та «проактивні» алгоритмічні системи залежно від їхньої орієнтованості на аналіз наявної чи передбачення майбутньої інформації [58]. Інші науковці розрізняють системи «першого покоління» (засновані на правилах) та «другого покоління» (засновані на навчанні) [39]. Для цілей цього дослідження найбільш продуктивною видається класифікація за функціональним призначенням у судовому процесі, що дозволяє охопити всю різноманітність алгоритмічних застосувань.

Аналітична модель використання алгоритмічних систем передбачає їх застосування для опрацювання, класифікації та структурування масивів правової інформації з метою надання суддям та іншим учасникам судового процесу релевантних знань [1, с. 4]. Ця модель є найменш юридично суперечливою,

оскільки не зачіпає безпосередньо процес прийняття рішень. У рамках аналітичної моделі ШІ виконує переважно епістемічну функцію — полегшує доступ до правових знань та їх осмислення. Системи правового дослідження, такі як Casetext, ROSS Intelligence, Luminance, здатні у лічені секунди проаналізувати мільйони сторінок правових текстів, виокремити релевантні прецеденти та виявити суперечності у правозастосовній практиці. Це дозволяє суттєво скорочувати транзакційні витрати правосуддя та підвищувати якість правового аналізу.

Аналітична модель охоплює також системи аналізу аргументації, що виявляють логічну структуру правових документів, виокремлюють правові позиції сторін та оцінюють їх взаємозв'язок. Правовий аспект аналітичної моделі пов'язаний насамперед із питаннями доступу до інформації, захисту персональних даних та авторського права на правові тексти. Концептуально ця модель не порушує вимог права на справедливий суд, оскільки не замінює суддівського судження, а лише розширює його інформаційну базу.

Допоміжна (асистивна) модель передбачає більш глибоке інтегрування алгоритмічних систем у процес прийняття рішень через надання суддям структурованих рекомендацій, оцінок, пропозицій щодо кваліфікації обставин справи або визначення санкцій. На відміну від аналітичної моделі, допоміжна система не просто подає інформацію — вона синтезує її у форму висновків, що безпосередньо орієнтують суддю у напрямі конкретного рішення.

Прогностична модель є найбільш технологічно складною та юридично суперечливою. Вона передбачає використання алгоритмічних систем для передбачення майбутніх подій або результатів — рецидиву злочину, результату апеляційного оскарження, можливих дій сторін судового процесу — на основі статистичного аналізу минулих даних. Теоретичним підґрунтям прогностичної моделі є концепція «передбачувальної поліції» (predictive policing)

та «предиктивного правосуддя» (predictive justice), що отримали широке поширення у США, Великій Британії та низці інших країн [50]. Системи типу PredPol (тепер Geolitica) і HunchLab застосовують алгоритми машинного навчання для прогнозування злочинів у певних просторово-часових координатах. Перенесення цього підходу безпосередньо у судову діяльність означало б, що алгоритм «передбачає» результат судового процесу ще до того, як він розпочнеться.

Прогностична модель у найбільш радикальній формі представлена проєктом «Кейс Кранч» (CaseCrunch), у рамках якого у 2017 році алгоритм прогнозував результати судових рішень Суду ЄС з прав людини з точністю 86,6 %, тоді як група юристів-практиків досягла лише 62,3 % [12].

Теоретична проблематика прогностичної моделі пов'язана з кількома фундаментальними концептуальними протиріччями. По-перше, існує онтологічна суперечність між статистичною природою алгоритмічного прогнозу та індивідуальним характером судового рішення: навіть якщо певна категорія осіб з визначеними характеристиками рецидивує у 80 % випадків, кожен конкретний індивід є унікальним суб'єктом права, а не статистичною абстракцією [34]. По-друге, виникає епістемологічна суперечність: прогностична система навчається на минулих даних, що містять у собі всі систематичні упередження й дискримінаційні практики минулого правосуддя, і тому її «передбачення» є, по суті, відтворенням і легітимізацією цих упереджень [14].

Французьке законодавство зайняло радикально обмежувальну позицію щодо прогностичних моделей: ст. 33 Закону № 2019-222 про програмування та реформу правосуддя 2019 року прямо забороняє аналітичне або статистичне опрацювання даних про особу судді або члена суду з метою прогнозування їхніх майбутніх рішень, встановлюючи кримінальну відповідальність за порушення

цієї заборони [42]. Ця норма відображає фундаментальне занепокоєння щодо небезпеки перетворення правосуддя з нормативно-правового на статистичне явище.

Кожна з описаних моделей — аналітична, допоміжна та прогностична — передбачає специфічний баланс між технологічними можливостями та правовими обмеженнями. Цей баланс і є предметом теоретичного дослідження, що здійснюється в даному розділі монографії.

Правозастосування як особлива форма юридичної діяльності традиційно розглядається у правовій доктрині як інтелектуально-вольовий процес, що передбачає встановлення фактичних обставин справи, вибір та тлумачення норми права, її застосування до конкретних фактів та формування обов'язкового владного припису [3]. Саме ця багатоступенева структура правозастосування, яка поєднує пізнавальний, оціночний та вольовий компоненти, є предметом найбільш гострої теоретичної дискусії щодо допустимості й меж автоматизації судових рішень.

Вихідним теоретичним питанням є: чи є правозастосування за своєю природою алгоритмізованим процесом, що принципово піддається автоматизації, чи воно містить невід'ємний невідчужуваний людський елемент, що унеможливлює повноцінну заміну судді алгоритмом? Відповідь на це питання є не суто академічною — від неї залежать принципові правові висновки щодо допустимості делегування судових функцій алгоритмічним системам.

У теорії права сформувалися дві полярні позиції щодо природи правозастосування. Формалістична традиція, представлена у чистому вигляді концепцією «механічного правосуддя» (mechanical jurisprudence) Р. Паунда, виходить з уявлення про судовий процес як логічну дедукцію: суддя встановлює факти, підводить їх під відповідну норму та виводить юридичний наслідок [51]. Ця модель, що тяжіє до силогістичної схеми (норма + факт = рішення

суду), є теоретичною основою для оптимістичних поглядів на можливості алгоритмізації правосуддя.

О. Голмс у знаменитому афоризмі стверджував, що «загальне право — це не логіка, а досвід», тим самим наголошуючи на принциповій невідчужуваності правосуддя до алгоритмічної процедури [36].

Традиція нормативного позитивізму визнає, що правозастосування поєднує і логічні, і дискреційні елементи: чітке «ядро» норми може застосовуватися відносно механічно, тоді як «відкрита текстура» (open texture) права, за Г. Хартом, завжди залишає простір для розсуду суду [35]. Ця позиція є теоретично найбільш адекватною для аналізу проблеми автоматизації: різні типи судових справ та різні стадії правозастосовного процесу мають неоднаковий потенціал для алгоритмізації.

Осмислення цієї теоретичної розбіжності у контексті ШІ-правосуддя виводить нас на концепцію градуйованої автоматизації. Згідно з нею, правозастосовний процес можна умовно поділити на три зони: «зону автоматизації» (рутинні, стандартизовані операції — реєстрація документів, розподіл справ, розрахунок строків), «зону сприяння» (системи підтримки прийняття рішень, що надають рекомендації без їх нав'язування) та «зону людського резерву» (індивідуалізована оцінка обставин справи, тлумачення оціночних понять, вирішення моральних дилем) [57]. Лише перша зона є цілком безпечною для автоматизації без правових застережень; друга — припустима за умови збереження людського контролю; третя — принципово вимагає участі людини-судді.

Важливим кроком для розмежування допустимої та недопустимої автоматизації є аналіз структури судового рішення. Будь-яке судове рішення містить: встановлення фактичних обставин справи; юридичну кваліфікацію фактів; вибір та тлумачення норми права; застосування правових наслідків. Ці стадії мають принципово різний характер з точки зору потенціалу алгоритмізації.

Встановлення фактів є процесом оцінки доказів, що містить у собі іманентно людський елемент — оцінку достовірності свідків, зважування суперечливих доказів, усунення логічних протиріч. Системи ШІ можуть сприяти систематизації та структуруванню доказової бази, проте кінцева оцінка доказів є результатом процесу розсуду суду, що апелює до загальнолюдського розуміння достовірності та чесності.

Юридична кваліфікація є найближчою до алгоритмічної логіки стадією правозастосування, оскільки передбачає підведення конкретних фактів під абстрактний склад правової норми. Проте і тут виникають непереборні перешкоди для повної автоматизації: оціночні поняття («значна шкода», «розумний строк», «добросовісність»), конкуруючі кваліфікації та нестандартні фактичні ситуації вимагають суддівської інтерпретації, що виходить за межі будь-якого кінцевого переліку правил [40].

Вибір та тлумачення норми права є ще більш очевидно «людською» діяльністю, оскільки передбачає звернення до цілей законодавця, системного контексту норми, конституційних цінностей та принципів права. К. Ендікот переконливо показує, що жодна норма не є «самоінтерпретуючою» — між текстом норми та рішенням у конкретній справі завжди існує герменевтичний розрив, подолання якого є прерогативою людського судження [28].

Нарешті, прийняття рішення по справі поєднує юридично-технічні й морально-аксіологічні судження: суддя враховує не лише законодавчо встановлені критерії, а й принципи справедливості, пропорційності та гуманізму, що формуються у процесі живого осмислення конкретної ситуації [61].

З огляду на викладене, межі автоматизації судових рішень визначаються такими критеріями. По-перше, критерій стандартизованості: чим більш стандартизованим та передбачуваним є зміст рішення, тим вищим є потенціал його автоматизації. По-друге,

критерій оціночності: наявність у правозастосовному процесі оціночних суджень, що апелюють до моральних та аксіологічних категорій, є бар'єром для повної автоматизації. По-третє, критерій правових наслідків: що більш серйозними є правові наслідки рішення для людини (свобода, власність), то вищим є рівень правових гарантій, що вимагають участі людини-судді. По-четверте, критерій фундаментальних прав: будь-яке рішення, що суттєво зачіпає основоположні права людини, має бути прийняте людиною і підлягати відповідальності з боку людини.

Ці критерії знаходять своє нормативне відображення у ст. 22 Загального регламенту про захист даних (GDPR), яка проголошує право фізичної особи не бути суб'єктом рішення, що ґрунтується виключно на автоматизованій обробці, якщо таке рішення має для неї правові або подібні наслідки [53]. Це положення є відправним нормативним орієнтиром для визначення меж автоматизації в судовій сфері.

Розсуд суду є одним із центральних понять теорії правосуддя, що водночас є предметом численних концептуальних суперечок. Розуміння природи розсуду суду та її співвідношення з алгоритмічними методами обробки даних є ключовим для вирішення питання про допустимий ступінь технологічного впливу на судовий процес.

Фундаментальна теоретична проблема полягає в тому, що алгоритмічна обробка даних і розсуд суду діють на принципово різних епістемологічних засадах. Алгоритм оперує статистичними закономірностями: він «навчається» на основі кореляцій між ознаками справ і результатами рішень у минулому та відтворює ці кореляції у нових ситуаціях. Розсуд суду, натомість, є нормативним судженням: вона спрямована не на опис того, що «зазвичай відбувається», а на встановлення того, що «має бути» у конкретному випадку відповідно до вимог права та справедливості [49].

Це розмежування має критичне значення для розуміння того, що алгоритм може робити і чого він принципово не може.

Алгоритм здатний відтворювати минулі закономірності правозастосування, але не здатний відступати від усталених закономірностей на основі моральних міркувань, що не можуть бути виведені з минулих даних [18]. Розсуд суду, у свою чергу, є необхідним інструментом правового розвитку: саме через неї право адаптується до нових соціальних реалій і моральних розумінь, що не могли бути передбачені законодавцем.

Водночас було б теоретично некоректним заперечувати будь-яку корисність алгоритмічних систем у контексті розсуду суду. ШІ може відігравати важливу роль у структуруванні розсуду — виявленні та нагадуванні про всі релевантні правові та фактичні чинники, що мають бути взяті до уваги, перевірці внутрішньої послідовності обґрунтування рішення, виявленні потенційних протиріч з усталеною практикою [59]. Ця функція ШІ не замінює розсуд суду, а робить її більш структурованою.

Таким чином, алгоритмічна обробка даних і розсуд суду є не конкуруючими, а взаємодоповнювальними елементами правосуддя, за умови правильного розуміння їхнього функціонального призначення. Алгоритм може розширювати і структурувати інформаційну базу на якій буде ґрунтуватись розсуд суду, але не може підмінювати його зміст — нормативне судження про те, що є справедливим і правильним у конкретній справі.

Крім того, ще одним дискусійним питанням, яке широко обговорюється в наукових колах, є питання делегування застосування функцій алгоритмічних систем. Це питання поєднує в собі конституційно-правовий, процесуальний та філософський виміри.

Вирішення цієї проблеми потребує відповіді на принципове запитання: чи може правозастосовна функція, що традиційно є прерогативою людини-судді, бути законно і легітимно передана (делегована) автоматизованій системі?

Делегування повноважень є важливим конституційно-правовим інститутом, що являє собою передачу повноважень від одного суб'єкта владних повноважень іншому. Делегування повноважень не є формою остаточної їх передачі. Вони залишаються повноваженнями органу, від якого делеговані, і можуть бути повернуті або змінені [5]. Класична теорія делегування у публічному праві встановлює щонайменше три умови його правомірності: наявність правової підстави (законодавчого повноваження на делегування); персональна відповідальність делегуючого за результати здійснення делегованих повноважень; збереження можливості відкликання делегованих повноважень [60].

Перенесення цих умов на відносини між суддею та алгоритмічною системою виявляє принципові складнощі. Щодо першої умови — правової підстави — чинне законодавство більшості держав не містить прямих норм, що уповноважували б суддів делегувати правозастосовні функції алгоритмам. Відсутність законодавчого регулювання автоматично означає відсутність легітимної підстави для повного делегування. Щодо другої умови — персональної відповідальності — делегування судових функцій алгоритму створює проблему «зникнення відповідальності» (responsibility gap): якщо рішення прийняте алгоритмом, хто несе за нього юридичну і моральну відповідальність [24]?

Проблема зникнення відповідальності є однією з найбільш глибоких у теорії алгоритмічного правосуддя. Вона пов'язана із феноменом розподіленої причинності в людино-алгоритмічних системах: алгоритм виробляє рекомендацію, суддя покладається на неї, розробник програми забезпечує технічну реалізацію, замовник несе організаційну відповідальність. У цьому ланцюжку відповідальність «розмивається» між численними суб'єктами, жоден з яких не відчуває себе повноцінно відповідальним за кінцеве рішення [22, с. 10].

Правовий вимір проблеми делегування судових функцій алгоритмам пов'язаний із принципом судової незалежності. Концепція незалежності суду у її сутнісному розумінні означає, що жодна особа чи орган за межами судової влади не може впливати на зміст судового рішення [2]. Якщо ж суддя делегує вирішення справи алгоритму, розробленому приватною компанією, державним органом або міжнародною організацією, — чи не означає це «зовнішній вплив» на судове рішення, несумісний із принципом незалежності?

Це питання набуло практичного виміру у справі Loomis v. Wisconsin, де суд визнав, що використання COMPAS при призначенні покарання не порушує конституційних прав обвинуваченого, оскільки суддя не пов'язаний рекомендацією алгоритму [43]. Проте критики цього рішення вказують, що фактичний вплив алгоритмічних рекомендацій на судові рішення є значно більшим, ніж це формально визнається — ефект автоматизованих рішень забезпечує де-факто залежність суддів від алгоритмічних результатів.

Необхідно розмежувати делегування процедурних функцій та делегування нормативних функцій правозастосування. Делегування процедурних функцій — реєстрації, розподілу справ, обчислення строків, формування повісток — не порушує принципу незалежності судової влади, оскільки не зачіпає нормативного змісту рішення. Воно є законним і доцільним. Делегування нормативних функцій — оцінки доказів, кваліфікації діяння, призначення покарання — є принципово іншою ситуацією, що вимагає законодавчого регулювання та конституційно-правового обґрунтування.

Важливим орієнтиром у цьому відношенні є Висновок № 14 Консультативної ради європейських суддів, де прямо зазначається, що «використання нових технологій не повинно підміняти суддю у прийнятті рішення» [23].

Ще одним виміром проблеми делегування є питання про суб'єктність алгоритму у правозастосовному відношенні. У чинному

законодавству жодної держави алгоритмічні системи не визнаються правовими суб'єктами, здатними нести юридичну відповідальність за прийняті рішення. Це означає, що делегування правозастосовних функцій алгоритму є, так би мовити, юридично нікчемним — адже суб'єкт, якому делегуються повноваження, не є суб'єктом. Відповідальність за рішення, прийняте за участю алгоритму, завжди залишається за людиною-суддею, що є ще одним аргументом на користь збереження обов'язкового контролю з боку людини.

Деякі дослідники пропонують концепцію «часткового делегування» (partial delegation) як проміжну модель: алгоритму делегується виконання чітко структурованих процедур правозастосування (наприклад, верифікація документів, розрахунок строків позовної давності, визначення підсудності), тоді як людина зберігає контроль над значущими рішеннями [15]. Ця модель є теоретично обґрунтованою та практично прийнятною, однак її реалізація потребує чіткого законодавчого розмежування між делегованими та не делегованими функціями.

Філософсько-правовий вимір проблеми делегування пов'язаний із питанням про моральну значущість правосуддя. Якщо право є не лише системою норм, але й втіленням суспільних цінностей та морального порядку (як стверджують прихильники природно-правової традиції від Аристотеля до Дж. Фінніса), то акт правосуддя є моральним актом, що вимагає морального суб'єкта [31]. Алгоритм, позбавлений будь-якого аксіологічного виміру, не може бути суб'єктом — і, отже, не може у повному сенсі «вершити правосуддя».

Цей аргумент знаходить своє відображення у тезі про «символічну функцію» правосуддя: коли суддя-людина виносить рішення, це є актом суспільного визнання, морального обговорення та колективного засудження чи виправдання, що має значення, яке не зводиться до технічного вирішення правового спору. Заміна

людини алгоритмом позбавляє правосуддя цього символічного виміру, перетворюючи його на суто функціональний механізм розподілу правових наслідків — і тим самим руйнуючи один із фундаментальних компонентів легітимності права [27].

Таким чином, проблема делегування правозастосовних функцій алгоритмам не має простого вирішення. Воно є законним і доцільним у процедурно-технічних аспектах правосуддя, проте принципово неприйнятним у тих сферах, де правозастосування передбачає нормативне судження, моральну оцінку та персональну відповідальність. Ця диференціація є теоретичним фундаментом для побудови правової концепції «людина в контурі» (human-in-the-loop), яка буде детально розглянута у шостому розділі монографії.

2. Публічний інтерес у запровадженні штучного інтелекту в систему правосуддя

Категорія публічного інтересу посідає особливе місце у системі правових цінностей, виступаючи водночас підставою для обмеження приватних прав та орієнтиром для визначення напрямів розвитку правових інститутів. Щодо застосування штучного інтелекту у правосудді публічний інтерес виявляє себе передусім через три взаємопов'язані переваги: ефективність, швидкість та доступність правосуддя. Ці переваги не є простими адміністративними показниками — вони є конституційно значущими вимогами, що відображають суспільний запит на дієве правосуддя як умову соціальної злагоди та законності.

Поняття публічного інтересу в теорії права не має однозначного визначення, що зумовлено його поліфункціональним характером. У широкому значенні публічний інтерес розуміється як сукупність суспільно значущих потреб і цілей, реалізація яких є умовою нормального функціонування суспільства та держави [7, с. 152]. У вузькому — як легально визнаний і нормативно закріплений суспільний

інтерес, що підлягає захисту з боку держави і може слугувати підставою для втручання в приватну сферу. Застосування ШІ у правосудді може бути виправдане публічним інтересом лише тоді, коли воно реально сприяє реалізації суспільних інтересів — і насамперед забезпеченню ефективного, своєчасного та доступного правосуддя.

Ефективність правосуддя є багатовимірною категорією, що охоплює як інституційно-процесуальний, так і результативний аспекти. З точки зору процесуального права — ефективність означає здатність судової системи вирішувати правові конфлікти з мінімальними витратами ресурсів — часових, фінансових, організаційних — при збереженні якості рішень [13]. З точки зору матеріального права — здатність судового рішення реально відновлювати порушені права, захищати законні інтереси та забезпечувати дотримання правопорядку. Ці два виміри не тотожні: рішення, прийняте ефективно з процесуального погляду, може бути неефективним з погляду відновлення справедливості, і навпаки.

Штучний інтелект пропонує реальні інструменти підвищення ефективності правосуддя. Автоматизована обробка рутинних процедур — реєстрація позовних заяв, розподіл справ, формування повісток, обчислення процесуальних строків — дозволяє суттєво скорочувати адміністративне навантаження на суддів і звільняти їх для виконання власне правосудної функції.

Швидкість правосуддя є конституційно значущою вимогою, що отримала нормативне закріплення у численних міжнародно-правових документах. Вимога «розумного строку» у ст. 6(1) ЄКПЛ, що тлумачиться Страсбурзьким судом через критерії складності справи, поведінки сторін і судових органів та значення справи для заявника [32], є нормативним вираженням принципу своєчасного правосуддя.

Практика Європейського суду з прав людини свідчить про системний характер проблеми порушення розумного строку

у багатьох державах. Зокрема, Україна є одним із лідерів за кількістю рішень ЄСПЛ проти неї у справах про порушення ст. 6 ЄКПЛ у зв'язку з надмірною тривалістю судового розгляду [10]. Ця ситуація є не лише правовою, а й соціальною проблемою, що підриває довіру суспільства до правосуддя.

Алгоритмічні системи здатні суттєво прискорювати окремі стадії судового процесу. Системи автоматизованого аналізу документів (document review AI), що застосовуються у рамках відкриття провадження у цивільних справах, скорочують час опрацювання великих масивів доказів з місяців до днів. Системи автоматичної транскрипції судових засідань усувають потребу у ручному веденні протоколів, що суттєво прискорює підготовку матеріалів справи до апеляційного перегляду. Системи онлайн-вирішення спорів (ODR) у справах про незначні цивільні вимоги дозволяють вирішувати конфлікти у кілька разів швидше, ніж традиційні судові процедури [4].

Доступність правосуддя є третьою перевагою, що виправдовує застосування ШІ в судовій системі. Право на доступ до суду є невідємним компонентом права на справедливий суд. Однак реальна доступність правосуддя визначається не лише формальним правом на звернення до суду, а й фактичними умовами його реалізації — фінансовими, географічними, інформаційними та мовними.

Фінансова доступність правосуддя є гострою проблемою у більшості держав. Фінансова та фактична доступність правосуддя залишається серйозною проблемою у багатьох правових системах. Дослідження Legal Needs Survey 2023, проведене Legal Services Board та Law Society у Великій Британії, засвідчило, що близько 66 % дорослого населення Англії та Уельсу протягом останніх чотирьох років стикалися принаймні з однією правовою проблемою, однак значна частина громадян не отримує професійної юридичної допомоги. Зокрема, 38 % осіб, які мали правову проблему, не зверталися по жодну юридичну допомогу,

а приблизно 32 % респондентів повідомили про незадоволені правові потреби, що свідчить про наявність системних бар'єрів доступу до правової підтримки. Такі дані підтверджують, що значна кількість громадян змушена вирішувати правові питання без професійного супроводу, що негативно впливає на ефективність реалізації права на судовий захист [41]. ШІ-інструменти правової допомоги, такі як DoNotPay, Rocket Lawyer та низка некомерційних платформ, здатні демократизувати доступ до базових правових послуг, надаючи автоматизовані консультації та допомагаючи у підготовці процесуальних документів.

Географічна доступність є особливо актуальною проблемою для України з її великою територією та нерівномірним розміщенням судової інфраструктури. Судова реформа 2017 року, що передбачала укрупнення судів та зміну підсудності, створила ситуацію, коли мешканці багатьох сільських районів змушені долати значні відстані для участі у судовому засіданні. Системи відеоконференц-зв'язку та повноцінного онлайн-судочинства (e-court) є технологічним рішенням цієї проблеми, що набуло особливого значення в умовах воєнного стану.

Інформаційна доступність правосуддя пов'язана із здатністю учасників судового процесу орієнтуватися у правовій системі та розуміти свої права і можливості. ШІ-системи у форматі «правових чат-ботів» здатні надавати громадянам зрозумілу правову інформацію, роз'яснювати процесуальні права, допомагати в заповненні судових форм і тим самим суттєво знижувати «правову безграмотність» як бар'єр доступу до правосуддя.

Варто підкреслити, що ефективність, швидкість та доступність правосуддя, попри їхню очевидну значущість як публічних цінностей, не є абсолютними критеріями, що виправдовують будь-яке технологічне втручання. Вони мають розглядатися у нерозривному зв'язку з якістю та справедливістю правосуддя: «швидке

несправедливе рішення» не відповідає публічному інтересу більше, ніж «повільне справедливе» [64, с. 21].

На основі вищезазначеного можемо зазначити, що використання штучного інтелекту в правосудді є одним із найбільш перспективних інструментів реалізації публічного інтересу в ефективному, доступному та єдиному судочинстві. Публічний інтерес у цій сфері має конкретний конституційно-правовий зміст: він виражається у суспільній потребі в судовій системі, що здатна своєчасно вирішувати правові конфлікти, забезпечувати рівний доступ до правосуддя незалежно від соціального статусу та місцезнаходження особи, а також гарантувати послідовність і передбачуваність правозастосування як умову правової визначеності. Саме у цих вимірах ШІ демонструє найбільш очевидний і документально підтверджений потенціал. Автоматизація рутинних організаційних процедур — розподілу справ, обчислення строків, опрацювання документів — звільняє людський ресурс для виконання власне функції правосуддя та скорочує строки розгляду справ, що безпосередньо корелює з вимогою «розумного строку» у ст. 6(1) Конвенції про захист прав людини і основоположних свобод. Системи правового пошуку та аналізу судової практики на основі ШІ суттєво знижують фінансові витрати правосуддя і демократизують доступ до правової інформації, яка раніше була доступна переважно великим юридичним фірмам із значними ресурсами. У такий спосіб технологія стає інструментом подолання структурної нерівності у доступі до правосуддя, що є однією з ключових складових публічного інтересу в правовій державі.

Не менш значущим є внесок штучного інтелекту у забезпечення єдності судової практики як публічної цінності, що безпосередньо пов'язана з принципами правової визначеності та рівності перед законом. Алгоритмічні системи моніторингу судових рішень здатні в режимі реального часу виявляти розбіжності у правозастосуванні,

що дозволяє вищим судовим інстанціям оперативно реагувати на «кризи» практики шляхом формування обов'язкових правових позицій. Це є критично важливим для суспільств із великою кількістю судів і суддів, де забезпечення послідовності правозастосування традиційними методами є об'єктивно неможливим. Водночас системи підтримки прийняття рішень здатні структурувати розсуд суду, нагадуючи про всі релевантні правові та фактичні чинники і тим самим підвищуючи якість обґрунтування судових рішень. Публічний інтерес, таким чином, реалізується через ШІ не всупереч, а завдяки збереженню розсуду людини в центрі правосудного процесу: технологія посилює інституційну спроможність судової системи служити суспільству, не підміняючи нормативний зміст правосуддя статистичними розрахунками.

3. Приватний інтерес в умовах запровадження використання штучного інтелекту в правосудді

Приватний інтерес у впровадженні штучного інтелекту в судову систему є не менш реальним і обґрунтованим, ніж публічний, хоча у науковій літературі він значно рідше розглядається саме у позитивному ключі — переважно через домінування дискурсу ризиків над дискурсом можливостей. Між тим конкретна особа, що звертається до суду за захистом своїх прав, має цілком визначений приватний інтерес у тому, щоб судовий процес був швидким, доступним, передбачуваним і вільним від суб'єктивних упереджень судді. Саме у цих вимірах ШІ здатен забезпечити приватний інтерес. Алгоритмічні системи правового пошуку та аналізу судової практики суттєво знижують інформаційну асиметрію між особою та судовою системою: громадянин, що не має можливості найняти дорогого адвоката, отримує доступ до інструментів, які дозволяють йому самостійно орієнтуватися у правовому полі, розуміти свої процесуальні права, готувати процесуальні документи

та прогнозувати можливі результати справи. Це є прямою реалізацією приватного інтересу в рівному доступі до правосуддя, що традиційно залишається привілеєм тих, хто може дозволити собі кваліфіковане юридичне представництво.

Окремим і надзвичайно значущим виміром приватного інтересу у впровадженні ШІ є інтерес особи у захисті від суддівського свавілля та невиправданої непослідовності правозастосування. Емпіричні дослідження переконливо документують феномен «невиправданого розходження» у судових рішеннях: два судді, що розглядають ідентичні справи, нерідко приходять до кардинально різних висновків — під впливом особистих переконань, стресу, втоми або підсвідомих упереджень [45]. Для конкретної особи, доля якої залежить від того, якому судді випадково була розподілена її справа, така непослідовність є реальним порушенням права на рівне ставлення з боку закону. Алгоритмічні системи підтримки прийняття рішень, що структурують розсуд суду і нагадують про релевантні прецеденти та правові позиції вищих судів, здатні суттєво знижувати цю непослідовність — і тим самим реалізовувати приватний інтерес кожної особи в тому, щоб результат її справи визначався в рамках закону, а не упередженістю судді. У такий спосіб ШІ стає інструментом забезпечення не лише публічного, але й приватного інтересу — за умови, що його впровадження здійснюється з дотриманням усіх необхідних правових гарантій.

Визнання як публічного, так і приватного інтересу у впровадженні штучного інтелекту в судову систему не знімає, а навпаки загострює фундаментальне питання про те, яким має бути концептуальний орієнтир, що визначає допустимі межі та напрями цього впровадження. Відповіддю правової думки на цей виклик стала концепція людиноцентричного підходу — підходу, що відмовляється розглядати технологію як самодостатню цінність і наполягає на тому, що будь-яка цифрова трансформація правосуддя повинна

оцінюватися насамперед за критерієм її відповідності потребам, гідності та правам людини як центрального суб'єкта правовідносин. Цей підхід є не романтичним антитехнологічним імпульсом, а цілком раціональною нормативною позицією, що спирається на систему конституційних цінностей і міжнародно-правових стандартів: принцип людської гідності, закріплений у ст. 1 Хартії основних прав ЄС та преамбулі Загальної декларації прав людини, є тим нормативним фундаментом, на якому будується вся архітектура правових обмежень алгоритмічного правосуддя. Людиноцентричний підхід виходить із того, що жодна особа не може бути зведена до сукупності цифрових показників або статистичного профілю — вона завжди залишається унікальним суб'єктом, що потребує індивідуалізованого правового ставлення, і саме ця невідчужувана індивідуальність є тим, що алгоритм за своєю природою не здатен повноцінно врахувати.

Людиноцентричний підхід у сфері штучного інтелекту загалом отримав потужне нормативне закріплення на міжнародному рівні протягом останнього десятиліття. Рекомендація ЮНЕСКО щодо етики штучного інтелекту 2021 року проголошує людиноцентричність одним із чотирьох основоположних принципів розвитку ШІ, наголошуючи, що системи ШІ мають розроблятися і застосовуватися таким чином, щоб посилювати, а не підміняти автономію людини та здатність до самовизначення. Керівні принципи ЄС з етики надійного штучного інтелекту, розроблені Групою експертів з питань ШІ у 2019 році, формулюють вимогу «людського нагляду та контролю» як одну з семи ключових умов надійності ШІ-систем, що передбачає збереження за людиною реальної, а не формальної можливості втручатися у функціонування алгоритму, коригувати його результати та скасовувати його рішення [29]. У сфері правосуддя ці загальні принципи набувають особливої нормативної ваги: Етична хартія CEPEJ з використання штучного

інтелекту в судових системах 2018 року прямо встановлює, що технологічні інструменти мають бути підпорядковані меті служіння правосуддю, а не навпаки, і що суддя завжди повинен зберігати повний контроль над процесом прийняття рішення [30]. Перенесення людиноцентричного підходу у площину конкретних правових вимог до судових ШІ-систем означає, що критерієм оцінки будь-якого алгоритмічного застосування у правосудді є не його технічна досконалість або економічна ефективність, а його здатність розширювати можливості людини — судді, сторін, суспільства в цілому — у здійсненні справедливого правосуддя, не підміняючи судження людини машинним розрахунком [9, с. 59].

Визнання людиноцентричного підходу концептуальним орієнтиром цифровізації правосуддя неминуче породжує практичне питання про те, яким чином цей підхід співвідноситься із об'єктивною логікою технологічного розвитку, що тяжіє до розширення автономності алгоритмічних систем і мінімізації людського втручання як джерела «неефективності». Технократичний підхід до впровадження ШІ у правосуддя виходить із протилежної ціннісної передумови: він розглядає людський фактор у судочинстві передусім як джерело помилок, упереджень і непослідовності, що підлягають усуненню засобами алгоритмічної стандартизації. З технократичної перспективи суддя є «слабкою ланкою» системи — суб'єктом, що схильний до когнітивних викривлень, емоційних реакцій і підсвідомих упереджень, тоді як алгоритм є носієм «чистої» раціональності, вільної від людських вад. Ця позиція має певне емпіричне підґрунтя — дослідження суддівської поведінки справді фіксують феномени «втоми від рішень», ситуативних упереджень та невиправданої непослідовності, — однак вона ґрунтується на глибокому методологічному редукціонізмі: вона зводить правосуддя до функції обробки інформації, ігноруючи його нормативний, моральний і символічний виміри, що

принципово не піддаються алгоритмізації. Технократичний підхід, доведений до логічного завершення, веде до повної автоматизації судочинства — результату, несумісного із конституційними гарантіями права на справедливий суд та принципом гідності людини.

Баланс між людиноцентризмом і технократизмом у використанні ШІ у правосудді не може бути досягнутий через просте «усереднення» двох крайніх позицій — він вимагає принципово іншої концептуальної рамки, що визначає функціональний розподіл між людиною і алгоритмом на основі нормативних, а не суто технічних критеріїв. Такою методологічною рамкою виступає концепція комплементарності (від лат. complementum — доповнення) людського судження та алгоритмічної обробки інформації. В її основі лежить розуміння того, що людина і алгоритм у процесі здійснення правосуддя виконують різні за природою, але взаємодоповнювальні функції. Алгоритмічні системи здатні забезпечувати швидку обробку значних обсягів даних, виявлення закономірностей та аналітичну підтримку прийняття рішень, тоді як суддя здійснює нормативну інтерпретацію права, оцінку фактичних обставин справи та морально-ціннісне зважування наслідків рішення. У такій моделі жоден із цих елементів не розглядається як субститут іншого: алгоритм виступає інструментом підтримки правозастосування, тоді як остаточне рішення та відповідальність за нього залишаються за людиною. Саме поєднання технологічної аналітики та людського правового судження створює передумови для більш обґрунтованого, послідовного та справедливого здійснення правосуддя. Алгоритм є незамінним у тому, що стосується масштабної обробки інформації, виявлення статистичних закономірностей, забезпечення послідовності стандартизованих процедур і структурування доказової бази — тобто у тих операціях, де «більше інформації» і «більше послідовності» є безумовними перевагами. Людина-суддя є незамінною у тому, що стосується індивідуалізованої оцінки обставин

справи, тлумачення оціночних понять та вирішення моральних дилем — тобто у тих операціях, де «правильна відповідь» визначається не статистичною закономірністю, а правовими цінностями та принципами справедливості. Судовий розгляд майже ніколи не зводиться до механічного застосування правила до встановлених обставин. Значна частина правових норм сформульована через оціночні поняття — «розумність», «добросовісність», «справедливість», «пропорційність», «значна шкода», «суспільний інтерес». Такі категорії навмисно залишаються відкритими, оскільки неможливо передбачити всі можливі життєві ситуації. Саме тому остаточне наповнення цих понять змістом відбувається у процесі судового тлумачення, де суддя враховує особливість кожної справи, співвідносить норму з її метою та зважує інтереси сторін.

Ця діяльність за своєю природою є інтерпретаційною та аксіологічною. Суддя не просто констатує факти, а здійснює їх правову кваліфікацію, визначаючи, яке значення мають певні обставини у світлі принципів права. Вирішення справи часто передбачає балансування між конкуруючими правами чи інтересами: наприклад, між свободою вираження поглядів і правом на повагу до честі та гідності, між захистом приватності і суспільним інтересом у розкритті інформації, між економічною свободою і захистом прав споживача. Такі конфлікти не можуть бути розв'язані лише шляхом статистичного аналізу попередніх рішень або виявлення найбільш ймовірного результату. Вони вимагають нормативного зважування, у якому визначальну роль відіграють правові цінності, принципи справедливості та уявлення про пропорційність втручання у права особи.

Крім того, судове рішення часто пов'язане з оцінкою індивідуальних життєвих обставин, які не піддаються повній формалізації. Суддя оцінює поведінку сторін, їх наміри, ступінь вини, щирість пояснень, соціальні та моральні наслідки рішення. У таких

ситуаціях значення має не лише фактична інформація, а й здатність до правового розсуду, емпатії та розуміння поведінки людини. Саме ці елементи формують те, що у теорії права називають розсуд суду, в межах якого суддя обирає найбільш обґрунтоване рішення серед кількох юридично допустимих варіантів.

Особливо важливою ця роль стає у ситуаціях, де постають моральні дилеми або складні питання справедливості. Право не існує у вакуумі: воно функціонує в соціальному середовищі та взаємодіє з моральними уявленнями суспільства. Суддя змушений враховувати не лише букву закону, а й його цілі, загальні принципи правової системи та наслідки рішення для конкретної людини і для правопорядку загалом. Відтак, судове рішення є результатом практичного розуму, а не лише формальної логіки.

Розвиток алгоритмічних технологій у сфері правосуддя зумовлює необхідність формування комплексної системи етичних та правових стандартів, покликаних забезпечити баланс між ефективністю цифрових інструментів та фундаментальними принципами верховенства права. Використання штучного інтелекту у судових системах відкриває значні можливості для підвищення швидкості обробки інформації, аналізу судової практики та оптимізації адміністративних процедур, однак водночас породжує низку ризиків, пов'язаних із прозорістю алгоритмів, потенційною дискримінацією, відповідальністю за автоматизовані рішення та збереженням незалежності суддів. Саме тому міжнародні організації та наукова спільнота дедалі активніше формують нормативні орієнтири, які визначають межі допустимого застосування алгоритмічних систем у правосудді.

Одним із ключових документів у цій сфері є Європейська етична хартія щодо використання штучного інтелекту в судових системах, ухвалена Європейською комісією з питань ефективності правосуддя (CEPEJ) у 2018 році. У цьому документі сформульовано

п'ять базових принципів використання штучного інтелекту у судових системах: повага до основних прав людини, недискримінація, якість та безпека алгоритмічних систем, прозорість і пояснюваність алгоритмів, а також принцип контролю з боку людини, відповідно до якого остаточне рішення повинно залишатися за суддею [30].

Схожі підходи відображені й у документах Європейського Союзу. Зокрема, Регламент ЄС про штучний інтелект запроваджує ризик-орієнтовану модель регулювання алгоритмічних систем, відповідно до якої технології, що використовуються у сфері правосуддя, віднесені до категорії високого ризику. Це означає, що такі системи підлягають суворим вимогам щодо прозорості, якості даних, аудиту алгоритмів і людського контролю. Відповідно до положень цього регламенту, використання ШІ у правозастосуванні повинно супроводжуватися механізмами пояснюваності та можливістю оскарження автоматизованих рішень, що забезпечує захист права на справедливий суд і процесуальні гарантії сторін.

Важливим орієнтиром для формування етичних стандартів алгоритмічного правосуддя є також міжнародні рекомендації щодо відповідального використання штучного інтелекту. Так, Рекомендація Ради Організації економічного співробітництва та розвитку щодо штучного інтелекту, визначає принципи надійного та людиноцентричного використання алгоритмічних систем. Серед них особливе значення мають принципи прозорості, підзвітності, безпеки та поваги до прав людини, які повинні бути інтегровані на всіх етапах життєвого циклу алгоритмічних технологій.

Формування правових стандартів використання штучного інтелекту у правосудді також пов'язане з проблемою автоматизованого прийняття рішень та меж алгоритмічної автономії. У цьому контексті значну роль відіграють положення статті 22 Загального регламенту ЄС про захист даних (GDPR), яка встановлює право особи не піддаватися рішенню, що ґрунтується виключно

на автоматизованій обробці даних і має суттєві юридичні наслідки. Ця норма фактично закріплює принцип людського контролю над алгоритмічними рішеннями та підкреслює необхідність забезпечення можливості перегляду таких рішень людиною.

У науковій літературі підкреслюється, що алгоритмічне правосуддя повинно будуватися на поєднанні технологічної ефективності та гуманістичних засад правової системи. Як зазначає Річард Саскінд, цифрова трансформація судових систем не означає повної автоматизації правосуддя, а передбачає створення нових моделей взаємодії між технологіями та людиною. За його словами, головним завданням сучасної судової реформи є формування системи «онлайн суд», у якій цифрові інструменти підвищують доступність правосуддя, не порушуючи фундаментальних процесуальних гарантій [57].

На сьогоднішній день, особливого значення набуває визначення напрямів розвитку нормативного регулювання використання штучного інтелекту у правосудді. По-перше, доцільним є формування чіткої класифікації алгоритмічних систем залежно від рівня їхнього впливу на процес прийняття судових рішень. На нашу думку, тут доречним є виокремити три функціональні категорії таких систем. Перша категорія охоплює адміністративні алгоритмічні системи, які використовуються для організаційного забезпечення діяльності судів і не мають впливу на зміст правозастосування. До цієї групи належать технології автоматичного розподілу справ між суддями, системи електронного документообігу, інструменти управління судовими календарями, а також програмні засоби, що оптимізують обробку процесуальних документів. Їх використання спрямоване передусім на підвищення ефективності судового адміністрування та скорочення процедурних витрат часу, а тому вони можуть підлягати відносно гнучкому правовому регулюванню, за умови дотримання вимог прозорості та інформаційної безпеки. Друга категорія включає аналітичні або допоміжні алгоритмічні системи,

що використовуються як інструменти підтримки суддівського рішення. Йдеться про системи аналізу судової практики, прогнозування ймовірних результатів розгляду справи, автоматизованого пошуку правових норм та формування рекомендацій щодо можливих варіантів правозастосування. Такі технології можуть значно підвищувати якість правового аналізу, дозволяючи судді працювати з великими масивами юридичної інформації та виявляти закономірності судової практики. Водночас їх використання не повинно набувати характеру обов'язкових або директивних рекомендацій, оскільки це може створити ризик непрямого впливу алгоритму на зміст судового рішення. Саме тому нормативне регулювання цієї категорії систем має передбачати обов'язкову прозорість алгоритмів, перевірку якості даних, на яких вони навчаються, а також чітке закріплення принципу, відповідно до якого рекомендації алгоритмічних систем не мають обов'язкової сили для судді. Третю категорію становлять алгоритмічні системи, що потенційно впливають на формування судового рішення або процес оцінки доказів. До цієї групи можуть належати системи оцінювання ризиків, інструменти автоматизованого визначення санкцій або алгоритмічні моделі, які формують висновки щодо правової кваліфікації певних дій. Саме такі системи становлять найбільший виклик для правової системи, оскільки їх використання може впливати на реалізацію фундаментальних принципів правосуддя, зокрема незалежності судді, змагальності процесу та права особи на справедливий суд.

Запропонована класифікація дозволяє сформувати диференційований підхід до правового регулювання алгоритмічних технологій у правосудді. Вона забезпечує можливість поєднання інноваційного потенціалу цифрових технологій із гарантіями верховенства права та справедливого судочинства, оскільки дозволяє визначити межі допустимого використання штучного інтелекту залежно від ступеня його впливу на правозастосовний процес.

По-друге, важливим напрямом є створення процедур аудиту алгоритмічних систем, що використовуються у судових органах. Такий аудит повинен включати перевірку якості навчальних даних, виявлення потенційних алгоритмічних упереджень та оцінку відповідності системи принципам недискримінації. У цьому контексті науковці наголошують на необхідності розвитку концепції «алгоритмічна підзвітність», яка передбачає можливість контролю та перевірки алгоритмічних рішень незалежними експертами [49].

По-третє, нормативне регулювання має передбачати механізми забезпечення прозорості алгоритмів та права сторін на отримання пояснення щодо використання технологічних інструментів у процесі розгляду справи. Принцип пояснюваності є ключовою умовою забезпечення довіри до алгоритмічних систем, оскільки без розуміння логіки алгоритму неможливо забезпечити ефективний судовий контроль за його використанням. У цьому контексті доцільним видається запровадження спеціального процесуального права сторін на алгоритмічне пояснення, яке передбачатиме можливість отримання інформації про характер використаної технології, джерела даних, на основі яких функціонує алгоритм, а також загальні принципи формування його рекомендацій чи висновків. Така інформація не обов'язково повинна розкривати технічні деталі програмного коду, однак вона має бути достатньою для того, щоб сторони могли зрозуміти роль алгоритмічного інструменту у процесі правозастосування та, у разі необхідності, поставити під сумнів його результати.

Крім того, перспективним напрямом є створення реєстру алгоритмічних систем, що використовуються у судовій діяльності, який міститиме інформацію про їх функціональне призначення, сферу застосування, розробника та основні характеристики. Такий реєстр сприятиме підвищенню інституційної прозорості та забезпечить публічний контроль за використанням цифрових технологій

у правосудді. Запровадження зазначених механізмів дозволить сформувати модель алгоритмічного правосуддя, у межах якої інноваційні технології інтегруються у судову систему без порушення фундаментальних гарантій справедливого судового розгляду та принципу верховенства права.

Нарешті, одним із найважливіших напрямів розвитку правового регулювання є закріплення принципу пріоритету розсуду людини у процесі правозастосування. Алгоритмічні системи можуть виступати інструментами підтримки судді, допомагаючи аналізувати великі масиви даних або формувати прогностичні моделі, однак остаточне рішення повинно залишатися за людиною. Такий підхід відповідає фундаментальним принципам верховенства права та забезпечує збереження гуманістичної природи правосуддя в умовах цифрової трансформації судових систем. Відтак, на нашу думку, доцільно нормативно закріпити принцип обов'язкового контролю з боку людини над алгоритмічними інструментами у правосудді, відповідно до якого будь-які результати роботи систем штучного інтелекту повинні розглядатися лише як допоміжні інструменти, що не мають самостійної юридичної сили. Суддя повинен мати можливість як прийняти, так і відхилити алгоритмічну рекомендацію, виходячи з оцінки конкретних обставин справи, доказів та принципів справедливості.

Крім того, доцільним є встановлення процесуального обов'язку суду фіксувати у мотивувальній частині рішення факт використання алгоритмічних інструментів, якщо такі застосовувалися під час підготовки або аналізу матеріалів справи. Така практика сприятиме підвищенню прозорості судового процесу та дозволить сторонам розуміти, яку роль відігравали технологічні інструменти у формуванні правової позиції суду. Одночасно це створить додаткові гарантії того, що алгоритмічні системи не перетворяться на прихований механізм впливу на зміст судового рішення.

Не менш важливим є й формування професійних стандартів використання цифрових технологій у судовій діяльності. У цьому зв'язку доцільно передбачити спеціальну підготовку суддів щодо принципів функціонування алгоритмічних систем, їхніх можливостей і обмежень. Розуміння логіки роботи таких технологій є необхідною передумовою для здійснення ефективного контролю з боку людини над ними та запобігання ситуаціям, коли суддя фактично покладається на алгоритмічні рекомендації без критичної оцінки їх обґрунтованості.

Отже, закріплення принципу пріоритету розсуду людини має супроводжуватися створенням комплексної системи гарантій, що включає обов'язковий контроль з боку людини над алгоритмами, прозорість використання технологічних інструментів у судовому процесі та належну підготовку суддів до роботи з такими системами. Лише за таких умов штучний інтелект може інтегруватися у судову діяльність як інструмент підвищення ефективності правосуддя, не підриваючи при цьому його фундаментальної ціннісної основи.

Список використаних джерел:

1. Абзалов Д. В., Габорець О. Цифрові загрозив умовах війни: роль аналітичних технологій у їх нейтралізації. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 26 грудня 2025) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2026. С. 3–5. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/9298/1/Конф%20Інформац.-тех.pdf

2. Зозуля Є. Незалежність і відповідальність судової влади як принцип правової держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. № 18. 2025. URL: https://reicst.com.ua/pmtl/article/view/2025-18-01-09/2025-18-01-09

3. Кельман М. С., Мурашин О. Г. Загальна теорія держави і права : підруч. Київ : Кондор, 2006. С. 298.

4. Куркова К. М., Шкарупа К. В. Онлайн вирішення правових спорів: до питання розвитку концепції.

5. Організація державної влади. Офіційний сайт Конституційного суду України. URL: https://ccu.gov.ua/storinka-knygy/5-organizaciya-derzhavnoyi-vlady

6. Про судоустрій і статус суддів : Закон України від 2 червня 2016 року № 1402-VIII. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text

7. Раімов Р. І., Пасічник А. В. Особливості публічного інтересу. *Юридичний науковий електронний журнал*. 2018. № 2. С. 150–153. URL: https://lsej.org.ua/2_2018/41.pdf

8. Савчук В. С. Цифровізація цивільного судочинства: переваги та недоліки. *Юридичний науковий електронний журнал*. 2024. № 3. С. 171–175. URL: https://www.lsej.org.ua/3_2024/40.pdf

9. Ужевко А. О. Етична складова використання штучного інтелекту в судочинстві. *Правовий вимір конституційної та кримінальної юрисдикції в Україні та світі. Сьомі юридичні читання* : зб. тез доп. Всеукр. щоріч. наук.-практ. дистанц. конф. (Одеса, 19 квіт. 2024 р.) / за заг. ред. Т. В. Степанової, О. А. Чувакова ; уклад. М. О. Саракуца, О. В. Нарожна. Електрон. текст. дані (1 файл : 1,6 МБ). Одеса : Одес. нац. ун-т ім. І. І. Мечникова, 2024. С. 56–60. URL: https://dspace.onu.edu.ua/server/api/core/bitstreams/ab7c590d-c4ce-42ca-9cd1-f098fdd1a86a/content

10. Україна лідирує за порушеннями у ЄСПЛ через системну кризу правосуддя. URL: https://www.rbc.ua/rus/news/ukrayina-lidirue-porushennyami-espl-cherez-1770735767.html

11. Access to Justice and the Judiciary: Towards New European Standards of Affordability, Quality and Efficiency of Civil Adjudication. URL: https://www.academia.edu/15726264/Access_to_Justice_and_the_Judiciary_Towards_New_European_Standards_of_Affordability_Quality_and_Efficiency_of_Civil_Adjudication

12. Aletras N. et al. Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective.

PeerJ Computer Science. 2016. Vol. 2. e93. DOI: https://doi.org/10.7717/peerj-cs.93

13. Ashley K.D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge: Cambridge University Press, 2017. URL: https://iamaeg.net/files/267A598B-5C9B-4F1A-8500-BDFCB5FAF823.pdf

14. Barocas S., Hardt M., Narayanan A. Fairness and Machine Learning: Limitations and Opportunities. Cambridge: MIT Press, 2023. URL: https://fairmlbook.org

15. Bayraktaroğlu-Özçelik G., Barış Özçelik S. Use of AI-Based Technologies in International Commercial Arbitration. URL: https://ejlt.org/index.php/ejlt/article/view/814

16. Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York: Basic Books, 1973. 507 p.

17. Bench-Capon T., Sartor G. A model of legal reasoning with cases incorporating theories and values. URL: https://www.csc.liv.ac.uk/~tbc/publications/aijsartor.pdf

18. Calo R. Artificial Intelligence Policy: A Primer and Roadmap. *UC Davis Law Review*. 2017. Vol. 51. URL: https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-2_Calo.pdf

19. Castells M. The Rise of the Network Society. The Information Age: Economy, Society and Culture. Oxford: Blackwell, Vol. 1: 1996. 594 p. URL: https://deterritorialinvestigations.wordpress.com/wp-content/uploads/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

20. CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. URL: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment

21. Chalkidis I. et al. LEGAL-BERT: The Muppets straight out of Law School. Findings of EMNLP 2020. URL: https://aclanthology.org/2020.findings-emnlp.261

22. Coeckelbergh M. Moral Responsibility and the Problem of Many Hands. *AI & Society*. 2020. Vol. 35. P. 1–14.

23. Consultative Council of European Judges (CCJE). Opinion No. 14 (2011). Op. cit. Para. 39. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/rizne/Opinion_14_eng.pdf

24. Danaher J. Robots, Law and the Retribution Gap. Ethics and Information Technology. 2016. URL: https://www.researchgate.net/publication/303355500_Robots_law_and_the_retribution_gap

25. Digital Government Review: Assessing the Digital Transformation of Government. Paris: OECD Publishing, 2020. URL: https://www.oecd.org/gov/digital-government/digital-government-review.htm

26. Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013L0011

27. Dubber M.D. The Sense of Justice: Empathy in Law and Punishment. New York : NYU Press, 2006. URL: https://www.researchgate.net/publication/361560060_The_Sense_of_Justice_Empathy_in_Law_and_Punishment

28. Endicott T. Vagueness in Law. Oxford: Oxford University Press, 2000. URL: https://juristpanel.com/wp-content/uploads/2023/04/Vagueness-in-Law_compressed.pdf

29. Ethics guidelines for trustworthy AI. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

30. European Commission for the Efficiency of Justice (CEPEJ). European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

31. Finnis J. Natural Law and Natural Rights. 2nd ed. Oxford: Oxford University Press. URL: https://etica.uazuay.edu.ec/sites/etica.uazuay.edu.ec/files/public/Natural%20Law%20and%20Natural%20Rights%20%28Clarendon%20Law%29%20%28%20PDFDrive%20%29.pdf

32. Guide on Article 6 of the European Convention on Human Rights. URL: https://rm.coe.int/1680700aaf

33. Halupova L. Prospects of using artificial intelligence in legal practice. Digitalization, Metaverse, Artificial Intelligence in The Context of Human and Individual Rights Protection in Ukraine and The World : Monograph. Scientific Approbation. 2025. C. 220–240. URL: https://sciformat.ca/books/index.php/sf/catalog/view/6/6/159

34. Harcourt B.E. Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age. Chicago : University of Chicago Press, 2006. P. 336.

35. Hart H.L.A. The Concept of Law. 2nd ed. Oxford : Clarendon Press, 1994. URL: https://books-library.website/files/books-library.online-02052042Jy2T4.pdf

36. Holmes O.W. The Common Law. Boston : Little, Brown, 1881. URL: https://www.academia.edu/6105700/The_Common_Law

37. Jordan M. I., Mitchell T. M. Machine learning: Trends, perspectives, and prospects. Science. 2015. Vol. 349, No. 6245. P. 255–260.

38. Judicial Office, Her Majesty's Courts and Tribunals Service. Online Procedure Rules: Digital justice system overview. London : HMCTS, 2021. URL: https://www.gov.uk/guidance/modernising-courts-and-tribunals-benefits-of-digital-services

39. L'accès à la justice à l'épreuve du numérique. URL: http://crjfc.univ-fcomte.fr/wp-content/uploads/2020/11/Mémoire_Ouattara.pdf

40. Law and Language. URL: https://plato.stanford.edu/entries/law-language/

41. Legal Services Board. Two in three people have legal problems, but many don't get professional help (18 April 2024). URL: https://legalservicesboard.org.uk/news/two-in-three-people-have-legal-problems-but-many-dont-get-professional-help

42. LOI organique no 2019-221 du 23 mars 2019 relative au renforcement de l'organisation des juridictions.

URL: https://www.legifrance.gouv.fr/download/pdf?id=phaGIaahl7hd3j9yBC-NoYstvrbVw7vibSIX3L_C8eE=

43. Loomis v. Wisconsin, 881 N.W. 2d 749 (Wis. 2016). URL: https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690

44. Making Justice Systems More Effective and People Centred. URL: https://www.oecd.org/en/publications/making-justice-systems-more-effective-and-people-centred_e02fd90b-en.html

45. Measuring Interjudge Sentencing Disparity: Before and After the Federal Sentencing Guidelines. URL: https://www.jstor.org/stable/10.1086/467426

46. Multidisciplinary Perspectives on Artificial Intelligence and the Law. URL: https://library.oapen.org/bitstream/handle/20.500.12657/86900/978-3-031-41264-6.pdf;jsessionid=C004B18FB568890A3A9B9B2776685F61?sequence=1

47. Nilsson N. J. The Quest for Artificial Intelligence: A History of Ideas and Achievements. Cambridge : Cambridge University Press, 2010. URL: https://ai.stanford.edu/~nilsson/QAI/qai.pdf.

48. ODR у зарубіжній практиці. *Юридичний науковий електронний журнал*. 2024. № 4. URL: https://lsej.org.ua/4_2024/189.pdf#:~:text=Тобто%20ODR%20в%20системі%20судочинства%20–%20це,логічних%20методів%20та%20інструментів%2C%20які%20дозволяють%20сторо%2D

49. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge : Harvard University Press, 2015. URL: https://tetrazolelover.at.ua/Frank_Pasquale-The_Black_Box_Society-The_Secret_Al.pdf

50. Perry W.L. et al. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Santa Monica : RAND Corporation, 2013. URL: https://www.rand.org/pubs/research_reports/RR233.html

51. Pound R. Mechanical Jurisprudence. *Columbia Law Review*. 1908. Vol. 8, No. 8. URL: https://www.scribd.com/document/816775031/1108954

52. Recommendation CM/Rec(2010)12 of the Committee of Ministers to member states on judges: independence, efficiency and responsibilities. URL: https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016805afb78%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

53. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR). OJ L 119/1. Art. 22. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

54. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

55. Resolution 57/238 "Information and communication technologies for development". A/RES/57/238, 20 December 2002. URL:

56. Sourdin T. M. Justice and technological innovation. *Journal of Judicial Administration*. URL: https://www.researchgate.net/publication/346452653_Digital_Technology_and_Justice_Justice_Apps

57. Susskind R. E. Online Courts and the Future of Justice. Oxford: Oxford University Press, 2019. 368 p. URL: https://scispace.com/pdf/online-courts-and-the-future-of-justice-susskind-r-e-3c7rrhu5xm.pdf

58. Sutton R.S., Barto A.G. Reinforcement Learning: An Introduction. 2nd ed. Cambridge. URL: https://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf

59. The accuracy, fairness, and limits of predicting recidivism. URL: https://www.science.org/doi/10.1126/sciadv.aao5580

60. The sndependent review of administrative law. URL: https://assets.publishing.service.gov.uk/media/6053383dd3bf7f0454647fc4/IRAL-report.pdf

61. Von Hirsch A. Doing Justice: The Choice of Punishments. New York : Hill and Wang, 1976. URL: https://heyzine.com/flip-book/abcbcdef40.html#page/24

62. Westerman G., Bonnet D., McAfee A. Leading Digital: Turning Technology into Business Transformation. Boston : Harvard Business Review Press, 2014. P. 25–28.

63. Zhang J. Artificial Intelligence in China's Internet Courts. *SSRN Electronic Journal*. 2019. URL: https://ssrn.com/abstract=3489428

64. Zuckerman A. On Civil Procedure: Principles of Practice. 3rd ed. London : Sweet & Maxwell, 2013. P. 21.

References:

1. Abzalov, D. V., & Haborets, O. (2026). Tsyfrovi zahrozy v umovakh viiny: rol analitychnykh tekhnolohii u yikh neitralizatsii [Digital threats in wartime: the role of analytical technologies in their neutralization]. In T. V. Maherovska (Ed.), Information and analytical support of the security and defense sector of Ukraine: Proceedings of the scientific-practical conference (Lviv, December 26, 2025) (pp. 3–5). Lviv: Lviv State University of Internal Affairs. Retrieved from https://dspace.lvduvs.edu.ua/bitstream/1234567890/9298/1/Конф%20Інформац.-тех.pdf

2. Zozulia, Ye. (2025). Independence and accountability of the judiciary as a principle of the rule of law. Problems of Modern Transformations. Series: Law, Public Administration and Administration, (18). Retrieved from https://reicst.com.ua/pmtl/article/view/2025-18-01-09/2025-18-01-09

3. Kelman, M. S., & Murashyn, O. H. (2006). General theory of state and law. Kyiv: Kondor.

4. Kurkova, K. M., & Shkarupa, K. V. Online dispute resolution: on the development of the concept. Retrieved from https://lsej.org.ua/4_2024/189.pdf#:~:text=Тобто%20ODR%20в%20системі%20судочинства%20–%20це,логічних%20методів%20та%20інструментів%2C%20які%20дозволяють%20сторо%2D.

5. Constitutional Court of Ukraine. Organization of state power. Retrieved from https://ccu.gov.ua/storinka-knygy/5-organizaciya-derzhavnoyi-vlady

6. Law of Ukraine "On the Judiciary and Status of Judges" No. 1402-VIII (June 2, 2016). Retrieved from https://zakon.rada.gov.ua/laws/show/1402-19#Text

7. Raimov, R. I., & Pasichnyk, A. V. (2018). Features of public interest. *Legal Scientific Electronic Journal*, (2), 150–153. Retrieved from https://lsej.org.ua/2_2018/41.pdf

8. Savchuk, V. S. (2024). Digitalization of civil proceedings: advantages and disadvantages. *Legal Scientific Electronic Journal*, (3), 171–175. Retrieved from https://www.lsej.org.ua/3_2024/40.pdf

9. Uzhevko, A. O. (2024). Ethical aspects of artificial intelligence use in judicial proceedings. In T. V. Stepanova & O. A. Chuvakov (Eds.), Legal dimension of constitutional and criminal jurisdiction in Ukraine and the world (pp. 56–60). Odesa: Odesa National University. Retrieved from https://dspace.onu.edu.ua/server/api/core/bitstreams/ab7c590d-c4ce-42ca-9cd1-f098fdd1a86a/content

10. Ukraine leads in ECHR violations due to systemic judicial crisis. Retrieved from https://www.rbc.ua/rus/news/ukrayina-lidirue-porushennyami-espl-cherez-1770735767.html

11. Access to Justice and the Judiciary: Towards New European Standards of Affordability, Quality and Efficiency of Civil Adjudication. Retrieved from https://www.academia.edu/15726264/Access_to_Justice_and_the_Judiciary_Towards_New_European_Standards_of_Affordability_Quality_and_Efficiency_of_Civil_Adjudication

12. Aletras, N., et al. (2016). Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, 2, e93. https://doi.org/10.7717/peerj-cs.93

13. Ashley, K. D. (2017). Artificial Intelligence and Legal Analytics. Cambridge: Cambridge University Press. Retrieved from https://iamaeg.net/files/267A598B-5C9B-4F1A-8500-BDFCB5FAF823.pdf

14. Barocas, S., Hardt, M., & Narayanan, A. (2023). Fairness and Machine Learning. Cambridge: MIT Press. Retrieved from https://fairmlbook.org

15. Bayraktaroğlu-Özçelik, G., & Özçelik, S. B. Use of AI-based technologies in international commercial arbitration. Retrieved from https://ejlt.org/index.php/ejlt/article/view/814

16. Bell, D. (1973). The Coming of Post-Industrial Society. New York: Basic Books.

17. Bench-Capon, T., & Sartor, G. A model of legal reasoning with cases incorporating theories and values. Retrieved from https://www.csc.liv.ac.uk/~tbc/publications/aijsartor.pdf

18. Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. UC Davis Law Review, 51. Retrieved from https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-2_Calo.pdf

19. Castells, M. (1996). The Rise of the Network Society. Oxford: Blackwell. Retrieved from https://deterritorialinvestigations.wordpress.com/wp-content/uploads/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

20. CEPEJ. European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. Retrieved from https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment

21. Chalkidis, I., et al. (2020). LEGAL-BERT: The Muppets straight out of law school. Retrieved from https://aclanthology.org/2020.findings-emnlp.261

22. Coeckelbergh, M. (2020). Moral responsibility and the problem of many hands. *AI & Society*, 35.

23. Consultative Council of European Judges (CCJE). Opinion No. 14 (2011). Retrieved from https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/rizne/Opinion_14_eng.pdf

24. Danaher, J. (2016). Robots, law and the retribution gap. Retrieved from https://www.researchgate.net/publication/303355500_Robots_law_and_the_retribution_gap

25. OECD. (2020). Digital Government Review. Retrieved from https://www.oecd.org/gov/digital-government/digital-government-review.htm

26. Directive 2013/11/EU. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013L0011

27. Dubber, M. D. (2006). The Sense of Justice. Retrieved from https://www.researchgate.net/publication/361560060

28. Endicott, T. (2000). Vagueness in Law. Retrieved from https://juristpanel.com/wp-content/uploads/2023/04/Vagueness-in-Law_compressed.pdf

29. Ethics guidelines for trustworthy AI. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

30. CEPEJ. European Ethical Charter on AI. Retrieved from https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

31. Finnis, J. Natural Law and Natural Rights. Retrieved from https://etica.uazuay.edu.ec/sites/etica.uazuay.edu.ec/files/public/Natural%20Law%20and%20Natural%20Rights%20%28Clarendon%20Law%29%20%28%20PDFDrive%20%29.pdf

32. Guide on Article 6 of the ECHR. Retrieved from https://rm.coe.int/1680700aaf

33. Halupova, L. (2025). Prospects of using artificial intelligence in legal practice. Retrieved from https://sciformat.ca/books/index.php/sf/catalog/view/6/6/159

34. Harcourt, B. E. (2006). Against Prediction.

35. Hart, H. L. A. (1994). The Concept of Law. Retrieved from https://books-library.website/files/books-library.online-02052042Jy2T4.pdf

36. Holmes, O. W. (1881). The Common Law. Retrieved from https://www.academia.edu/6105700/The_Common_Law

37. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349.

38. HMCTS. (2021). Digital justice system overview. Retrieved from https://www.gov.uk/guidance/modernising-courts-and-tribunals-benefits-of-digital-services

39. L'accès à la justice à l'épreuve du numérique. Retrieved from http://crjfc.univ-fcomte.fr/wp-content/uploads/2020/11/Mémoire_Ouattara.pdf

40. Law and Language. Retrieved from https://plato.stanford.edu/entries/law-language/

41. Legal Services Board. (2024). Retrieved from https://legalservicesboard.org.uk/news/two-in-three-people-have-legal-problems-but-many-dont-get-professional-help

42. LOI organique no 2019-221. Retrieved from https://www.legifrance.gouv.fr/download/pdf?id=phaGIaahl7hd3j9yBC-NoYstvrbVw7vibSIX3L_C8eE=

43. Loomis v. Wisconsin, 881 N.W.2d 749 (2016). Retrieved from https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690

44. OECD. Making Justice Systems More Effective. Retrieved from https://www.oecd.org/en/publications/making-justice-systems-more-effective-and-people-centred_e02fd90b-en.html

45. Measuring interjudge sentencing disparity. Retrieved from https://www.jstor.org/stable/10.1086/467426

46. Multidisciplinary Perspectives on Artificial Intelligence and the Law. Retrieved from https://library.oapen.org/bitstream/handle/20.500.12657/86900/978-3-031-41264-6.pdf

47. Nilsson, N. J. (2010). The Quest for Artificial Intelligence. Retrieved from https://ai.stanford.edu/~nilsson/QAI/qai.pdf

48. ODR in foreign practice. Retrieved from https://lsej.org.ua/4_2024/189.pdf

49. Pasquale, F. (2015). The Black Box Society. Retrieved from https://tetrazolelover.at.ua/Frank_Pasquale-The_Black_Box_Society-The_Secret_Al.pdf

50. Perry, W. L., et al. (2013). Predictive Policing. Retrieved from https://www.rand.org/pubs/research_reports/RR233.html

51. Pound, R. (1908). Mechanical jurisprudence. Retrieved from https://www.scribd.com/document/816775031/1108954

52. Recommendation CM/Rec(2010)12. Retrieved from https://search.coe.int/cm

53. GDPR (Regulation (EU) 2016/679). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

54. Artificial Intelligence Act (EU) 2024/1689. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

55. UN Resolution 57/238.

56. Sourdin, T. Justice and technological innovation. Retrieved from https://www.researchgate.net/publication/346452653

57. Susskind, R. (2019). Online Courts and the Future of Justice. Retrieved from https://scispace.com/pdf/online-courts-and-the-future-of-justice

58. Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning. Retrieved from https://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf

59. The accuracy, fairness, and limits of predicting recidivism. Retrieved from https://www.science.org/doi/10.1126/sciadv.aao5580

60. Independent Review of Administrative Law. Retrieved from https://assets.publishing.service.gov.uk/media/6053383dd3bf7f0454647fc4/IRAL-report.pdf

61. Von Hirsch, A. (1976). Doing Justice. Retrieved from https://heyzine.com/flip-book/abcbcdef40.html

62. Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading Digital.

63. Zhang, J. (2019). Artificial intelligence in China's Internet Courts. Retrieved from https://ssrn.com/abstract=3489428

64. Zuckerman, A. (2013). On Civil Procedure.

ГУМАНІТАРНА ТА СОЦІАЛЬНА ФУНКЦІЇ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ: ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЇХ РОЗМЕЖУВАННЯ В СИСТЕМІ ПРАВА

HUMANITARIAN AND SOCIAL FUNCTIONS OF INTELLECTUAL PROPERTY LAW: THEORETICAL AND LEGAL FOUNDATIONS OF THEIR DISTINCTION WITHIN THE LEGAL SYSTEM

Mazurenko S. V.,
PhD in Law, Associate Professor,
Associate Professor of the Department
of Intellectual Property Law and Patent Justice,
National University "Odesa Law Academy",
Odesa, Ukraine

Abstract. The study is devoted to a comprehensive theoretical and legal analysis of the humanitarian and social functions of intellectual property law and to the substantiation of the conceptual foundations for their differentiation within the legal system. It is argued that in the context of digital transformation, globalization, and wartime and post-war societal challenges, intellectual property law increasingly performs not only economic but also value-oriented functions aimed at ensuring access to knowledge, protecting cultural diversity, and promoting social cohesion.

The research reveals that the humanitarian function of intellectual property law is primarily manifested in safeguarding human dignity,

supporting creativity, and ensuring access to cultural and scientific achievements, while the social function is oriented toward balancing private and public interests, facilitating equitable distribution of the results of intellectual activity, and preventing the abuse of exclusive rights. Particular attention is paid to the risks of functional overlap and the absence of clear doctrinal criteria for distinguishing these functions in contemporary legal science.

Based on the analysis of national and international legal approaches, the study proposes criteria for differentiating the humanitarian and social functions of intellectual property law, including their axiological orientation, regulatory purpose, and the scope of protected interests. It is substantiated that a clear differentiation of these functions enhances the effectiveness of legal regulation, contributes to the development of a human-centered model of intellectual property law, and ensures a more balanced interaction between innovation, societal needs, and fundamental human values.

Keywords: intellectual property law, humanitarian function, social function, functions of law, balance of private and public interests, access to knowledge, cultural diversity, human-centered approach, digital transformation, abuse of rights

1. Теоретичне розуміння функцій права у сучасній правовій доктрині

Категорія функцій права належить до фундаментальних понять загальної теорії права і водночас є одним із найбільш дискусійних концептів юридичної науки. Попри тривалу традицію дослідження цього феномену, що сягає корінням класичної юриспруденції, питання про природу, зміст і класифікацію функцій права залишається відкритим як у вітчизняній, так і в зарубіжній правовій доктрині. Це пояснюється не лише методологічною складністю проблеми, а й тим, що функції права є динамічною категорією, яка

відображає трансформацію суспільних відносин і змінює свій зміст разом із розвитком правової системи.

Класична дефініція, визначає функції права як основні напрями правового впливу, що виражають роль права у впорядкуванні суспільних відносин відповідно до завдань держави і суспільства. Ця дефініція, при всій її поширеності, зазнавала критики за надмірну прив'язаність до державної волі, що обмежувало розуміння права виключно як інструменту державного регулювання і не враховувало його самостійного соціального виміру [14, с. 16].

Більш операціональним є підхід, що розглядає функцію права як інтегральну характеристику правового впливу, в якій відображаються соціальне призначення права, його роль у суспільстві та конкретні механізми реалізації цієї ролі. У такому розумінні функція права — це не просто напрям впливу, а специфічна форма зв'зку між правом і суспільством, в якій синтезуються онтологічний, аксіологічний та інструментальний виміри правового регулювання [3]. Подібне трактування дає змогу розглядати функції права не лише крізь призму держави, а й у контексті ширших соціальних, культурних і гуманістичних цілей правового регулювання.

У сучасній західній правовій думці проблема функцій права розглядається у тісному зв'язку з теорією соціальних систем та функціоналізмом як загальносоціологічним методом. Зокрема, Н. Луман у своїй соціологічно-правовій концепції розглядає право як аутопоетичну соціальну систему, функцією якої є стабілізація нормативних очікувань у суспільстві [33]. Луманівська перспектива є принципово важливою, оскільки вона відриває категорію функцій права від нормативно-позитивістської традиції і вписує її в ширший контекст соціальної комунікації, що відкриває нові аналітичні можливості для дослідження гуманітарної та соціальної функцій права інтелектуальної власності.

Паралельно розвивається інструменталістський підхід, зокрема в американській правовій традиції, де право розглядається насамперед як засіб досягнення соціальних цілей. Р. Паунд у своїй соціологічній юриспруденції обстоював ідею про те, що право є засобом соціального контролю та інструментом балансування конкуруючих соціальних інтересів — індивідуальних, публічних і суспільних [34]. Ця концепція має безпосереднє методологічне значення для аналізу функцій права інтелектуальної власності, оскільки проблема балансу між приватним інтересом правовласника і суспільним інтересом в доступі до знань є центральною для всієї архітектури цієї галузі.

У контексті класифікації функцій права слід зазначити, що в сучасній юридичній науці не існує єдиного загальновизнаного підходу до їх систематизації. Найбільш поширеним є поділ функцій на загальносоціальні та спеціально-юридичні [18]. До загальносоціальних зазвичай відносять економічну, політичну, виховну, культурну та інформаційну функції; до спеціально-юридичних — регулятивну (у її статичному та динамічному різновидах) і охоронну. Проте такий поділ піддається критиці за його умовність: будь-яка загальносоціальна функція реалізується через спеціально-юридичні механізми, а спеціально-юридичні функції, у свою чергу, завжди несуть соціальне навантаження.

Важливим внеском у розвиток теорії функцій права є концепція М. І. Козюбри, який наполягав на необхідності розрізнення функцій права як об'єктивно існуючих напрямів його впливу та функцій права як цілепокладання, тобто тих напрямів, які свідомо визначаються законодавцем [8]. Це розрізнення має особливе значення для розуміння гуманітарної та соціальної функцій права інтелектуальної власності: вони є одночасно об'єктивно зумовленими самою природою творчої діяльності та суспільних відносин і свідомо конструйованими законодавчою та правозастосовною практикою.

Окремої уваги заслуговує ціннісний вимір функцій права. П. М. Рабінович вказує, що функції права є проявом його соціальної цінності і не можуть розглядатися у відриві від аксіологічних засад правового регулювання [18]. Цей підхід є особливо продуктивним у контексті дослідження гуманітарної функції права інтелектуальної власності, оскільки остання безпосередньо пов'язана з такими ключовими правовими цінностями, як людська гідність, свобода творчості і право на культурну ідентичність.

2. Функціональна природа права інтелектуальної власності

У зарубіжній доктрині прав інтелектуальної власності питання про функції цієї галузі набуло специфічного концептуального оформлення. Такі дослідники, як В. Ландес і Р. Познер, аналізуючи економічні функції авторського права і патентного права, вказують на те, що система інтелектуальної власності виконує подвійну функцію: з одного боку, вона стимулює виробництво інтелектуальних благ через надання виключних прав, а з іншого — забезпечує дифузію знань і культурних продуктів у суспільстві [32]. Таким чином, у самій архітектурі системи інтелектуальної власності закладено структурну напругу між приватним і суспільним інтересом, яка і є рушієм функціональної диференціації цієї галузі.

Принципово важливим є й питання про місце гуманітарної та соціальної функцій у загальній системі функцій права. Слід визнати, що ні «гуманітарна», ні «соціальна» функції не є загальновизнаними самостійними функціями права в традиційних класифікаціях. Однак у контексті сучасного розуміння права як людиноцентричного феномену дедалі більшого значення набуває концепція, відповідно до якої функція права не вичерпується регуляцією поведінки чи охороною суб'єктивних прав, а охоплює ширший спектр завдань, пов'язаних із забезпеченням розвитку людини, культурного прогресу та соціальної справедливості.

Поява категорії «гуманітарна функція права» в правовій доктрині пов'язана із загальним рухом до гуманізації права, що особливо виразно проявляється в конституційній теорії та міжнародному праві прав людини другої половини XX — початку XXI ст. ЮНЕСКО у своїх рекомендаціях неодноразово вказувала на необхідність забезпечення права кожної людини на участь у культурному житті та користування результатами наукового прогресу, що прямо кореспондує зі статтею 27 Загальної декларації прав людини 1948 року [7]. Ця норма є концептуальним місточком між правами людини, культурними правами та правом інтелектуальної власності і засвідчує, що право інтелектуальної власності з самого початку своєї міжнародно-правової кодифікації несло в собі конфлікт між правом автора та правом суспільства, між гуманітарним і соціальним вимірами інтелектуальної власності.

Отже, теоретичне розуміння функцій права у сучасній правовій доктрині характеризується переходом від вузько-нормативістських трактувань до багатовимірних концепцій, які поєднують інструментальний, ціннісний та соціологічний підходи. Саме тому, гуманітарна та соціальна функції права постають не як маргінальні чи похідні, а як самостійні й концептуально значущі виміри правового регулювання, що відображають поненційний конфлікт або протиріччя між особистісним і суспільним, між індивідуальним творцем і колективним одержувачем результатів творчої діяльності. Саме це протиріччя є методологічним ядром дослідження функцій права інтелектуальної власності.

Право інтелектуальної власності посідає особливе місце у системі сучасного права, і ця особливість зумовлена насамперед унікальною природою об'єктів, які воно регулює. На відміну від матеріальних речей, результати інтелектуальної, творчої діяльності є нематеріальними благами, що мають властивість невичерпності при використанні та здатність до одночасного використання

необмеженою кількістю осіб. Саме ця онтологічна специфіка об'єктів інтелектуальної власності визначає функціональну своєрідність відповідної галузі права, оскільки традиційні правові механізми, розроблені для регулювання відносин власності на матеріальні об'єкти, виявляються концептуально недостатніми для забезпечення адекватного балансу між інтересами творця і суспільства. Фундаментальна теоретична проблема, що лежить в основі функціональної природи права інтелектуальної власності, пов'язана з тим, що знання і результати творчості за своїми природними властивостями є суспільними благами у розумінні економічної теорії, тобто благами, виключення з користування якими є технічно складним або неможливим і споживання яких однією особою не зменшує їх доступності для інших. На цю обставину звернули увагу ще класики економічної теорії, зокрема П. Самуельсон, який сформулював концепцію суспільних благ [35]. Правова система інтелектуальної власності є, у певному сенсі, штучним інституційним механізмом, покликаним вирішити цю суперечність: шляхом надання виключних прав законодавець перетворює нематеріальне благо на штучно дефіцитний ресурс, що дозволяє його комерціалізацію та створює стимули до творчої діяльності. Проте ця конструктивна логіка породжує внутрішню функціональну напругу, яка пронизує всю систему права інтелектуальної власності.

Вільям Фішер, аналізуючи теоретичні основи авторського права, виокремлює чотири конкуруючі теоретичні підходи до обґрунтування існування системи інтелектуальної власності: утилітарний, природньо-правова, теорія особистості і теорія соціального планування [29, с. 175]. Кожен із цих підходів акцентує різні функціональні аспекти права інтелектуальної власності: утилітарний (теорія стимулювань) — суспільний добробут і стимулювання інновацій; природньо-правова (теорія Джона Локка) — природне право творця на результати своєї праці; теорія особистості (теорія

Гегеля та Канта) — самовираження особистості та захист особистісного зв'язку автора з твором; теорія соціального планування — інтелектуальна власність повинна служити розвитку суспільства та культури. Ця теоретична поліфонія є безпосереднім відображенням функціональної багатовимірності права інтелектуальної власності. Локіанська природньо-правова теорія, адаптована до сфери інтелектуальної діяльності, обґрунтовує природне право творця на результати своєї розумової праці. Дж. Локк стверджував, що кожна людина є власником своєї особи і своєї праці, а тому результати праці також належать їй [31, с. 27]. У застосуванні до сфери права інтелектуальної власності ця теорія обґрунтовує передусім гуманітарну функцію відповідного права: захист творця як особистості, що вклала свою інтелектуальну енергію та творчий потенціал у створення твору чи винаходу. Водночас сам Локк застерігав, що привласнення є правомірним лише за умови збереження достатньої кількості ресурсу для інших — т. зв. «локіанський провізо» (Lockean proviso), — що у сфері інтелектуальної власності трансформується у вимогу суспільного доступу до знань як умову легітимності виключних прав.

Теорія особистості, розвинена у правовій доктрині Гегеля та Й. Канта і пізніше переосмислена такими дослідниками, як М. Раддін і П. Дракос, акцентує на зв'язку між особистістю автора і результатом його творчої діяльності [27]. Ця теорія є концептуальним фундаментом гуманітарної функції права інтелектуальної власності: вона пояснює, чому особисті немайнові права автора — право на авторство, право на недоторканність твору, право на оприлюднення — є невідчужуваними і не можуть бути зведені до виключно майнових категорій. Право автора на твір є, у гегелівській перспективі, проявом зовнішньої свободи особи, матеріалізацією її волі у зовнішньому світі, і саме тому воно заслуговує на правову охорону незалежно від будь-яких економічних міркувань.

Утилітарна теорія, що домінує в англо-американській правовій традиції, обґрунтовує систему інтелектуальної власності інакше: не через природне право творця, а через суспільну корисність правового стимулювання творчої діяльності. Класична утилітарна аргументація, найбільш чітко виражена у рішенні Верховного суду США у справі Mazer v. Stein (347 U.S. 201, 1954), полягає в тому, що надання тимчасових виключних прав є «ціною», яку суспільство платить за виробництво нових творів і винаходів. Ця логіка безпосередньо формує соціальну функцію права інтелектуальної власності: система виключних прав легітимна настільки, наскільки вона реально сприяє суспільному прогресу, поширенню знань і культурному розвитку. Саме тому утилітарна традиція акцентує не лише на правах правовласника, а й на обмеженнях цих прав — строках охорони, винятках і обмеженнях, доктрині добросовісного використання.

Специфіка функціонального призначення права інтелектуальної власності виявляється також у його структурній дуальності: воно одночасно є галуззю приватного права, що захищає суб'єктивні права приватних осіб, і галуззю, що переслідує публічні інтереси. Ця дуальність знаходить відображення у конституційних засадах правового регулювання інтелектуальної власності.

В українській правовій системі дуальна природа права інтелектуальної власності отримала конституційне закріплення у статті 54 Конституції України, яка одночасно гарантує свободу творчої діяльності та захист інтелектуальної власності з одного боку, і право громадян користуватися досягненнями культури та мистецтва — з іншого [10]. Ця конституційна норма є нормативним відображенням функціональної двоїстості права інтелектуальної власності: вона закріплює як гуманітарну функцію захисту творця, так і соціальну функцію забезпечення суспільного доступу до результатів інтелектуальної, творчої діяльності.

У доктрині міжнародного права інтелектуальної власності функціональна природа цієї галузі отримала осмислення через концепцію балансу інтересів, що є стрижневою для сучасної системи міжнародно-правового регулювання. Угода ТРІПС, яка є основоположним міжнародно-правовим актом у сфері інтелектуальної власності, у своїй преамбулі визнає, що цілі охорони та дотримання прав інтелектуальної власності повинні сприяти технічним інноваціям, а також передачі та поширенню технологій на взаємовигідній основі, що забезпечує соціально-економічний добробут [22]. Таким чином, ТРІПС нормативно закріплює поєднання приватноправових механізмів охорони та суспільних інтересів у єдиній функціональній системі.

Важливим теоретичним внеском у розуміння функціональної природи права інтелектуальної власності є концепція «інформаційного феодалізму», запропонована П. Дракосом і Дж. Брейтвейтом, які критикують сучасні тенденції до розширення та посилення прав інтелектуальної власності як таких, що підривають її соціальну функцію та призводять до приватизації знань, що традиційно належали суспільному надбанню [28]. Ця критична перспектива є надзвичайно важливою для розуміння сучасних функціональних трансформацій права інтелектуальної власності: вона показує, що функціональний баланс між приватним і суспільним інтересом не є стабільним і може зміщуватися під впливом економічних і політичних чинників.

Поєднання приватноправових механізмів охорони прав автора та суспільних інтересів у праві інтелектуальної власності реалізується через низку специфічних правових інструментів. Перш за все, це обмежений строк правової охорони: на відміну від права власності на матеріальні речі, яке є безстроковим, авторські права охороняються протягом визначеного строку, після чого твори переходять до суспільного надбання. Цей інструмент є безпосереднім вираженням

соціальної функції права інтелектуальної власності: суспільство погоджується на тимчасову монополію автора в обмін на гарантоване майбутнє поповнення суспільного надбання [26].

По-друге, система обмежень і винятків із виключних прав — доктрина fair use в американському праві, концепція fair dealing у британській традиції, вільне використання у системах континентального права — є нормативним механізмом реалізації соціальної функції права інтелектуальної власності. Ці механізми забезпечують доступ суспільства до результатів інтелектуальної діяльності в освітніх, наукових, критичних та інших суспільно значущих цілях навіть без дозволу правовласника [36].

Слід також зазначити, що функціональна природа права інтелектуальної власності знаходить своє відображення у структурній диференціації галузі. Авторське право з його акцентом на особистому немайновому зв'язку автора з твором більш виразно реалізує гуманітарну функцію. Патентне право, зосереджене на стимулюванні технічних інновацій та забезпечені технологічного прогресу, більш виразно реалізує соціальну функцію. Однак у кожній із підгалузей присутні обидві функції — у різному співвідношенні та через різні правові механізми. Ця структурна диференціація функцій є одним із ключових аналітичних результатів, що дозволяє глибше зрозуміти внутрішню логіку системи права інтелектуальної власності як цілісного функціонального феномену.

3. Гуманітарна функція права інтелектуальної власності

Гуманітарна функція права інтелектуальної власності є однією з найбільш концептуально насичених і водночас найменш систематизованих у правовій доктрині категорій. Її зміст не зводиться до простого захисту суб'єктивних прав автора у їх майновому вимірі, а охоплює значно ширший спектр правових відносин, пов'язаних із визнанням творчої особистості, захистом її індивідуальності,

забезпеченням невідчужуваного зв'язку між автором і результатом його творчої діяльності. По суті, гуманітарна функція права інтелектуальної власності є правовим відображенням філософської ідеї про те, що творчість є найбільш повним виразом свободи і гідності людини і способом її самовираження, а правова система зобов'язана забезпечити умови для реалізації цієї свободи та захисту її результатів.

Правова природа особистих немайнових прав автора є предметом тривалої наукової дискусії. У континентальній правовій традиції, зокрема у французькій та німецькій доктринах, «моральні права» розглядаються як прояв загального права особи, що робить їх невідчужуваними за самою їх природою. Саме цей підхід найбільш повно відображає гуманітарну функцію права інтелектуальної власності: особисті немайнові права автора охороняються не тому, що це економічно вигідно або соціально корисно, а тому, що вони є невід'ємним атрибутом творчої особистості, яка заслуговує на повагу і захист як така.

В українському законодавстві гуманітарна функція права інтелектуальної власності знаходить нормативне втілення передусім у системі особистих немайнових прав автора, закріплених у статті 423 Цивільного кодексу України. До них належать: право на визнання людини творцем (автором, виконавцем, винахідником тощо) об'єкта права інтелектуальної власності; право перешкоджати будь-якому посяганню на право інтелектуальної власності, здатному завдати шкоди честі чи репутації творця об'єкта права інтелектуальної власності; інші особисті немайнові права інтелектуальної власності, встановлені законом. Особисті немайнові права інтелектуальної власності належать творцеві об'єкта права інтелектуальної власності. У випадках, передбачених законом, особисті немайнові права інтелектуальної власності можуть належати іншим особам. Особисті немайнові права інтелектуальної власності

не залежать від майнових прав інтелектуальної власності. Особисті немайнові права інтелектуальної власності не можуть відчужуватися (передаватися), за винятками, встановленими законом. Принципово важливою є норма частини першої статті 439 ЦК України, яка закріплює положення відповідно до якого, автор має право вимагати збереження цілісності твору, протидіяти будь-якому перекрученню, спотворенню чи іншій зміні твору, включаючи супроводження твору ілюстраціями, передмовами, післямовами, коментарями тощо без згоди автора [23]. Ця норма є прямим нормативним вираженням гуманітарної функції: вона захищає не майновий інтерес автора, а його гідність як творчої особистості.

Забезпечення охорони творчої індивідуальності автора як центральний елемент гуманітарної функції права інтелектуальної власності передбачає передусім правову охорону оригінальності як конститутивної ознаки об'єкта авторського права. Вимога оригінальності є не лише технічним критерієм охороноздатності, а й правовим визнанням унікальності творчої особистості: право охороняє твір саме тому, що він є виразом індивідуального творчого вибору автора. Суд Європейського Союзу у справі Infopaq International A/S v. Danske Dagblades Forening сформулював автономне поняття оригінальності для цілей авторського права ЄС, визначивши її як «власну інтелектуальну творчість автора», що відображає його особистість через вільні та творчі рішення. Це формулювання є надзвичайно показовим з точки зору гуманітарної функції: воно прямо пов'язує правову охорону з особистісним виміром творчості [30].

Право на недоторканність твору є, мабуть, найбільш яскравим проявом гуманітарної функції права інтелектуальної власності. Це право захищає творчий задум автора від спотворень, перекручень і змін, що можуть порушити художню або наукову цілісність твору. Французька судова практика розвинула надзвичайно широке

розуміння цього права: у справі Huston v. Turner Entertainment французький касаційний суд визнав, що колоризація чорно-білого фільму Джона Г'юстона без згоди спадкоємців режисера порушує право на цілісність твору, оскільки змінює художній задум творця [38]. Ця справа є яскравою ілюстрацією того, як гуманітарна функція права інтелектуальної власності протистоїть комерційним інтересам правовласників, захищаючи творчу індивідуальність автора навіть після його смерті.

Питання про посмертну охорону особистих немайнових прав автора є особливо значущим для розуміння гуманітарної функції права інтелектуальної власності. На відміну від майнових прав, що переходять у спадщину і в кінцевому підсумку переходять до суспільного надбання, особисті немайнові права автора в більшості правових систем є або безстроковими, або охороняються значно довше за майнові права.

Значення гуманітарної функції для розвитку культури є багатовимірним і не зводиться лише до охорони прав конкретного автора. По-перше, правова охорона творчої індивідуальності є передумовою культурного різноманіття: якщо правова система захищає унікальну творчість кожного автора від привласнення та спотворення, вона тим самим сприяє збереженню різноманіття культурних виразів у суспільстві. Це положення знайшло відображення у Конвенції ЮНЕСКО про охорону та заохочення різноманітності форм культурного самовираження 2005 року, яка визнає тісний зв'язок між правами авторів і культурним різноманіттям як суспільним благом [39].

По-друге, гуманітарна функція права інтелектуальної власності є важливим чинником формування культурної пам'яті та збереження культурної спадщини. Право на цілісність твору і право на авторство забезпечують автентичність культурних творів у часі: завдяки цим правовим механізмам суспільство отримує твори у тому вигляді, в якому вони були задумані їхніми

творцями, а не у деформованому чи адаптованому вигляді, що відповідає поточним комерційним інтересам. Відтак, гуманітарна функція права інтелектуальної власності перетинається з правом на культурну спадщину як елементом ширшого масиву культурних прав людини.

По-третє, гуманітарна функція права інтелектуальної власності має важливе значення для наукового розвитку. Захист права на авторство у науковій сфері — атрибуція наукових результатів їх дійсним авторам — є не лише питанням справедливості щодо конкретного дослідника, а й умовою нормального функціонування наукового співтовариства як такого. Академічна доброчесність, боротьба з плагіатом, правила цитування — усі ці інституційні механізми є проявом гуманітарної функції права інтелектуальної власності у науковій сфері.

Окремої уваги заслуговує питання про співвідношення гуманітарної функції права інтелектуальної власності та права на свободу творчості як фундаментального права людини. Свобода творчості, закріплена у статті 54 Конституції України та статті 10 Конвенції про захист прав людини і основоположних свобод (у її інтерпретації Європейського суду з прав людини), є не лише вихідним пунктом для виникнення прав інтелектуальної власності, а й їх постійним ціннісним орієнтиром. Право інтелектуальної власності у його гуманітарному вимірі покликане не обмежувати творчу свободу, а навпаки — забезпечувати умови для її реалізації: захищаючи результати творчості від привласнення та спотворення, правова система створює стимули для подальшої творчої діяльності та формує середовище, в якому творча особистість може реалізовувати свій потенціал [20, с. 111].

Слід також розглянути питання про обмеження гуманітарної функції права інтелектуальної власності та її взаємодію з іншими правами і цінностями. Право на недоторканність твору може

вступати у конфлікт із свободою художньої критики та пародії; право на авторство може обмежуватися у контексті анонімних або псевдонімних творів; право автора контролювати оприлюднення твору може конкурувати зі свободою слова та правом суспільства на інформацію. Ці конфлікти не є патологічними для правової системи, а навпаки — є проявом її нормального функціонування: саме через вирішення цих конфліктів право знаходить баланс між гуманітарним захистом особи-автора та іншими суспільно значущими цінностями.

Таким чином, гуманітарна функція права інтелектуальної власності є комплексним правовим феноменом, що охоплює охорону творчої індивідуальності автора, захист особистих немайнових прав та невідчужуваного зв'язку між автором і результатом його творчої діяльності, а також забезпечення умов для реалізації свободи творчості як фундаментального права людини. Її значення для розвитку культури, науки і творчості є не інструментальним, а внутрішнім: правова система охороняє творця не для того, щоб отримати якийсь суспільний результат, а тому що визнання і захист творчої особистості є самостійною правовою цінністю, що випливає з фундаментального принципу поваги до людської гідності.

4. Соціальна функція права інтелектуальної власності

Соціальна функція права інтелектуальної власності є тим виміром правового регулювання, який визначає легітимність усієї системи виключних прав у контексті суспільного інтересу. Якщо гуманітарна функція звернена передусім до творця — до його особистості, гідності та невідчужуваного зв'язку з результатом творчої діяльності, — то соціальна функція звернена до суспільства в цілому: вона обґрунтовує, чому право погоджується надати приватній особі монопольні права на нематеріальні блага і яку суспільну ціну воно готове за це заплатити. По суті, соціальна

функція права інтелектуальної власності є правовою відповіддю на питання про те, як узгодити приватний інтерес правовласника із суспільною потребою у вільному доступі до знань, культури і технологій.

У вітчизняній правовій науці питання соціальної функції права інтелектуальної власності довгий час залишалося на периферії наукових досліджень, які традиційно концентрувалися на цивілістичних аспектах охорони прав авторів і правовласників. Однак із розвитком української правової доктрини в умовах євроінтеграції та формування інформаційного суспільства це питання набуває дедалі більшої актуальності. О. П. Орлюк, аналізуючи систему права інтелектуальної власності України, наголошує на тому, що право інтелектуальної власності виконує не лише охоронну функцію щодо прав творців, а й функцію регулювання суспільного обігу результатів інтелектуальної діяльності, що передбачає забезпечення доступу суспільства до цих результатів як необхідну умову інноваційного та культурного розвитку [15].

Теоретичним підґрунтям соціальної функції права інтелектуальної власності є концепція знання як суспільного блага, яка у вітчизняній доктрині розроблялася у контексті ширших досліджень інформаційного права та права інтелектуальної власності. В. С. Дмитришин, досліджуючи розпорядження майновими правами інтелектуальної власності, вказує на те, що виключні права є лише одним із механізмів регулювання відносин у сфері інтелектуальної власності, тоді як забезпечення суспільного доступу до результатів інтелектуальної діяльності є самостійним завданням правового регулювання, що не може бути зведене до похідного наслідку охорони приватних прав [5].

Роль права інтелектуальної власності у забезпеченні доступу суспільства до результатів інтелектуальної діяльності реалізується через кілька взаємопов'язаних правових механізмів, кожен

з яких є конкретним нормативним втіленням соціальної функції. Перш за все, це система обмежень і винятків із майнових прав. А. С. Штефан, досліджуючи обмеження авторського права в українській правовій системі, наголошує на тому, що система обмежень є не «виключенням із правила», а органічним елементом самої системи авторського права, що відображає її соціальну природу: право надає монополію автору не заради неї самої, а заради суспільного блага, і саме тому воно обмежує цю монополію там, де суспільний інтерес вимагає вільного доступу до твору [25]. Це твердження є принципово важливим для концептуального розуміння соціальної функції: вона є не зовнішнім обмеженням права інтелектуальної власності, а його внутрішнім елементом, закладеним у саму архітектуру системи виключних прав. Стимулювання інноваційного розвитку та технологічного прогресу є другим за значенням проявом соціальної функції права інтелектуальної власності. Науковці, досліджуючи патентну систему України, вказують на те, що патентне право виконує подвійну соціальну роль: воно стимулює винахідницьку діяльність через надання часткової монополії на використання технічного рішення, і водночас забезпечує суспільний доступ до технічних знань через систему обов'язкового розкриття інформації у патентних заявках [6]. Ця подвійна роль патентного права є класичним прикладом реалізації соціальної функції: суспільство надає винахіднику тимчасові виключні права в обмін на розкриття технічного рішення, що збагачує суспільний технологічний фонд і дозволяє подальший розвиток на основі відомого технічного рівня.

При дослідженні соціальної функції особливого значення набуває питання про доступ до знань як елемент права на освіту. На нашу думку, надмірне розширення виключних прав у сфері авторського права може призводити до обмеження права на освіту, яке є фундаментальним соціальним правом людини. Цей

зв'язок між правом інтелектуальної власності та конституційним правом на освіту є важливим свідченням того, що соціальна функція права інтелектуальної власності має конституційний вимір і не може розглядатися виключно в межах приватноправового регулювання.

Забезпечення балансу між монополією правовласника та суспільними потребами є центральною проблемою соціальної функції права інтелектуальної власності. Р. Б. Шишка, досліджуючи теоретичні засади права інтелектуальної власності в Україні, стверджує, що право інтелектуальної власності є за своєю природою соціально обтяженим правом: на відміну від права власності на матеріальні речі, право інтелектуальної власності з самого початку конструюється як право з вбудованими соціальними обмеженнями, що відображають суспільний інтерес у широкому доступі до інтелектуальних благ [24]. Це спостереження є концептуально важливим: воно показує, що соціальна функція не є зовнішнім обмеженням, накладеним на систему виключних прав ззовні, а є конституюючою характеристикою самого права інтелектуальної власності як правового інституту.

Питання про строки правової охорони є одним із найбільш наочних проявів соціальної функції права інтелектуальної власності і водночас одним із найбільш дискусійних у сучасній доктрині. О. А. Підопригора та О. О. Підопригора у своїй фундаментальній праці з права інтелектуальної власності зазначають, що строк охорони авторського права є результатом законодавчого компромісу між приватним інтересом правовласника у тривалій монополії та суспільним інтересом у якнайшвидшому переході творів до суспільного надбання [17]. Цей компроміс реалізується через встановлення строку охорони авторського права тривалістю все життя автора плюс сімдесят років після його смерті відповідно до Закону України «Про авторське право і суміжні права», що відповідає

вимогам Директиви ЄС 2006/116/ЄС про строк охорони авторського права.

Доктрина суспільного надбання є, по суті, нормативним механізмом реалізації соціальної функції права інтелектуальної власності у часовій перспективі. Коли строк охорони спливає, твір або винахід переходить до суспільного надбання і стає доступним для вільного використання будь-якою особою без будь-яких обмежень. І. І. Петренко, аналізуючи інститут суспільного надбання в українському праві, розглядає його як важливий механізм реалізації конституційного права громадян на доступ до культурних цінностей, адже саме через суспільне надбання суспільство отримує безумовний і безоплатний доступ до культурної спадщини людства [16].

Соціальна функція права інтелектуальної власності виявляється також у системі примусового ліцензування, яка є одним із найбільш дискусійних інструментів сучасного права інтелектуальної власності. Примусова ліцензія — це механізм, що дозволяє державі надати третім особам право використовувати об'єкт інтелектуальної власності без згоди правовласника, якщо суспільний інтерес вимагає такого використання. Допускається надання примусових ліцензій у випадках, коли власник патенту не використовує винахід або використовує його недостатньо, або відмовляє у видачі ліцензії на прийнятних умовах, що завдає шкоди суспільним інтересам [21, с. 147]. Інститут примусового ліцензування є одним із найбільш виразних нормативних втілень соціальної функції патентного права, оскільки він прямо підпорядковує приватне право правовласника суспільному інтересу у певних обставинах.

Питання доступу до лікарських засобів є найбільш гострим практичним проявом колізії між соціальною функцією права інтелектуальної власності та приватним інтересом правовласника. Дохійська декларація про Угоду ТРІПС і охорону здоров'я населення 2001 року, прийнята на Четвертій міністерській конференції

СОТ, підтвердила право країн — членів СОТ використовувати гнучкості ТРІПС, включаючи примусове ліцензування та паралельний імпорт, для захисту охорони здоров'я населення та забезпечення доступу до лікарських засобів [37]. В умовах пандемії COVID-19 та збройної агресії Росії проти України питання про доступ до медичних технологій і можливість примусового ліцензування патентів на лікарські засоби набуло для України особливої практичної актуальності.

Соціальна функція права інтелектуальної власності знаходить своє вираження також у системі колективного управління майновими правами, яка в Україні регулюється Законом України «Про ефективне управління майновими правами правовласників у сфері авторського права і (або) суміжних прав» від 01.12.2022 р. Цей механізм дозволяє масове використання творів на основі ліцензій, виданих організаціями колективного управління, що суттєво спрощує доступ суспільства до культурних продуктів і одночасно забезпечує справедливу винагороду правовласникам. Л. В. Кузнєцова та М. Ф. Солонько розглядають систему колективного управління як один із найбільш ефективних механізмів узгодження приватного і публічного інтересу у сфері авторського права, оскільки вона дозволяє уникнути як блокування доступу до творів через відсутність ліцензії, так і безоплатного використання, що порушує права правовласників [11, с. 129].

Важливим аспектом соціальної функції права інтелектуальної власності є його роль у забезпеченні економічного зростання та конкурентоспроможності національної економіки. Науковці переконливо вказують, що ефективна система охорони інтелектуальної власності є необхідною умовою залучення іноземних інвестицій, трансферу технологій і розвитку інноваційної економіки [2]. Ця теза набуває особливого значення в контексті повоєнної відбудови України, коли система охорони інтелектуальної власності стає

одним із ключових чинників формування привабливого інвестиційного клімату та розвитку вітчизняного інноваційного сектору.

Соціальна функція права інтелектуальної власності в сучасних умовах трансформується від простого забезпечення доступу до результатів інтелектуальної діяльності до активного стимулювання створення і дифузії інновацій як основи суспільного прогресу. Ця трансформація відображає більш широкий процес переосмислення соціальної функції права у постіндустріальному суспільстві, де знання і творчість стають основними рушіями економічного і соціального розвитку.

Таким чином, соціальна функція права інтелектуальної власності є багатовимірним правовим явищем, що охоплює забезпечення суспільного доступу до результатів інтелектуальної діяльності, стимулювання інноваційного розвитку та технологічного прогресу, підтримку культурного різноманіття та економічного зростання. Вона реалізується через систему правових механізмів — обмежень і винятків з виключних прав, примусового ліцензування, суспільного надбання, колективного управління правами, — які в сукупності утворюють нормативний каркас балансу між монополією правовласника та суспільними потребами. У вітчизняній правовій системі ці механізми набувають особливого значення в контексті євроінтеграційних зобов'язань України та необхідності формування ефективної інноваційної економіки в умовах повоєнної відбудови.

5. Співвідношення гуманітарної та соціальної функцій права інтелектуальної власності

Співвідношення гуманітарної та соціальної функцій права інтелектуальної власності є одним із найбільш складних і концептуально насичених питань теорії права інтелектуальної власності. Ці дві функції не є взаємовиключними і не перебувають у стані простого протистояння — вони утворюють діалектичну єдність,

у якій кожна з них є необхідною умовою повноцінної реалізації іншої і водночас потенційним джерелом конфлікту з нею. Розуміння цієї діалектики є ключем до розуміння внутрішньої логіки системи права інтелектуальної власності як цілісного правового феномену, що поєднує в собі захист приватної особи і служіння суспільному благу.

Вихідною теоретичною проблемою є питання про те, чи є гуманітарна та соціальна функції рівноцінними складовими системи права інтелектуальної власності, чи одна з них є первинною, а інша — похідною. У вітчизняній правовій доктрині це питання не отримало однозначної відповіді. О. П. Орлюк наголошує на тому, що система права інтелектуальної власності побудована на засадах балансу інтересів, який передбачає рівнозначність приватного інтересу творця та суспільного інтересу в доступі до результатів творчої діяльності: жоден з цих інтересів не може бути апріорно визнаний пріоритетним, оскільки саме їх рівновага є умовою нормального функціонування системи [15]. Натомість Р. Б. Шишка обстоює позицію, відповідно до якої соціальна функція є первинною у тому сенсі, що вона визначає легітимність самого існування виключних прав: система інтелектуальної власності існує не заради самої себе і не заради приватного збагачення правовласників, а заради суспільного блага, і саме тому соціальна функція є тим критерієм, відповідно до якого має оцінюватися будь-яке розширення чи звуження виключних прав [24].

Проблема узгодження інтересів автора, правовласника та суспільства є структурно складнішою, ніж може здатися на перший погляд, оскільки вона передбачає розрізнення трьох суб'єктів, інтереси яких далеко не завжди збігаються. Автор і правовласник — це нерідко різні суб'єкти: в умовах сучасної культурної індустрії та інноваційної економіки майнові права на результати інтелектуальної діяльності часто відчужуються від творців на користь видавців,

кіностудій, звукозаписних компаній, роботодавців або інвесторів. Розщеплення між автором як носієм гуманітарних інтересів і правовласником як носієм комерційних інтересів є однією з центральних суперечностей сучасного авторського права, яка суттєво ускладнює реалізацію гуманітарної функції: у системі, де майнові права повністю відчужені від автора, гуманітарна функція виявляється зведеною до охорони особистих немайнових прав, позбавлених реального економічного підкріплення.

Ця обставина породжує принципово важливий теоретичний висновок: гуманітарна та соціальна функції права інтелектуальної власності можуть конфліктувати не лише між собою, а й із комерційними інтересами правовласників, які не є авторами. У такому разі і гуманітарна, і соціальна функції виступають як спільний фронт проти надмірної комерціалізації системи інтелектуальної власності. Це спостереження є концептуально важливим: воно показує, що протистояння гуманітарного та соціального вимірів права інтелектуальної власності не є єдиним і навіть не є головним функціональним конфліктом у системі. Значно гостріший конфлікт виникає між інтересами авторів і суспільства з одного боку та інтересами великих правовласників — транснаціональних корпорацій, що контролюють культурну індустрію, — з іншого. П. Дракос і Дж. Брейтвейт описують цей процес як «захоплення» системи інтелектуальної власності корпоративними інтересами, що призводить до системного підриву як гуманітарної, так і соціальної функцій права [28].

Взаємодія особистісних та суспільних аспектів інтелектуальної власності виявляється найбільш рельєфно у питанні про межі охорони особистих немайнових прав автора. Право на недоторканність твору, будучи центральним елементом гуманітарної функції, може вступати у конфлікт із соціальною функцією у тих випадках, коли суспільний інтерес вимагає адаптації чи переробки твору.

Класичним прикладом є питання про доступність творів для осіб із порушеннями зору або слуху: адаптація твору для потреб людей з інвалідністю може технічно означати зміну форми його представлення, що формально торкається права на недоторканність. Аналізуючи це питання, доходимо висновку, що у таких випадках соціальна функція права інтелектуальної власності, яка виражається у забезпеченні доступу до творів усіх членів суспільства без дискримінації, повинна мати пріоритет над буквальним тлумаченням права на недоторканність, якщо адаптація не спотворює художнього задуму автора. Марракеський договір про полегшення доступу до опублікованих творів для осіб із порушенням зору, вадами зору або іншими труднощами сприйняття друкованої інформації 2013 року є міжнародно-правовим відображенням цього підходу і яскравим прикладом нормативного розв'язання конфлікту між гуманітарною та соціальною функціями права інтелектуальної власності на користь соціальної [13].

Конфлікти між охороною прав автора і потребами суспільства в доступі до знань найбільш гостро виявляються у сфері наукових публікацій та академічного знання. Парадоксальна ситуація сучасної академічної видавничої системи полягає в тому, що наукові дослідження, доступ до яких часто обмежується через систему платних підписок, що контролюються приватними видавничими корпораціями. Рух відкритого доступу — Open Access — є практичною відповіддю наукового співтовариства на цей конфлікт і водночас яскравим прикладом того, як соціальна функція права інтелектуальної власності може бути реалізована через добровільні інституційні механізми, а не лише через примусові правові норми.

Ще одним виміром конфлікту між гуманітарною та соціальною функціями є питання про строки охорони авторського права. О. А. Підопригора та О. О. Підопригора зазначають, що поступове

подовження строків охорони авторського права протягом XX — початку XXI ст. — від 14 років у перших авторсько-правових актах до 70 років після смерті автора у сучасних системах — є результатом успішного лобіювання інтересів великих правовласників і фактично означає відтермінування реалізації соціальної функції права інтелектуальної власності у часі [17]. Показово, що тривале подовження строків охорони відбувається всупереч інтересам самих авторів, переважна більшість творів яких утрачає комерційну цінність задовго до спливу строку охорони: основним бенефіціаром надтривалих строків охорони є не автор, а корпоративний правовласник. Таким чином, у питанні строків охорони гуманітарна та соціальна функції несподівано виявляються союзниками: обидві зацікавлені у встановленні розумних строків охорони, тоді як їх надмірне подовження відповідає лише комерційним інтересам правовласників.

Системний аналіз взаємодії гуманітарної та соціальної функцій права інтелектуальної власності дозволяє виявити кілька типових моделей їх співвідношення. Перша модель — гармонійна взаємодія — виявляється в тих випадках, коли захист творчої особистості автора одночасно слугує суспільному інтересу у розвитку культури і науки: захищаючи право автора на авторство і недоторканність твору, право забезпечує автентичність культурної спадщини та достовірність наукового знання, що є суспільним благом. Друга модель — функціональна напруга — виявляється у тих випадках, коли посилення охорони прав автора відбувається за рахунок обмеження суспільного доступу до результатів творчості, і навпаки: розширення вільного використання творів послаблює економічні стимули до творчої діяльності. Третя модель — функціональний союз проти спільного противника — виявляється у тих випадках, коли і гуманітарні, і соціальні інтереси виступають проти надмірної комерціалізації системи інтелектуальної власності

корпоративними правовласниками. Натомість, правозастосовна практика нерідко стикається з ситуаціями, коли гуманітарний і соціальний виміри права інтелектуальної власності вступають у пряме протиріччя і суд змушений здійснювати ціннісний вибір між ними. Такий вибір не може бути зроблений на основі суто технічного тлумачення закону — він вимагає звернення до фундаментальних цінностей правової системи, конституційних принципів і загальних засад права інтелектуальної власності. Це свідчить про те, що питання співвідношення гуманітарної та соціальної функцій права інтелектуальної власності є не лише теоретичним, а й глибоко практичним: від його правильного вирішення залежить якість правозастосовних рішень у конкретних справах.

На нашу думку, ефективна система права інтелектуальної власності повинна забезпечувати динамічну рівновагу між гуманітарними та соціальними функціями: надмірне посилення будь-якої з них за рахунок іншої призводить до дисфункції системи в цілому. Ця ідея динамічної рівноваги є ключовою для розуміння функціональної природи права інтелектуальної власності: система не може бути статично збалансованою, оскільки суспільні відносини постійно змінюються, а разом із ними змінюється і оптимальне співвідношення між гуманітарними та соціальними пріоритетами правового регулювання.

Особливо гострими стають конфлікти між гуманітарною та соціальною функціями права інтелектуальної власності в умовах цифрового середовища, де технологічні можливості необмеженого копіювання і поширення творів вступають у принципове протиріччя з системою виключних прав. Цифрове середовище радикально змінює баланс між гуманітарною та соціальною функціями: з одного боку, цифрові технології надають авторам принципово нові можливості для самовираження і поширення своєї творчості, що посилює гуманітарний вимір системи; з іншого боку, легкість

копіювання і поширення цифрових творів підриває економічну основу виключних прав і ставить під сумнів їх здатність слугувати стимулом до творчої діяльності.

Принциповою теоретичною проблемою, що пронизує все питання про співвідношення гуманітарної та соціальної функцій права інтелектуальної власності, є питання про те, чи існує об'єктивний критерій оптимального балансу між ними, чи цей баланс є завжди ситуативним і залежить від конкретного контексту правового регулювання. М. І. Козюбра, розмірковуючи про принцип справедливості як засаду правового регулювання, стверджує, що пошук балансу між конкуруючими правовими інтересами є не технічним завданням, що має єдино правильне рішення, а ціннісним судженням, яке відображає конкретно-історичний рівень розвитку суспільства та його правової культури [8]. Застосований до проблеми співвідношення гуманітарної та соціальної функцій права інтелектуальної власності, цей підхід означає, що оптимальний баланс між ними не є незмінним і повинен переглядатися у відповідь на зміни технологічного, економічного та культурного контексту.

Таким чином, співвідношення гуманітарної та соціальної функцій права інтелектуальної власності є складним діалектичним феноменом, який не може бути зведений ні до простої гармонії, ні до непримиренного конфлікту між ними. Ці функції перебувають у постійній динамічній взаємодії, в якій моменти гармонії чергуються з моментами напруги, а характер їх співвідношення змінюється залежно від контексту правового регулювання, суб'єктного складу правовідносин і рівня технологічного та соціального розвитку суспільства. Ключовим завданням правової системи є не усунення цієї напруги — що є неможливим за самою природою речей, — а її продуктивне управління через систему правових механізмів, що забезпечують динамічний баланс між охороною творчої особистості і служінням суспільному благу.

6. Баланс публічного та приватного інтересу як критерій розмежування функцій права інтелектуальної власності

Категорія балансу публічного та приватного інтересу є одним із фундаментальних принципів сучасного права і водночас одним із найбільш складних для операціоналізації правових концептів. У сфері права інтелектуальної власності ця категорія набуває особливого значення, оскільки саме через неї здійснюється нормативне розмежування між гуманітарною та соціальною функціями права: перша переважно обслуговує приватний інтерес творця, друга — публічний інтерес суспільства в доступі до результатів інтелектуальної діяльності. Однак таке спрощене розмежування потребує суттєвого уточнення, оскільки і гуманітарна, і соціальна функції мають одночасно і приватний, і публічний виміри, а сам баланс між публічним і приватним інтересом є не статичною точкою рівноваги, а динамічним правовим завданням, що вирішується по-різному залежно від контексту, суб'єктного складу правовідносин і рівня суспільного розвитку.

Теоретичне осмислення співвідношення публічного та приватного інтересу у праві має глибоке філософсько-правове коріння. У вітчизняній доктрині це питання отримало ґрунтовну розробку у працях П. М. Рабіновича, який розглядає інтерес як об'єктивно зумовлену потребу суб'єкта, що набуває правового значення через її визнання і захист правовою системою [18]. Ця дефініція є важливою методологічною основою для аналізу балансу інтересів у праві інтелектуальної власності: вона дозволяє розглядати і приватний інтерес правовласника, і публічний інтерес суспільства як об'єктивно існуючі правові феномени, що заслуговують на рівну правову увагу і потребують узгодження, а не механічного підпорядкування одного іншому.

Сучасні науковці вказують, що демократична правова держава не може ані абсолютизувати приватний інтерес, перетворюючи

право на інструмент захисту привілеїв окремих осіб, ані абсолютизувати публічний інтерес, підпорядковуючи особу суспільству і знецінюючи її індивідуальність [8]. Застосований до права інтелектуальної власності, цей підхід означає, що ані необмежена монополія правовласника, ані безумовний пріоритет суспільного доступу до результатів творчості не можуть бути визнані конституційно прийнятними: право зобов'язане знайти точку рівноваги між цими двома полюсами, яка відповідає принципам справедливості, пропорційності та поваги до людської гідності.

Публічний інтерес у сфері інновацій є одним із найбільш виразних проявів соціальної функції права інтелектуальної власності і одночасно одним із найважливіших критеріїв розмежування між публічним і приватним у системі виключних прав. Публічний інтерес в інноваціях є комплексним явищем, яке охоплює інтерес держави у підвищенні технологічного рівня національної економіки, інтерес суспільства у доступності нових технологій і продуктів, а також інтерес наступних поколінь дослідників у можливості будувати свою роботу на фундаменті вже відомих технічних рішень. Цей багатовимірний публічний інтерес і є тим критерієм, відповідно до якого правова система встановлює обмеження виключних прав у патентному праві — строки охорони, обов'язкове розкриття технічного рішення у патентній заявці, виключення наукових досліджень із сфери патентної монополії.

Публічний інтерес у сфері освіти є ще одним принципово важливим виміром соціальної функції права інтелектуальної власності, що безпосередньо визначає межі приватного інтересу правовласника. Конституційне право на освіту, закріплене у статті 53 Конституції України, є не лише декларативним положенням, а й конкретним правовим обмеженням для системи виключних прав: правовласник не може реалізовувати свої виключні права у такий спосіб, що фактично унеможливлює доступ до освіти для певних верств населення.

Ця позиція знаходить нормативне підтвердження у системі освітніх винятків із авторського права, передбачених статтею 23 Закону України «Про авторське право і суміжні права», яка допускає вільне відтворення творів у навчальних виданнях, хрестоматіях та посібниках у обсязі, виправданому навчальною метою.

Публічний інтерес у сфері культурного розвитку є третьою складовою публічного інтересу, що визначає межі приватної монополії у системі авторського права. Культурний розвиток суспільства вимагає не лише виробництва нових культурних продуктів, але й забезпечення їх широкої доступності та можливості творчого переосмислення попередніх культурних надбань. Ця ідея є фундаментальною для розуміння інституту суспільного надбання як механізму реалізації публічного інтересу у культурному розвитку: коли твори переходять до суспільного надбання, суспільство отримує можливість не лише вільно використовувати їх, але й творчо переосмислювати, адаптувати та будувати на їх основі нові культурні продукти, що є необхідною умовою живого культурного процесу.

Приватний інтерес правовласника у здійсненні виключних прав є не менш складним і багатовимірним явищем, ніж публічний інтерес. В. С. Дмитришин, досліджуючи зміст майнових прав інтелектуальної власності, виокремлює кілька складових приватного інтересу правовласника: економічний інтерес у комерційній експлуатації результатів інтелектуальної діяльності, контрольний інтерес у визначенні умов і способів використання твору чи винаходу, репутаційний інтерес у підтримці якості продуктів, що асоціюються з його іменем або торговельною маркою, а також стратегічний інтерес у формуванні конкурентних переваг на ринку [5]. Ця багатовимірність приватного інтересу є важливою для розуміння механізмів балансування: правова система повинна враховувати не лише економічний, але й інші виміри приватного інтересу при встановленні меж виключних прав.

Центральним питанням у контексті балансу публічного та приватного інтересу є питання про правові механізми його забезпечення. У сучасному праві інтелектуальної власності ці механізми утворюють розгалужену систему, кожен елемент якої є конкретним нормативним відповіддю на певний аспект конфлікту між приватним і публічним інтересом. Р. Б. Шишка систематизує ці механізми, виокремлюючи такі їх групи: темпоральні обмеження виключних прав, що забезпечують неминучий перехід результатів інтелектуальної діяльності до суспільного надбання; змістові обмеження, що виключають певні категорії результатів інтелектуальної діяльності з-під охорони; функціональні обмеження, що допускають певні види використання без дозволу правовласника; примусові механізми, що дозволяють державі забезпечити суспільний доступ до охоронюваних об'єктів всупереч волі правовласника [24].

Принцип пропорційності є ключовим правовим інструментом забезпечення балансу між публічним і приватним інтересом у праві інтелектуальної власності. Будь-яке обмеження права, включаючи права інтелектуальної власності, повинно відповідати критеріям пропорційності: воно має переслідувати законну мету, бути необхідним у демократичному суспільстві та не перевищувати меж, виправданих цією метою. Застосований до права інтелектуальної власності, принцип пропорційності означає, що обмеження виключних прав на користь публічного інтересу є виправданими настільки, наскільки вони дійсно необхідні для досягнення суспільно значущої мети і не позбавляють правовласника можливості нормально реалізовувати свої права в інших сферах.

Тристороннє тестування обмежень авторського права, закріплене у статті 9(2) Бернської конвенції і відтворене у статті 13 Угоди ТРІПС, є міжнародно-правовою операціоналізацією принципу пропорційності у сфері авторського права: обмеження виправдані лише тоді, коли вони стосуються певних спеціальних

випадків, не суперечать нормальному використанню твору і не завдають невиправданої шкоди законним інтересам автора. Аналізуючи застосування тристороннього тесту в українській правовій системі, можемо дійти висновку, що цей тест є не лише технічним критерієм допустимості обмежень, а й нормативним вираженням принципу балансу публічного та приватного інтересу, що вимагає від законодавця і правозастосувача постійного зважування між потребами суспільства і правами правовласника у кожному конкретному випадку.

В. В. Луць, досліджуючи цивільно-правові механізми реалізації права інтелектуальної власності в Україні, звертає увагу на те, що договірне право є одним із ключових механізмів реалізації балансу між публічним і приватним інтересом у системі інтелектуальної власності: ліцензійні угоди, договори про передачу майнових прав, договори у сфері колективного управління правами дозволяють сторонам самостійно встановлювати умови використання результатів інтелектуальної діяльності з урахуванням як приватних, так і публічних інтересів [12]. Особливе значення в даному випадку набувають ліцензії типу Creative Commons, які дозволяють авторам добровільно розширювати публічний доступ до своїх творів, «жертвуючи» частиною приватного контролю заради суспільного блага. Це явище є показовим прикладом того, як баланс публічного та приватного інтересу може досягатися не лише через імперативне правове регулювання, але й через диспозитивні механізми, що ґрунтуються на добровільному виборі автора.

Ефективний баланс між публічним і приватним інтересом вимагає не лише належного нормативно-правового регулювання, але й розвиненої інституційної інфраструктури: судів, що здатні здійснювати тонке зважування конкуруючих інтересів у конкретних справах; патентних відомств і організацій колективного управління, що забезпечують реалізацію як приватних прав, так і суспільного

доступу; незалежних органів регулювання, що здійснюють антимонопольний контроль у сфері інтелектуальної власності. Ця інституційна перспектива є надзвичайно важливою, оскільки вона показує, що баланс публічного та приватного інтересу є не лише нормативним, але й інституційним завданням, вирішення якого залежить від якості правових інститутів та їх здатності забезпечувати справедливе правозастосування.

Антимонопольний вимір балансу між публічним і приватним інтересом у праві інтелектуальної власності є одним із найбільш складних і дискусійних аспектів сучасного права. Система виключних прав за своєю природою надає правовласникам монопольне становище на певних ринках, що може суперечити публічному інтересу у підтримці конкуренції та ефективному функціонуванні ринків. В такому випадку, антимонопольне регулювання є необхідним коректором системи виключних прав, що запобігає перетворенню законної монополії правовласника на зловживання домінуючим становищем на ринку.

Питання балансу публічного та приватного інтересу набуває особливої актуальності в контексті євроінтеграції України та гармонізації українського права інтелектуальної власності із правом Європейського Союзу. Право ЄС у сфері інтелектуальної власності ґрунтується на принципі балансу інтересів, який відображає європейське розуміння соціальної держави і зобов'язань держави перед суспільством у забезпеченні доступу до культури, освіти і технологій. Цей процес гармонізації є важливим чинником трансформації системи права інтелектуальної власності України у напрямку більш збалансованого співвідношення між гуманітарними та соціальними функціями.

Таким чином, баланс публічного та приватного інтересу є не лише теоретичним принципом, але й практичним критерієм розмежування функцій права інтелектуальної власності, що реалізується

через розгалужену систему правових механізмів на нормативному, інституційному та правозастосовному рівнях. Цей баланс є динамічним і контекстуально зумовленим: він змінюється залежно від характеру об'єкта права інтелектуальної власності, суб'єктного складу правовідносин, суспільно значущих цілей використання та рівня технологічного і соціального розвитку суспільства. Правова система, що прагне до оптимального балансу між гуманітарною та соціальною функціями права інтелектуальної власності, повинна забезпечувати не статичну рівновагу між конкуруючими інтересами, а динамічний і справедливий процес їх узгодження, що ґрунтується на принципах пропорційності, верховенства права і поваги до людської гідності як вищої правової цінності.

7. Висновки

Проведене дослідження гуманітарної та соціальної функцій права інтелектуальної власності дозволяє сформулювати узагальнюючі висновки щодо тенденцій їх трансформації в умовах цифровізації та розвитку штучного інтелекту — тих двох технологічних мегатрендів, які у сукупності радикально змінюють саму природу творчої діяльності, умови виробництва і поширення результатів інтелектуальної діяльності, а також характер відносин між автором, правовласником і суспільством. Ці трансформації не є лише технічними змінами у способах використання охоронюваних об'єктів — вони зачіпають концептуальні основи системи права інтелектуальної власності і ставлять під сумнів адекватність правових конструкцій, що формувалися протягом кількох століть в умовах принципово відмінного технологічного і соціального контексту.

Цифровізація радикально змінила умови реалізації соціальної функції права інтелектуальної власності, перетворивши проблему доступу суспільства до результатів інтелектуальної діяльності з переважно економічної на переважно правову. В аналоговому

середовищі обмеженість тиражів, вартість відтворення і фізична прив'язаність носіїв природним чином обмежували поширення творів незалежно від правових норм. Цифрове середовище зруйнувало ці природні обмеження: технічна можливість необмеженого копіювання і миттєвого глобального поширення будь-якого твору означає, що єдиними реальними перепонами для суспільного доступу до результатів інтелектуальної діяльності є правові норми і технологічні засоби захисту авторських прав. Цей перехід породив принципово нову конфігурацію конфлікту між соціальною функцією права інтелектуальної власності та приватним інтересом правовласника: в умовах, коли технологія сама по собі забезпечує необмежений доступ, саме право стає єдиним інструментом обмеження цього доступу, що надає йому якісно нового соціального навантаження.

Крім того, цифровізація суттєво трансформувала гуманітарну функцію права інтелектуальної власності, одночасно розширивши можливості для її реалізації і створивши принципово нові загрози для неї. З одного боку, цифрові технології надали авторам безпрецедентні можливості для самовираження і самостійного поширення своєї творчості поза традиційними посередниками — видавцями, кіностудіями, звукозаписними компаніями, — що теоретично посилює гуманітарний вимір системи, наближаючи її до ідеалу безпосереднього захисту творчої особистості. З іншого боку, цифрове середовище породило масштабні загрози для права на авторство і права на недоторканність твору: легкість маніпулювання цифровим контентом, поширення deepfake-технологій, анонімність інтернет-середовища і складність атрибуції цифрових творів створюють умови, в яких гуманітарна функція права інтелектуальної власності зазнає системного тиску. Таким чином, традиційні правові механізми захисту права на авторство і права на недоторканність твору виявляються недостатньо ефективними в умовах, коли ідентифікація порушника і фіксація факту порушення є технічно складними завданнями [9].

Третім і концептуально найбільш значущим висновком є те, що розвиток технологій штучного інтелекту ставить під сумнів саму концептуальну основу гуманітарної функції права інтелектуальної власності — ідею про творчість як унікальний прояв людської особистості, що заслуговує на особливий правовий захист. Генеративні системи штучного інтелекту — такі як GPT-4, DALL-E, Midjourney, Stable Diffusion та інші — здатні продукувати результати, що формально відповідають критеріям охороноздатності творів: вони є оригінальними у тому сенсі, що не є простим копіюванням існуючих творів, і мають художню чи наукову цінність. Однак за ними не стоїть жодна творча особистість у традиційному розумінні — жодна індивідуальність людини, що прагне самовираження, жоден суб'єкт, що вклав у твір свою духовну енергію і заслуговує на захист свого зв'язку з його результатом. Генеративний штучний інтелект створює «безсуб'єктну творчість» — феномен, для якого у традиційній правовій системі немає адекватного концептуального інструментарію [1].

Навчання систем штучного інтелекту відбувається на масивах даних, що включають мільйони охоронюваних творів — текстів, зображень, музичних творів, — використання яких без дозволу правовласників є потенційно масовим порушенням виключних прав. Водночас обмеження доступу систем штучного інтелекту до охоронюваних творів може суттєво обмежити розвиток технологій, що мають величезний суспільний потенціал — від медичної діагностики до наукових досліджень. Це протиріччя є найгострішим проявом конфлікту між приватним інтересом правовласника і публічним інтересом у технологічному прогресі, з яким сучасна система права інтелектуальної власності стикається на сьогоднішній день, і вирішення якого вимагає принципового переосмислення балансу функцій права інтелектуальної власності.

Трансформація функцій права інтелектуальної власності в умовах цифровізації і штучного інтелекту відбувається у принципово

різний спосіб у різних правових системах, що породжує проблему фрагментації міжнародно-правового регулювання і послаблює ефективність глобальної системи охорони інтелектуальної власності. Право Європейського Союзу, зокрема Директива про авторське право на єдиному цифровому ринку 2019/790/ЄС [4], намагається збалансувати інтереси правовласників і користувачів в умовах цифрового середовища через запровадження нових виключень і обмежень — зокрема, виключення для text and data mining у наукових дослідженнях, — що є прямим нормативним виразом соціальної функції права інтелектуальної власності в умовах цифровізації. В Україні імплементація цієї Директиви є частиною євроінтеграційних зобов'язань, що набуває особливої актуальності в умовах підготовки до вступу в ЄС та необхідності привести національне законодавство у відповідність до стандартів цифрового єдиного ринку. Цей процес гармонізації є не лише технічним юридичним завданням, а й можливістю для України закласти у своє законодавство більш прогресивний і збалансований підхід до співвідношення гуманітарної та соціальної функцій права інтелектуальної власності в цифрову епоху.

Окремої уваги заслуговує питання про авторство творів, створених штучним інтелектом, і його наслідків для гуманітарної функції права інтелектуальної власності. Традиційна концепція авторства, що ґрунтується на ідеї творчої особистості як джерела охоронюваного твору, виявляється непридатною для творів, що генеруються системами штучного інтелекту без безпосередньої творчої участі людини. Різні правові системи обирають різні підходи до вирішення цього питання: повна відмова у правовій охороні творів штучного інтелекту, визнання автором розробника системи, визнання автором користувача, що формулює запит, або запровадження спеціального режиму охорони sui generis. На сьогоднішній день, жоден із них не є повністю задовільним з точки зору

як гуманітарної, так і соціальної функцій права інтелектуальної власності: відмова у правовій охороні усуває стимули до розвитку технологій штучного інтелекту, тоді як надання охорони без реального автора-людини позбавляє гуманітарну функцію її концептуального підґрунтя.

Цифрове середовище і штучний інтелект, з одного боку, послаблюють концептуальну основу гуманітарної функції, розмиваючи межі творчої індивідуальності і ускладнюючи ідентифікацію автора як суб'єкта правової охорони. З іншого боку, вони посилюють значення соціальної функції, збільшуючи суспільний запит на вільний доступ до результатів інтелектуальної діяльності як необхідної умови функціонування цифрової економіки і розвитку технологій штучного інтелекту. Таким чином, право перебуває у постійному процесі адаптації до нових соціальних умов і повинне знаходити нові форми рівноваги між конкуруючими цінностями, не відмовляючись від жодної з них.

Таким чином, аналіз гуманітарної та соціальної функцій права інтелектуальної власності у їх теоретичних засадах, нормативному втіленні та динаміці трансформації дозволяє сформулювати такі узагальнення. По-перше, функціональний підхід до аналізу права інтелектуальної власності є необхідним доповненням до традиційного нормативно-догматичного підходу, оскільки він дозволяє оцінювати правові норми і інститути не лише з точки зору їх формальної правильності, але й з точки зору їх реальної соціальної ефективності. По-друге, гуманітарна та соціальна функції права інтелектуальної власності є рівноцінними і взаємообумовленими складовими єдиної функціональної системи, жодна з яких не може бути принесена в жертву іншій без порушення цілісності і легітимності всієї системи. По-третє, баланс між цими функціями є динамічною правовою задачею, вирішення якої вимагає постійного діалогу між правовою доктриною, законодавством і правозастосовною

практикою в умовах технологічних і соціальних змін. По-четверте, в умовах цифровізації і розвитку штучного інтелекту цей баланс піддається безпрецедентному тиску, що вимагає від вітчизняної правової науки активної участі у формуванні нових концептуальних рамок, здатних забезпечити адекватну правову відповідь на виклики цифрової епохи. Реалізація цього завдання є одним із пріоритетних напрямків розвитку науки права інтелектуальної власності в Україні на сучасному етапі, що безпосередньо пов'язане із стратегічними цілями євроінтеграції та побудови інноваційної економіки в умовах повоєнної відбудови держави.

Список використаних джерел:

1. Андрощук Г. О. Штучний інтелект: економіка, інтелектуальна власність, загрози (2 ч.). *Теорія і практика інтелектуальної власності*. 2021. № 3. С. 45–56. URL: http://nbuv.gov.ua/UJRN/Tpiv_2021_3_6

2. Андрощук Г. О. Економічна безпека підприємства: захист комерційної таємниці : монографія / Г. А. Андрощук, П. П. Крайнів. К. : Издательський Дім «Ін Юре», 2000. 400 с.

3. Бачинин В. А. Філософія права : підручник / В. А. Бачинин, В. С. Журавський, М. І. Панов. К. : Видавничий Дім «Ін Юре», 2003. 472 с.

4. Директива Європейського парламенту і Ради (ЄС) 2019/790 від 17 квітня 2019 року про авторське право і суміжні права на Єдиному цифровому ринку та про внесення змін до директив 96/9/. URL: https://zakon.rada.gov.ua/laws/show/984_022-19#Text

5. Дмитришин В. С. Розпоряджання майновими правами інтелектуальної власності в Україні : навчальний посібник для студентів вищих навчальних закладів. К. : Інст. інтел. власн. і права, 2008. 248 с.

6. Лонг Доріс, Рей Патриція, Жаров В. О., Шевелева Т. М., Василенко І. Е., Дроб'язко В. С. Захист прав інтелектуальної власності: норми міжнародного і національного законодавства та їх правозастосування : практичний посібник. К. : К.І.С., 2007. 448 с.

7. Загальна декларація прав людини : Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text

8. Загальна теорія права : підручник / за заг. ред. М. І. Козюбри. К. : Ваіте, 2015. 392 с.

9. Захист авторського права в Україні: способи і механізми. URL: https://polikarpov.legal/blogposts/zahist-avtorskogo-prava-v-ukraïni-sposobi-i-mehanizmi/

10. Конституція України. *Відомості Верховної Ради України (ВВР)*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

11. Кузнецова Л. В., Солонько М. Ф. Цивільно-правове регулювання колективного управління авторськими правами. *Юридичний науковий електронний журнал*. 2023. № 8. С. 128–131. URL: https://lsej.org.ua/8_2023/27.pdf

12. Луць В. В. Контракти у підприємницькій діяльності [Текст] : навч. посіб. / Прикарпат. ун-т ім. В. С. Стефаника. К. : Юрінком Інтер, 1999. 556 с

13. Марракеський договір про полегшення доступу сліпих, осіб з порушеннями зору або іншими обмеженнями з причин інвалідності сприймати друковану інформацію до опублікованих творів. URL: https://zakon.rada.gov.ua/laws/show/999_001-13#Text

14. Миронець О. М. Функції права: поняття та класифікація. *Юридичний науковий електронний журнал*. 2014. № 2. С. 15–17. URL: https://lsej.org.ua/2_2014/5.pdf

15. Орлюк О. П. Право інтелектуальної власності: академічний курс. Київ : Видавничий дім «Ін Юре», 2007. 696 с.

16. Петренко І. І. Використання літературних творів, що набули статусу творів суспільного надбання. С. 114–118.

17. Підопригора О. А., Підопригора О. О. Право інтелектуальної власності України. Київ : Юрінком Інтер, 1998. 331 с.

18. Рабінович П. М. Основи загальної теорії права та держави. Львів : Видавництво «Край», 2007. 192 с. URL: https://lvivpravo.at.ua/_ld/3/312__.-2007-_____-2.pdf

19. Рабінович П. М. Основи теорії та філософії права: навч. посібник. Львів : Видавництво ЛОБФ «медицина і право», 2021. 256 с. URL: https://library.megu.edu.ua:9443/jspui/bitstream/123456789/2827/1/2021.pdf

20. Стефанишин Н. М. До визначення поняття права інтелектуальної власності в Цивільному кодексі України. *Збірник наукових статей*. С. 110–118.

21. Тарасенко Л. Л. Примусові ліцензії на винаходи, корисні моделі: окремі проблеми і перспективи застосування. *Юридичний науковий електронний журнал*. 2022. № 6. С. 146–150.

22. Угода про торговельні аспекти прав інтелдектуальної власності. URL: https://zakon.rada.gov.ua/laws/show/981_018#Text

23. Цивільний кодекс України 16 січня 2003 року № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#n2261

24. Шишка Р. Б. Охорона права інтелектуальної власності: авторсько-правовий аспект : монографія. Харків : Вид-во Нац. ун-ту внутр. справ, 2002. 386 с.

25. Штафан А. С. Авторське право і суміжні права: особливості правової охорони, здійснення та захисту : монографія / А. С. Штефан. К. : НДІ інтелектуальної власності НАПрНУ, ТОВ «НВП Інтерсервіс», 2017. 150 с. URL: https://fpk.in.ua/images/biblioteka/3bac_pravo/Shtefan.-avtorske-pravo-ta.pdf

26. Boyle J. The Public Domain: Enclosing the Commons of the Mind. New Haven : Yale University Press, 2008. URL: https://thepublicdomain.org/thepublicdomain1.pdf

27. Drahos P. A Philosophy of Intellectual Property. Aldershot : Dartmouth, 1996. URL: https://www.researchgate.net/publication/304514536_A_Philosophy_of_Intellectual_Property

28. Drahos P., Braithwaite J. Information Feudalism: Who Owns the Knowledge Economy? London : Earthscan, 2002. URL: https://www.researchgate.net/publication/246471223_Information_Feudalism_Who_Owns_the_Knowledge_Economy

29. Fisher W. Theories of Intellectual Property. In: Munzer S. (ed.) New Essays in the Legal and Political Theory of Property. Cambridge : Cambridge University Press, 2001. P. 168–200. URL: https://cyber.harvard.edu/people/tfisher/IP/Fisher%20IP%20Theory.pdf

30. INFOPAQ INTERNATIONAL A/S справа C-5/08 ВІД 16 липня 2009 року. URL: https://ipacademy.nipo.gov.ua/wp-content/uploads/2025/07/РІШЕННЯ-Infopaq-International-AS.pdf

31. John Locke, Two Treatises of Government (P. Laslett, ed., Cambridge : Cambridge University Press, 1970), Second Treatise, sec. 27.

32. Landes, W. M., & Posner, R. A. (2003). The Economic Structure of Intellectual Property Law. Cambridge, MA : Harvard University Press. URL: https://inter-droitetaffaires.com/wp-content/uploads/2020/03/The-Economic-Structure-of-Intellectual-Property-Law.pdf

33. Luhmann N. Law as a Social System. Oxford: Oxford University Press, 2004. URL: https://www.researchgate.net/publication/200026833_Law_as_a_Social_System

34. Pound R. Social control through law. New Haven : Yale Univ. Press; Oxford Univ. Press, 1942. 138 p.

35. Samuelson P. A. The Pure Theory of Public Expenditure. *Review of Economics and Statistics*. 1954. Vol. 36. No. 4. P. 387–389. URL: https://courses.cit.cornell.edu/econ335/out/samuelson_pure.pdf

36. Senftleben M. Copyright, Limitations and the Three-Step Test. The Hague: Kluwer Law International, 2004. URL: https://www.ivir.nl/publicaties/download/13_9789041122674.pdf

37. TRIPs and Public Health: The Doha Declaration and Africa. URL: https://www.researchgate.net/publication/4989287_TRIPs_and_Public_Health_The_Doha_Declaration_and_Africa

38. Turner Entertainment Co. v. Huston, CA Versailles, civ. ch., December 19, 1994, translated in Ent. L. Rep., Mar. 1995, at 3. URL: https://ccb.ff6.mwp.accessdomain.com/C/Turner_1994.pdf

39. UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions. Paris: UNESCO, 2005. URL: https://www.unesco.org/en/legal-affairs/convention-protection-and-promotion-diversity-cultural-expressions

References:

1. Androshchuk, H. O. (2021). Artificial Intelligence: Economics, Intellectual Property, Threats (Part 2). *Theory and Practice of Intellectual Property*, (3), 45–56. Retrieved from http://nbuv.gov.ua/UJRN/Tpiv_2021_3_6

2. Androshchuk, H. O., & Krainiv, P. P. (2000). Economic Security of the Enterprise: Protection of Trade Secrets. Kyiv: In Yure Publishing House.

3. Bachinin, V. A., Zhuravskyi, V. S., & Panov, M. I. (2003). Philosophy of Law. Kyiv: In Yure Publishing House.

4. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market. Retrieved from https://zakon.rada.gov.ua/laws/show/984_022-19#Text

5. Dmytryshyn, V. S. (2008). Disposition of Intellectual Property Rights in Ukraine. Kyiv: Institute of Intellectual Property and Law.

6. Long, D., Ray, P., Zharov, V. O., Sheveleva, T. M., Vasylenko, I. E., & Drobiazko, V. S. (2007). Protection of Intellectual Property Rights: Norms of International and National Law and Their Application. Kyiv: K.I.S.

7. Universal Declaration of Human Rights (1948). Retrieved from https://zakon.rada.gov.ua/laws/show/995_015#Text

8. Koziubra, M. I. (Ed.). (2015). General Theory of Law. Kyiv: Vaite.

9. Protection of Copyright in Ukraine: Methods and Mechanisms. Retrieved from https://polikarpov.legal/blogposts/zahist-avtorskogo-prava-v-ukraïni-sposobi-i-mehanizmi/

10. Constitution of Ukraine (1996). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

11. Kuznetsova, L. V., & Solonko, M. F. (2023). Civil Law Regulation of Collective Management of Copyright. *Legal Scientific Electronic Journal*, (8), 128–131. Retrieved from https://lsej.org.ua/8_2023/27.pdf

12. Luts, V. V. (1999). Contracts in Entrepreneurial Activity. Kyiv: Yurinkom Inter.

13. Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled. Retrieved from https://zakon.rada.gov.ua/laws/show/999_001-13#Text

14. Myronets, O. M. (2014). Functions of Law: Concept and Classification. *Legal Scientific Electronic Journal*, (2), 15–17. Retrieved from https://lsej.org.ua/2_2014/5.pdf

15. Orliuk, O. P. (2007). Intellectual Property Law: Academic Course. Kyiv: In Yure Publishing House.

16. Petrenko, I. I. Use of Literary Works in the Public Domain. Pp. 114–118.

17. Pidopryhora, O. A., & Pidopryhora, O. O. (1998). Intellectual Property Law of Ukraine. Kyiv: Yurinkom Inter.

18. Rabinovych, P. M. (2007). Fundamentals of General Theory of Law and State. Lviv: Krai Publishing House. Retrieved from https://lvivpravo.at.ua/_ld/3/312__.-2007-_____-2.pdf

19. Rabinovych, P. M. (2021). Fundamentals of Theory and Philosophy of Law. Lviv: Medicine and Law Publishing House. Retrieved from https://library.megu.edu.ua:9443/jspui/bitstream/123456789/2827/1/2021.pdf

20. Stefanyshyn, N. M. On Defining the Concept of Intellectual Property Law in the Civil Code of Ukraine. Pp. 110–118.

21. Tarasenko, L. L. (2022). Compulsory Licensing of Inventions and Utility Models: Issues and Prospects. *Legal Scientific Electronic Journal*, (6), 146–150.

22. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Retrieved from https://zakon.rada.gov.ua/laws/show/981_018#Text

23. Civil Code of Ukraine (2003). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15#n2261

24. Shyshka, R. B. (2002). Protection of Intellectual Property Rights: Copyright Aspect. Kharkiv: National University of Internal Affairs.

25. Shtefan, A. S. (2017). Copyright and Related Rights: Features of Protection, Exercise and Enforcement. Kyiv: Research Institute of Intellectual Property of NALS of Ukraine. Retrieved from https://fpk.in.ua/images/biblioteka/3bac_pravo/Shtefan.-avtorske-pravo-ta.pdf

26. Boyle, J. (2008). The Public Domain: Enclosing the Commons of the Mind. New Haven: Yale University Press.

27. Drahos, P. (1996). A Philosophy of Intellectual Property. Aldershot: Dartmouth.

28. Drahos, P., & Braithwaite, J. (2002). Information Feudalism: Who Owns the Knowledge Economy? London: Earthscan.

29. Fisher, W. (2001). Theories of Intellectual Property. In S. Munzer (Ed.), New Essays in the Legal and Political Theory of Property (pp. 168–200). Cambridge: Cambridge University Press.

30. Infopaq International A/S (Case C-5/08, 2009). Retrieved from https://ipacademy.nipo.gov.ua/wp-content/uploads/2025/07/РІШЕННЯ-Infopaq-International-AS.pdf

31. Locke, J. (1970). Two Treatises of Government (P. Laslett, Ed.). Cambridge: Cambridge University Press.

32. Landes, W. M., & Posner, R. A. (2003). The Economic Structure of Intellectual Property Law. Cambridge, MA: Harvard University Press.

33. Luhmann, N. (2004). Law as a Social System. Oxford: Oxford University Press.

34. Pound, R. (1942). Social Control through Law. New Haven: Yale University Press.

35. Samuelson, P. A. (1954). The Pure Theory of Public Expenditure. *Review of Economics and Statistics*, 36(4), 387–389.

36. Senftleben, M. (2004). Copyright, Limitations and the Three-Step Test. The Hague: Kluwer Law International.

37. TRIPS and Public Health: The Doha Declaration and Africa. Retrieved from https://www.researchgate.net/publication/4989287_TRIPs_and_Public_Health_The_Doha_Declaration_and_Africa

38. Turner Entertainment Co. v. Huston (1994). Retrieved from https://ccb.ff6.mwp.accessdomain.com/C/Turner_1994.pdf

39. UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions (2005). Retrieved from https://www.unesco.org/en/legal-affairs/convention-protection-and-promotion-diversity-cultural-expressions

БЕЗПЕКОВІ ВИКЛИКИ ШТУЧНОГО ІНТЕЛЕКТУ: ПРАВОВІ АСПЕКТИ

SECURITY CHALLENGES OF ARTIFICIAL INTELLIGENCE: LEGAL ASPECTS

Namiasenko O. K.,
Ph.D. in Law, Associate Professor,
Associate Professor of the Department of Private Law,
Law Institute, Kyiv National Economic University
named after Vadym Hetman,
Kjyv, Ukraine

Abstract. The subject of this study is the social relations that arise in connection with the use of artificial intelligence in public-private relations. Special attention is paid to the issues of artificial intelligence security.

In the modern world of digital technologies, artificial intelligence is gradually beginning to be used in all spheres of human life. The volume of use of artificial intelligence increases every year in geometric progression or, in other words, acquires signs of exponential growth. Legal regulation of the use of artificial intelligence often does not keep up with the volume of implementation. In recent years, various ethical rules and principles of artificial intelligence have been developed at the interstate level.

In many countries, national strategies and concepts for regulating AI technologies have been developed and adopted. At the same time, there is a difference in approaches to the scope of regulatory regulation of artificial intelligence. Thus, the European Union became the first to adopt the legislative document AI Act. The United States, on the other

hand, has chosen a soft model of regulation of artificial intelligence, fearing that strict control would hinder the inflow of investment into this industry.

In addition to the significant growth rates and the formation of different approaches to the legal regulation of AI, it should also be noted that only its developers can fully assess the consequences of the use of AI, as well as more or less predict the results of the implementation of AI in a particular area. This leads to the fact that the use of AI in certain areas of public relations, such as, for example, military technologies and the state's defense capability, the space industry, medicine, justice and human rights, etc., require the need to be aware of additional risks and apply other approaches to control and legal regulation.

Artificial intelligence undoubtedly has great potential to increase the efficiency and speed of response, improve the provision of services adapted to people's needs, support routine tasks and expand opportunities in various areas of public relations. At the same time, there are also significant risks of using artificial intelligence, in particular, such as prejudice and discrimination, disclosure of personal data, false or inaccurate information, excessive dependence on technology, hyper-abuse and others.

The purpose of this study is an attempt to consider the main legal aspects of potential and real threats associated with the use of artificial intelligence in modern society, primarily in the public sphere. **The objectives** are to identify different approaches to clarifying the content of the concept and typology of artificial intelligence, individual aspects related to existing theoretical views on the issues of legal regulation of artificial intelligence, taking into account the current state and main trends and prospects for its further development, to identify the features of the application of artificial intelligence in certain areas of public relations, to analyze possible risks of the application of

artificial intelligence, to identify problems of personal data protection as one of the main risks of the use of AI and other problems of the introduction of AI in Ukraine.

When conducting the study, general scientific and special **methods** of scientific knowledge were used, in particular the dialectical method, analysis and synthesis, comparative law, historical, etc.

General conclusions were made regarding the application of artificial intelligence in modern conditions in Ukraine, as well as in countries and associations with the highest level of application of AI, the prospects for applying the experience of other states and associations in Ukraine.

Keywords: Artificial Intelligence, Security Challenges, Legal Regulation, Digital Security, Ethical Risks, Technological Security.

1. Вступ

Протягом останніх років серед основних цілей в Україні проголошено побудову «найзручнішої цифрової держави у світі». Найголовнішою частиною цифровізації на даний момент є запровадження технологій штучного інтелекту (ШІ). Актуальність дослідження поняття, особливостей регулювання та безпеки застосування штучного інтелекту як в публічній, так і приватних сферах не викликає сумнівів, адже плани розробників ШІ неймовірно амбітні. Фактично час простого ознайомлення з першими технологіями штучного інтелекту закінчився і світ перейшов до початку масштабних технологічних трансформацій. Поряд з беззаперечними перевагами застосування ШІ існують й ризики, зростають вимоги до кібербезпеки.

Правове регулювання застосування штучного інтелекту часто не встигає за обсягами впровадження. Проблеми правового регулювання штучного інтелекту ускладняються також поглибленням різниці у підходах до регулювання штучного інтелекту. Якщо

в США обрали модель м'якого регулювання, фактично передавши всю відповідальність технологічним компаніям, що запроваджують ШІ, в ЄС прийняли Закон ЄС про ШІ, який класифікує ШІ-системи за рівнями ризику та забороняє найнебезпечніші практики.

Метою даного дослідження є спроба розглянути основні правові аспекти потенційних та реальних загроз, пов'язаних з використанням штучного інтелекту в сучасному суспільстві, в першу чергу в публічній сфері.

Завданнями є визначити різні підходи до з'ясування змісту поняття та типології штучного інтелекту, окремих аспектів, пов'язаних з існуючими теоретичними поглядами до питань правового регулювання штучного інтелекту з урахуванням сучасного стану та основних тенденцій і перспектив його подальшого розвитку, визначити особливості застосування штучного інтелекту в окремих сферах публічних відносин, проаналізувати можливі ризики застосування штучного інтелекту, визначити проблеми захисту персональних даних як один з основних ризиків використання ШІ та інші проблеми запровадження ШІ в Україні.

При проведенні дослідження було використано загальнонаукові та спеціальні методи наукового пізнання, зокрема діалектичний метод, аналізу та синтезу, порівняльно-правовий, історичний тощо.

2. Застосування штучного інтелекту в публічній сфері

Штучний інтелект в західному світі стає важливим компонентом цифрового урядування, пропонуючи суттєві переваги в різних сферах, таких як автоматизація, виявлення аномалій та покращення процесу прийняття рішень. Так, чат-боти на базі ШІ використовуються для відповідей на запити громадян та допомоги у заповненні форм, у сфері ліквідації наслідків стихійних лих ШІ допомагає передбачати стихійні лиха та пришвидшувати реагування,

у податковому адмініструванні ШІ використовується для виявлення шахрайства тощо.

З 2020 року в багатьох країнах світу в сфері електронного правосуддя почала застосовуватись концепція «розумних судів», яка стосується використання технологій та даних для підвищення ефективності, прозорості та доступності судових проваджень. Розумні суди включають різні новітні технології, такі як штучний інтелект, блокчейн, рішення для віртуальних конференцій та слухань, а також системи управління справами тощо.

В Україні штучний інтелект вже використовують у різних напрямах — від військових технологій до govtech. Крім того, фокус у розвитку технологій ШІ також має місце у сферах освіти, охорони здоров'я, економіки, урбаністичного планування та багатьох інших. За даними опитування Kantar Panel Ukraine за січень 2024 року до топ ШІ-продуктів, якими вже користувались українці відносяться:

— послуги чат-бота — 57 %;
— технології розпізнавання обличчя — 34 %;
— чат GPT — 33 %;
— персональні асистенти — 26 %;
— роботи-пилососи — 17 %;
— створення зображень на основі ШІ — 13 %;
— технології розумного будинку — 11 %.

Застосування ШІ найбільше спостерігається в таких системах як безпека та охоронні системи, креативна індустрія, банківські послуги, обслуговування клієнтів, медицина, медіа, транспорт та логістика, роздрібна торгівля та електронна комерція, виробництво продуктів харчування, урядові послуги та адміністрування тощо [1, с. 6].

Детальний аналіз проєктів та ініціатив у сфері ШІ в українському публічному секторі представлений в дослідженні Лабораторії цифрової безпеки «Дії та Мрії: штучний інтелект у публічному

секторі». Так, наприклад, в сфері публічного управління планується доповнити застосунок «Дія» додатковим інструментом ШІ «Надія» в формі віртуального помічника та новим проєктом «Дія Office», що покликаний цифровізувати роботу міністерств, зробити її прозорою і забезпечити публічний контроль за виконанням цілей та планів органів влади.

Поміж інших проєктів з діджиталізації та цифровізації є ініціатива під назвою «Голос громадян», у якій Мінцифри планує сканувати усе, що відбувається у соцмережах, в режимі реального часу. Метою є збирати інформацію про дискусії на форумах, у Facebook, Instagram, Telegram, щоб з'ясувати суспільні проблеми і потреби: де погано надають послуги, які існують скарги тощо. Згодом інформацію планується передавати в контакт-центри і комунікувати профільним державним органам, а також багато іншого [2, с. 31].

Застосування та значення штучного інтелекту в Україні зростає з кожним роком та поступово починає застосовуватись не лише в публічній сфері, але й бізнесом, стає одним з основних важелів впливу на трансформацію економіки України як під час війни, так і в перспективі післявоєнної відбудови. За даними Національного Інституту Стратегічних Досліджень у 2026 році штучний інтелект стає каталізатором нової хвилі технологічної революції та основою багатьох бізнес-процесів, що змінює правила гри в усіх секторах економіки — від ШІ-асистента в «Дії» до супутникового зв'язку та оборонних технологій. Україна переходить до агентивної держави, де інфраструктура для ШІ стає критично важливою нарівні з енергетикою та зв'язком. Завдяки проєкту AI Factory в Україні у 2026 р. планується впровадження першої державної інфраструктури для ШІ з високопродуктивним обладнанням та програмним забезпеченням від NVIDIA.

За прогнозами Deloitte, у 2026 р. понад 75 % великих компаній інвестуватимуть в агентні ШІ-системи, коли ШІ діє як автономний

учасник бізнес-процесів, самостійно ухвалюючи рішення без постійного контролю людини [3].

Як зазначає Організація Економічного Співробітництва та Розвитку, цифрові технології не лише створюють величезний потенціал для підвищення продуктивності компаній, вони також можуть покращити економічну стійкість та підтримати відновлення економіки під час війни. Уряд має на меті і надалі сприяти цифровізації малих та середніх підприємств, які є основою економіки України: вони складають 99,9 % усіх підприємств, на них припадає 81,6 % від загальної кількості зайнятих працівників у бізнесі, і вони створюють 70,2 % доданої вартості. Для цього Уряд готує Стратегію підтримки малих та середніх підприємств на період від 2024 до 2027 року. Протягом 2023 року ОЕСР надала Україні рекомендації щодо використання цифрових технологій, щоб підвищити продуктивність, підсилити стійкість і сприяти відновленню [4].

3. Поняття штучного інтелекту та особливості правового регулювання

Термін «штучний інтелект» вперше був використаний у 1956 році Джоном Маккарті на Дартмутській конференції, де зібралися дослідники щоб обговорити можливість створення машин, подібних до людського інтелекту.

Інвестиції та інтерес до ШІ зазнали буму в 2020-х роках, коли до багатьох задач науки та промисловості стали успішно застосовувати машинне навчання завдяки новим методам, використанню потужного обчислювального обладнання, та збиранню величезних наборів даних [5].

Протягом багатьох років було запропоновано значну кількість дефініцій ШІ. Зазвичай поняття штучного інтелекту визначається як інтелектуальне програмне забезпечення, метою якого

є створення інтелектуальних машин або систем, здатних імітувати людський інтелект та поведінку.

Штучний інтелект — це комплекс науки, теорії та техніки, мета яких полягає в тому, щоб відтворити за допомогою машини когнітивні можливості людини. Сучасний розвиток націлений на можливість передачі машині складних завдань, які раніше покладалися на людину [6, с. 58].

Як зазначає керівник наукового центру ДНУ ІІБП НАПрН України професор Баранов О. А., відсутність консенсусної дефініції терміну «штучний інтелект» хвилює практично всіх представників філософських, гуманітарних, технічних та інших наук. Але для представників правової науки ця проблема набуває особливо гострих форм. Це пояснюється тим, що термін «штучний інтелект» не є спеціально-юридичним, він скоріше має універсальний характер та має бути однаково зрозумілим для представників будь-яких політичних, наукових та бізнесових кіл, верств населення, сфер соціального життя тощо [7, с. 33].

В питанні визначення поняття та особливостей правового регулювання штучного інтелекту необхідно з'ясувати природу і зміст відносин з точки зору їх суб'єктних та об'єктних характеристик. Питання суб'єктності є центральним і, зважаючи на суспільний характер цих відносин, в якості їх учасників ми можемо розглядати абсолютну більшість суб'єктів суспільних відносин рівно публічного та приватного характеру. Але в цих відносинах з'являється новий додатковий елемент — штучний інтелект, який найчастіше визначається через інтелектуальний характер свого функціонування і потенційних соціальних наслідків цього.

Зокрема, ШІ інтерпретується через виконання функцій, які вимагають інтелектуальних здібностей для їх реалізації людиною (Реймонд Курцвейл) [8], здатність «робити такі речі, які люди сприймають розумними» (Патрік Вінстон) [9], автоматизацію дій,

що «асоціюються нами з людським мисленням, тобто таких дій, як прийняття рішень, вирішення завдань, навчання» (Річард Белл-ман) [10]. Такі підходи є абсолютно прийнятними з точки зору інженерних та загальнонаукових цілей розробки цього поняття і його подальшого застосування, але в контексті правового визначення та регулювання інструментальне значення таких дефініцій не є таким однозначним.

Логіка існування і застосування самого терміну «штучний інтелект» прямо передбачає наявність певної суб'єктності як ознаки останнього. Але відповідь на питання, чи є на сучасному рівні розвитку або чи виникнуть в осяжному майбутньому підстави для постановки питання про (право) суб'єктність ШІ, буде негативним. Поки що він залишається лише інструментом вирішення тих чи інших завдань інтелектуального характеру в інтересах суспільства в цілому та окремих суб'єктів суспільного життя [11, с. 132]. Задля формування більш прозорої та однозначної концепції ШІ можна констатувати, що машина чи комп'ютер дозволяють імітувати когнітивні функції людського мозку з такими якостями, які має людський розум, людський інтелект [7, с. 43].

Першим нормативно-правовим документом, який на законодавчому рівні закріпив поняття штучного інтелекту став Закон ЄС про ШІ, який визначає його таким чином: «система штучного інтелекту (система ШІ) означає програмне забезпечення, розроблене за допомогою однієї або кількох методик та підходів [12], яке може для заданого набору визначених людиною цілей генерувати такі результати, як контент, прогнози, рекомендації або рішення, що впливають на середовища, з якими вони взаємодіють».

Термін штучний інтелект проте піддається критиці експертами, які проводять різницю між штучним інтелектом, що розцінюється як «сильний» або «загальний» штучний інтелект (за здатністю

абсолютно автономно впроваджувати в контекст дуже різні специфічні питання) і «слабкий», «вузький» або «уповільнений» штучний інтелект (хоч і вкрай просунутий в галузі навчання).

«Вузький» або «слабкий» штучний інтелект стосується систем, призначених для виконання певних завдань або функцій у обмеженій області. Цей тип ШІ навчений досягати успіху у виконанні певних завдань і не має здатності узагальнювати свої знання або застосовувати їх до різних областей.

Генеративний ШІ (наприклад, ChatGPT) — це тип вузького ШІ. Він має здатність генерувати новий контент, такий як зображення, текст, музика або навіть цілі симуляції, на основі шаблонів та прикладів, з яких він навчився. Він навчається на великих наборах даних і використовує такі методи, як «глибоке навчання» та «генеративні моделі», для створення нового та оригінального контенту. Він може бути досить вражаючим своєю здатністю створювати реалістичні та нові результати, але не має здатності міркувати, розуміти контекст або виконувати широкий спектр інтелектуальних завдань у різних областях.

«Загальний» або «сильний» штучний інтелект — це теоретична концепція, яка стосується систем ШІ, що мають інтелект, подібний до людського, і можуть розуміти, навчатися та застосовувати знання в різних областях. Ці системи здатні виконувати будь-яке інтелектуальне завдання, яке може виконати людина.

«Сильний» штучний інтелект, на думку деяких експертів, потребує значного прогресу в фундаментальному дослідженні, щоб бути здатними цілісно моделювати світ, а не вносити прості покращення продуктивності існуючих систем [13, с. 6].

Окрім цих широких категорій, у ШІ також є підгалузі та спеціалізовані галузі, такі як машинне навчання, обробка природної мови (НЛП), комп'ютерний зір, робототехніка, експертні системи тощо.

ШІ значно розвинувся за останні кілька років завдяки двом основним факторам: наявності більших наборів даних, необхідних для навчання; та збільшенню обчислювальної потужності.

Правове регулювання штучного інтелекту, як абсолютно нового та незрозумілого до кінця явища, почалось з формування етичних правил та принципів його використання. До найперших документів, які визначили принципи використання штучного інтелекту відносяться Азіломарські принципи ШІ, які були розроблені на міжнародній конференції в Азіломарі (Каліфорнія, США) в 2017 р. [14], та Пекінські принципи ШІ, опубліковані в травні 2019 р. Пекінською академією штучного інтелекту [15]. Сформульовані переліки принципів можна класифікувати за критеріями дослідницької роботи, етичних та ціннісних аспектів, а також питань довгострокової перспективи (Азіломарські принципи) або за критеріями дослідження та розвитку, управління штучним інтелектом, адаптації та модернізації, реалізації та деталізації, довгострокового планування (Пекінські принципи) [11, с. 134].

ЮНЕСКО розпочала процес розробки «глобального інструменту встановлення стандартів щодо етики штучного інтелекту» в листопаді 2019 р. Думки зацікавлених сторін були зібрані в ході проведених форумів та спеціальних конференцій ЮНЕСКО з ШІ, а на Генеральній конференції у листопаді 2021 р. голосами 193 країн були прийняті Рекомендації щодо етики штучного інтелекту [16]. Документ базується на просуванні таких фундаментальних принципів, як прозорість і справедливість а також важливість людського контролю за системами ШІ, а його наріжним каменем став захист прав і гідності людини.

Окрім загальних принципів та етичних правил застосування ШІ, розроблено та прийнято етичні принципи застосування ШІ в різних сферах публічних відносин.

Зокрема, в межах ООН Центром ШІ та робототехніки ЮНІКРІ були підготовлені й опубліковані звіти: «ШІ та робототехніка для правоохоронних органів» (в партнерстві з Інтерполом в квітні 2019 р.) та «На шляху до відповідальних інновацій ШІ» (в травні 2020 р.).

В Раді Європи 3–4 грудня 2018 року на 31му пленарному засіданні Європейської Комісії з Ефективності Правосуддя було прийнято Європейську Етичну хартію щодо використання штучного інтелекту в судовій системі та її середовищі, яка визначила п'ять основних принципів використання штучного інтелекту в судових системах [6].

В 2023 році ЮНЕСКО представило Керівництво щодо генеративного штучного інтелекту в освіті та дослідженнях, яке стало першим глобальним документом ЮНЕСКО щодо генеративного штучного інтелекту в освіті та має на меті допомогти країнам у впровадженні негайних дій, плануванні довгострокової політики та розвитку людського потенціалу для забезпечення орієнтованого на людину бачення цих нових технологій. У керівництві представлена оцінка потенційних ризиків, які генеративний штучний інтелект може становити для основних гуманістичних цінностей, що сприяють людській діяльності, інклюзії, рівності, гендерній рівності, мовному та культурному розмаїттю, а також множинності думок та висловлювань. У ньому пропонуються ключові кроки для державних установ щодо регулювання використання інструментів генеративного штучного інтелекту, включаючи обов'язкове забезпечення захисту конфіденційності даних та розгляд вікового обмеження для їх використання, окреслюються вимоги до постачальників генеративного штучного інтелекту для забезпечення його етичного та ефективного використання в освіті [17].

Організація економічного співробітництва та розвитку розробила «Рекомендації ОЕСР щодо ШІ», які були прийняті у 2019 році та переглянуті у 2024 році. Документ призначений країнам-членам ОЕСР, але надалі планується, що його охоплення

буде значно більшим — він буде розповсюджуватись на всіх членів Глобального партнерства зі ШІ (GPAI). Індекс є модульним, що дозволяє інтегрувати нові показники по мірі їх напрацювання. Наразі він зосереджений на п'яти політичних рекомендаціях для урядів щодо надійного штучного інтелекту [18].

В січні 2024 року Всесвітня організація охорони здоров'я (ВООЗ) випустила нові рекомендації щодо етики та управління великими мультимодальними моделями (LMM) — типом швидкозростаючої технології генеративного штучного інтелекту (ШІ) із застосуванням у всій системі охорони здоров'я. Керівництво містить понад 40 рекомендацій для розгляду урядами, технологічними компаніями та постачальниками медичних послуг, щоб забезпечити належне використання LMM для зміцнення та захисту здоров'я населення [19].

Окреме місце в системі міжнародних джерел посідає перший у світі комплексний законодавчий акт — Європейський Акт про штучний інтелект (Artificial Intelligence Act — AI Act) [12], що обумовлено унікальною правовою природою ЄС, як інтеграційного об'єднання sui generis. Цей документ спрямований на створення гармонізованого внутрішнього ринку штучного інтелекту в Європейському Союзі, заохочення впровадження цієї технології та створення сприятливого середовища для інновацій та інвестицій за умов дотримання безпеки й забезпечення прав громадян. Законопроект був внесений Європейською Комісією ще в квітні 2021 р., після проходження остаточної перевірки, технічних уточнень та офіційних узгоджень з боку Європейської ради та Ради ЄС, 13 березня 2024 р. схвалений Парламентом Європейського Союзу і офіційно набув чинності з 1 серпня 2024 р.

В консолідованій версії Акт про штучний інтелект надає розробникам і впровадникам штучного інтелекту чіткі вимоги та зобов'язання щодо конкретних видів використання ШІ з наданням гарантій

захисту основних прав людини. Він запроваджує перспективне визначення штучного інтелекту, засноване на гнучкому підході, що ґрунтується на безпеці продукції та оцінці ризиків. Рівні ризиків, які виникають для користувачів при використанні різних систем ШІ та програм, класифіковані, відповідно до чого визначається більший чи менший ступінь регулювання. В цілому, регламент спрямований на зменшення адміністративного та фінансового тягаря для бізнесу, зокрема для малих та середніх підприємств. Разом із тим, підхід ЄС вирізняється суворістю щодо «неєвропейських» гравців ринку ШІ і включає заборону на найбільш нав'язливі форми технології, а також жорсткі правила для Google, Microsoft та інших лідерів ринку, які вимагають від них більшої відкритості у розробці ШІ-продуктів.

Значення Європейського Акту про штучний інтелект не обмежується тільки прямою дією, верховенством над нормами національного законодавства, обов'язковістю для всіх суб'єктів права ЄС. Він позиціонує Європу як провідну у світі в сфері правового регулювання ШІ і має всі шанси набути світового значення, як своєрідний модельний закон за змістом та концептуальними підходами за межами Європи.

Закон про ШІ класифікує системи ШІ на основі їхнього рівня ризику на чотири категорії:

- Неприйнятний ризик: Системи, заборонені через загрозу, яку вони становлять для безпеки або прав людини.
- Високий ризик: Системи, що вимагають суворого контролю та дотримання встановлених стандартів.
- Обмежений ризик: Системи з обмеженими вимогами до прозорості.
- Мінімальний ризик: Системи, що не підлягають спеціальному регулюванню.

Такий підхід дозволяє адаптувати регуляторні вимоги залежно від потенційного впливу систем ШІ на суспільство.

Таким чином, Закон про штучний інтелект встановлює чіткі правила розробки та використання ШІ в ЄС, балансуючи інновації із захистом прав людини [20].

14 березня 2024 Комітет зі штучного інтелекту Ради Європи прийняв текст Рамкової Конвенції зі штучного інтелекту, прав людини, демократії та верховенства права. В переговорному процесі взяло участь 46 держав-членів Ради Європи, а також Аргентина, Австралія, Японія, Мексика, Перу, Сполучені Штати Америки, Ватикан, Уругвай, Канада, Ізраїль, Коста Ріка. Окрім цього, до процесу були залучені понад 70 громадських організацій, міжнародних організацій та представників індустрії.

Україна приєдналася до Рамкової конвенції Ради Європи про ШІ, права людини, демократію та верховенство права. Підписання Конвенції відбулося в м. Страсбург, Франція, під час Конференції EURODIG 2025. Конвенція набере чинності після її ратифікації Верховною Радою України.

Як зазначає Т. Авдєєва, Рамкова конвенція, на відміну від Акта про ШІ, є загальним документом, що закріплює принципи і ціннісні підходи до регулювання ШІ. Вона не містить надміру технічних положень чи норм, які передбачають значну кількість процедур. Рамкова конвенція застосовна до систем, які використовують у публічному секторі або розробляються на замовлення і для публічного сектору, окрім сфери оборони [21].

В Україні на даний час Кабінетом Міністрів України прийнято Розпорядження від 02 грудня 2020 року № 1556-р., яким схвалено Концепцію розвитку штучного інтелекту в Україні, Розпорядження від 12 травня 2021 р. № 438-р Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки [22].

Міністерство цифрової трансформації України 07 жовтня 2023 р. презентувало Дорожню карту з регулювання штучного

інтелекту в Україні, основною метою якої є допомога українським компаніям в підготовці до ухвалення закону-аналога AI Act Європейського Союзу, а громадянам — навчитися захищати себе від ризиків штучного інтелекту [23].

Розпорядженням Кабінету Міністрів України від 13.04.2024 за № 320-р схвалено Концепцію Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 р. (втратила чинність з 14.01.2026 р.), згідно з якою використання технологій ШІ в пріоритетних галузях економіки дасть змогу підвищити ефективність ухвалення рішень шляхом автоматизованої обробки різноманітної інформації та виявлення нових інформаційних шаблонів і тенденцій. Використання технологій ШІ в пріоритетних галузях економіки вимагає зміни виробничих процесів, насамперед процесу ухвалення рішень на різних рівнях державного управління. До пріоритетних галузей економіки, у яких використовуються технології ШІ, відносяться: машинобудівна галузь; хімічна та нафто-хімічна галузь; вугільна промисловість; оборонна промисловість; ядерна промисловість; наукова та науково-технічна діяльність; сільське господарство; охорона здоров'я [24].

Необхідно також зазначити, що через сучасні реалії війни в Україні регулювання ШІ в сфері оборони залишається не публічним.

В зверненні Міністра цифрової трансформації зазначається, що для розвитку України необхідна максимальна дерегуляція та зменшення бюрократії, щоб позбутися перепон для впровадження технологій.

Водночас небезпеку стрімкого розвитку штучного інтелекту та його потенційного впливу на права людини зараз визнає весь світ. Щоб зберегти баланс, Урядом був розроблений підхід, який адресує виклики без упровадження обов'язкового регулювання

в найближчі 2–3 роки. Україна робить ставку на гнучкість і адаптивність. Ми даємо бізнесу час та інструменти для підготовки до майбутнього національного законодавства [1, с. 4–5].

Однак зауважу, що незважаючи на заклик до дерегуляції, Уряд визнає та розуміє необхідність виконання вимог ЄС та відповідно гармонізації законодавства України із законодавством ЄС як необхідної умови вступу! Це не тільки необхідно для євроінтеграції, а й дасть змогу активніше залучати інвестиції на український ринок. Зокрема, за рахунок ідентичних правових режимів.

4. Питання безпеки застосування штучного інтелекту в публічній сфері

На даний момент спостерігається жорстка конкуренція між виробниками штучного інтелекту, що має безпосередній вплив і на безпекові питання його використання. Адже ситуація складається таким чином, що США для прискорення темпів росту свідомо обмежила державний вплив на ШІ і повністю віддала контроль над ним самим розробникам ШІ. ЄС та окремі європейські країни запроваджують більш жорстке правове регулювання ШІ, що безперечно негативно впливає на темпи розробки. Китай здійснює державне регулювання ШІ як на рівні етичних норм та принципів, так і на рівні законодавства, однак завдяки своїм ресурсам створює безпосередню конкуренцію США.

На сьогодні абсолютним лідером в сфері ШІ є США, де працюють найбільші компанії: OpenAI (GPT-4, GPT-5), Google DeepMind (Gemini), Microsoft (Azure AI), Meta (LLaMA), Anthropic (Claude).

Найбільшими виробниками ШІ в Китаї є такі компанії як Baidu (Ernie Bot), Alibaba (Tongyi Qianwen), Huawei (PanGu) та DeepSeek AI, які створили власні мовні моделі, системи автоматизації та військові технології. В планах Пекіну стати лідером у ШІ до 2030 року.

Серед лідерів ШІ в Європі можна зазначити Великобританію (DeepMind, який зараз належить Google, значні університетські дослідження), Німеччину (Siemens, Bosch та SAP, які займаються автоматизацією та впроваджують ШІ в заводи, логістику, автомобільну промисловість) та Францію (Mistral AI як конкурент OpenAI, Thales і Airbus застосовують ШІ у військовій галузі).

Серед інших країн світу, які займаються розробкою ШІ, можна також зазначити Японію, Канаду, Південну Корею, Ізраїль та Індію.

Ще в 2020 році Європейська Комісія у Звіті про наслідки штучного інтелекту, Інтернету речей та робототехніки для безпеки та відповідальності наголошувала, що загальна мета правових рамок безпеки та відповідальності полягає в забезпеченні безпечної, надійної та стабільної роботи всіх продуктів і послуг, включаючи ті, що інтегрують новітні цифрові технології, а також ефективного усунення завданих збитків (п. 1.1). Системи штучного інтелекту повинні інтегрувати механізми безпеки та захисту ще на етапі проектування, щоб забезпечити їхню перевірену безпеку на кожному кроці, враховуючи фізичну та психічну безпеку всіх зацікавлених сторін (п. 2) [25].

Суд Справедливості ЄС в Стратегії ШІ виділяє два типи ризиків: ризик використання ШІ власними силами та ризик використання ШІ іншими. В обох випадках розуміння цих ризиків та вжиття проактивних заходів для їх пом'якшення є важливими [13, с. 17].

До основних ризиків віднесено наступні:

1) упередження, які можуть бути випадково введені в навчальні дані алгоритму та які можуть призвести до моделі, що мимоволі створюватиме дискримінацію;

2) розкриття конфіденційних даних під час використання алгоритмів у хмарі шляхом надання підказок, що містять конфіденційну або особисту інформацію;

3) хибна або неточна (або нерелевантна) інформація. Це може траплятися, наприклад, в алгоритмах, які були навчені

з недостатніми або низькоякісними даними. Крім того, у випадку генеративного ШІ вже було помічено, що результати часто бувають неправильними або неточними. Деякі фахівці називають це явище «галюцинаціями», коли генеративний алгоритм ШІ вигадує інформацію та робить її реальною;

4) надмірна залежність від технологій. Результати, що надаються алгоритмами ШІ, повинні постійно перевірятися, і має застосовуватися критичне мислення людини. У разі помилок машину необхідно перенавчати або виправляти. Більше того, якщо алгоритм недоступний, персонал все ще повинен мати можливість взяти на себе управління від машини та виконувати ці завдання вручну, і таким чином їхні навички та досвід необхідно зберігати як механізм стійкості;

5) гіперзловживання. Швидкий розвиток ШІ та використання алгоритмів може призвести до випадків надто швидкого та неконтрольованого прийняття рішень, ігнорування всіх внутрішніх правил належної практики (IT-архітектура, безпека та захист даних). Належна система управління аналізом та впровадженням таких інструментів є важливою для зменшення такого ризику;

6) дезінформація, цензура та контроль. У чужих руках алгоритми штучного інтелекту можуть бути використані для поширення фейкової інформації (створення фальшивих відео, зображень тощо) або для цензурування поширення інформації [13, с. 17].

Ризик та наслідки упередження та дискримінації між окремими особами та групами найкраще всього можна проілюструвати на прикладі використання алгоритмів у кримінальних справах з метою характеристики особистості: експерименти у Сполучених Штатах (COMPAS) та у Великобританії (HART).

Через обмеженість використовуваної методології цей суто статистичний підхід призвів до невірних результатів: з констатації того, що деякі афроамериканці частіше беруть участь у злочинних

діяннях, було зроблено висновок про те, що англо-американське населення загалом становить більший ризик. Таким чином, навіть у разі дрібних правопорушень ці системи давали негативні результати щодо обвинувачених афроамериканців, що призвело до несправедливого збільшення термінів їх покарань. Цей підхід має дискримінаційний і упереджений характер, повинен бути замінений іншим, більшою мірою відповідним європейським стандартам щодо кримінальних санкцій, що надає можливість реабілітації та реінтеграції будь-якій людині. Якщо, наприклад, алгоритмічні системи допоможуть покращити збір інформації для служб пробації і уможливити швидший збір необхідної інформації для того, щоб були дотримані права людини, то такі ініціативи можуть бути корисними (особливо в області прискореного судочинства). Будь-яке інше використання може бути упередженим і суперечити певним національним і наднаціональним основоположним принципам [6, с. 56; 26, с. 116].

Штучний інтелект може надати нові інструменти для складних кібератак, що дозволяє видавати себе за іншу особу та забруднювати дані, що можуть бути використані зловмисниками. Розуміння та усунення цих ризиків мають вирішальне значення для відповідального та безпечного використання технології штучного інтелекту. У міру розвитку штучного інтелекту та інших технологій кібербезпеки, розвиваються й самі кіберзагрози — і кіберзлочинці можуть використовувати силу ШІ для досягнення власних цілей. Конфіденційність і етика стануть більш критичними, оскільки системи штучного інтелекту стануть більш інтегрованими в кібербезпеку, що перетворить ШІ як на виклик, так і на можливість.

Державна служба спеціального зв'язку та захисту інформації України затвердила рекомендації з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту у відповідному Наказі від 23 лютого 2026 року № 154, який було видано на виконання плану заходів з реалізації Концепції

розвитку штучного інтелекту в Україні на 2025–2026 роки, ухваленої Урядом.

Документ розроблено як практичний орієнтир для власників та розпорядників державних і приватних інформаційних, електронних комунікаційних та технологічних систем. Рекомендації мають добровільний характер і призначені для використання під час розробки планів кіберзахисту та оцінки ризиків при впровадженні технологій ШІ [27].

Ризики надмірної залежності від технологій особливо впливають на неповнолітніх. Австралія стала першою країною у світі, яка запровадила заборону на користування соціальними мережами для дітей, молодших за 16 років, — відповідний закон набув чинності 10 грудня 2025 року. Під заборону потрапили Facebook, Instagram, Snapchat, Threads, TikTok, Twitch, X, YouTube, Kick та Reddit. А платформи зобов'язали вживати «розумних заходів» для блокування доступу неповнолітніх, інакше їм загрожують штрафи до 50 мільйонів австралійських доларів (близько $32 млн).

У листопаді 2025 року Європарламент ухвалив резолюцію про встановлення єдиного цифрового порогу в 16 років для самостійної реєстрації в соціальних мережах. Діти від 13 до 15 років зможуть отримувати доступ до них лише за згодою батьків. Для відеоплатформ і ШІ-сервісів встановлено інші правила: доступ можливий з 13 років за батьківською згодою [28].

Можливі стратегії пом'якшення перерахованих ризиків можуть включати забезпечення належного рівня обізнаності та навчання персоналу, який обирає, створює, тестує або впроваджує рішення на основі ШІ, належного рівня людського контролю та нагляду, заохочення критичного мислення щодо використання алгоритмів штучного інтелекту та ін.

Проблеми, пов'язані з ризиком розкриття конфіденційних та особистих даних, захистом персональної інформації, розглядаються в розділі 5.

5. Захист персональних даних при використанні штучного інтелекту

З появою великих наборів даних та швидким розвитком штучного інтелекту зростають ризики витоків даних, несанкціонованого доступу та маніпулювання персональною інформацією. Алгоритми здатні генерувати надзвичайно точні профілі користувачів на основі даних. Це створює як можливості, так і небезпеки.

Кіберзагрози заслуговують на особливу увагу. Масивні бази даних, що зберігають конфіденційну інформацію, регулярно приваблюють кіберзлочинців. У разі успішної атаки під загрозою може опинитися як репутація організації, так і безпека користувачів, оскільки їхні персональні дані можуть бути розкриті.

Це підкреслює необхідність чітких та прозорих правил щодо збору та використання персональних даних. Як наслідок, законодавці по всьому світу розробляють норми та стандарти, спрямовані на балансування інтересів комерційних компаній з правами громадян на конфіденційність та безпеку.

Основним нормативно-правовим актом ЄС у сфері захисту персональних даних є Загальний регламент про захист даних (GDPR), який був прийнятий у 2016 році та набув чинності 25 травня 2018 року. GDPR суттєво впливає на розробку та використання систем ШІ, встановлюючи вимоги до обробки персональних даних [29]. Згідно з GDPR, організації повинні забезпечити законність, прозорість та справедливість обробки даних, що є критично важливим під час навчання моделей ШІ на великих наборах даних, які можуть містити персональну інформацію.

Закон про ШІ доповнює Загальний регламент про захист даних (GDPR), не змінюючи його. Він встановлює вимоги до розробників та користувачів систем штучного інтелекту щодо безпеки, прозорості та підзвітності, забезпечуючи захист персональних даних та основних прав людини. До них належать обов'язкові оцінки

ризиків, заходи щодо пом'якшення потенційних негативних наслідків та підзвітність за використання ШІ.

Загальний регламент про захист даних (GDPR) встановлює високі стандарти захисту персональних даних, достатньо чіткі правила для компаній та організацій щодо обробки особистої інформації та суттєві обмеження, відповідальність для тих, хто не дотримується вимог щодо захисту даних, включаючи значні штрафи, що стимулює бізнес-структури ретельно виконувати вимоги.

Відповідно до Регламенту «персональні дані» означає будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи (ст. 4). «порушення захисту персональних даних» означає порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або іншим чином опрацьовано. Принципи захисту даних необхідно застосовувати до будь-якої інформації про фізичну особу, яку ідентифіковано чи можна ідентифікувати.

Відповідно до глави 3 Регламенту за суб'єктами даних закріплюються такі права, як право на доступ до своїх персональних даних (ст. 15), право на виправлення недостовірних даних (ст. 16), право на видалення даних (право на забуття) (ст. 17), право на обмеження опрацювання (ст. 18), право на мобільність даних (ст. 20), право на заперечення проти обробки даних (ст. 21). На практиці вони мають фіксуватися у політиках приватності та безпеки компанії та відображатися у всіх процесах її діяльності [29].

Право на доступ до персональних даних є одним із ключових прав суб'єкта даних. Воно реалізується шляхом подання запиту, за допомогою якого суб'єкт даних може отримати від контролера підтвердження факту обробки своїх персональних даних і, у випадку підтвердження, — доступ до цих даних. Право на доступ також включає отримання інформації про цілі обробки; категорію таких даних; одержувача, якому дані були або будуть розкриті; період, протягом якого передбачається, що такі відомості будуть зберігатись (чи критерії визначення такого періоду); інформацію про походження даних, якщо вони не були зібрані від самого суб'єкта даних; існування автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу тощо.

Дотримання встановлених Регламентом прав суб'єктів даних може бути важливим і для українських компаній. Багато українських компаній вже працюють або планують виходити на європейський ринок. Для уникнення штрафів та інших негативних наслідків для бізнесу їм важливо дотримуватися правил збору та обробки персональних даних, прав суб'єктів даних — громадян ЄС [9]. Доцільно зауважити, що дотримання Регламенту обов'язкове і для компаній, які ведуть бізнес в Україні, але мають серед своїх клієнтів резидентів Євросоюзу.

Наприклад, це актуально для розробників застосунків, які доступні для завантажування у країнах ЄС або для українських банків, що відкривають рахунки громадянам ЄС. Принагідно варто звернути увагу, що Україна також поступово робить кроки до приведення законодавства про захист персональних даних у відповідність до права ЄС [30, с. 117]. Так, у лютому 2024 року Верховна Рада відновила розгляд законопроєкту про захист персональних даних № 8153 від 25 жовтня 2022 року. Цей законопроєкт було включено до порядку денного парламенту, і наразі триває його неофіційне громадське обговорення [31].

Політика оцінки ризиків має ґрунтуватися на простому принципі обережності. Для повного використання потенціалу алгоритмів за дотримання принципів захисту даних слід застосовувати принцип обережності та проводити профілактичну політику для протидії потенційним ризикам, пов'язаним із використанням даних, оброблюваних цими алгоритмами, та впливом їх використання на окремих осіб та суспільство в цілому.

Принцип законності при обробці персональних даних та зобов'язання щодо запобігання або мінімізації впливу обробки даних на права та основні свободи суб'єктів персональних даних повинні зобов'язувати проведення попередньої оцінки ризиків потенційних наслідків, які може мати обробка персональних даних за допомогою штучного інтелекту на основні права та свободи суб'єктів. Ця оцінка має дозволити передбачити реалізацію відповідних заходів, а саме на стадії проектування за умовчанням, з метою зниження виявлених ризиків.

Оскільки персональні дані повинні оброблятися у певних та законних цілях, вони не повинні використовуватися іншим чином, не відповідно до даних цілями, а також не повинні ставати предметом такого використання, яке суб'єкт даних вважав би несподіваним, неприйнятним чи спірним (принцип лояльності). Тому питання повторного використання персональних даних, яким було відкрито публічний доступ, потребує найвищої обережності.

При розробці методів обробки даних, які використовуються алгоритмами, слід зводити до мінімуму наявність надлишкових або незначних даних та уникати будь-яких потенційних прихованих відхилень та будь-яких ризиків дискримінації чи негативного на основні права і свободи суб'єктів даних.

У разі використання штучного інтелекту особливе значення мають права суб'єктів даних та контроль, який кожен повинен мати над своєю особистою інформацією, що передбачає

можливість реалізації таких прав: право не ставати об'єктом автоматично виведеного рішення, що надає істотний вплив на особу, щодо якої вона винесена, без урахування її точки зору, без права отримання інформації про логіку, застосовану алгоритмами при обробці даних, право на заперечення проти такої обробки та право на оскарження у суді [6].

Україна взяла на себе зобов'язання щодо захисту персональних даних, однак чинний Закон України «Про захист персональних даних», прийнятий у 2011 році, вже не відповідає сучасним міжнародним стандартам. Цей факт підтверджують численні експертні оцінки, зокрема від Ради Європи. Щоб забезпечити належний рівень захисту даних, Україна потребує суттєвого реформування чинного законодавства.

Головним законодавчим актом, який має внести ці зміни, є Проєкт Закону України «Про захист персональних даних» № 8153, що зареєстрований 25.10.2022, та станом на сьогодні прийнятий Верховною Радою за основу.

Новий законопроєкт несе комплексну реформу, яка зобов'яже український бізнес та державні органи працювати з даними за європейськими принципами. Зокрема, Законопроєкт № 8153 значно розширює права громадян щодо контролю за власними даними, вводячи ключові концепції GDPR, а саме:

— право вимагати видалення своїх персональних даних, якщо вони більше не потрібні для цілей, з якими їх було зібрано;

— право отримувати інформацію про те, які дані обробляються, з якою метою, а також вимагати їх виправлення;

— право вимагати тимчасово припинити обробку даних за певних умов (наприклад, якщо дані оскаржуються);

— право заперечувати проти використання даних, наприклад, для цілей прямого маркетингу.

Крім цього, на відміну від чинного закону, який дозволяє «неявну» згоду, новий законопроєкт вимагає, щоб згода була:

— явно вираженою (повинна бути надана активною дією (наприклад, проставлення галочки в чекбоксі, підпис, натискання кнопки);

— конкретною (мати чітко зазначену мету обробки даних (не можна отримати загальну згоду «на все»);

— інформованою (суб'єкт даних має отримати повну та доступну інформацію про обробку).

Також положення законопроєкту передбачають різке збільшення фінансової відповідальності за порушення, що є однією з найболючіших новацій для бізнесу.

Штрафи для юридичних осіб можуть сягати до 30 мільйонів гривень (залежно від серйозності та характеру порушення). Ці штрафи покликані стимулювати компанії вкладати кошти в безпеку даних та комплаєнс-процедури.

Для ефективної підготовки до імплементації нового закону, ІТ-компаніям та іншим суб'єктам господарювання варто здійснити такі кроки:

— призначити Data Protection Officer (DPO) — фахівця з питань захисту даних. Його обов'язки мають включати моніторинг відповідності, взаємодію з державними органами та консультування щодо ризиків;

— переглянути та адаптувати чинні Політику конфіденційності, внутрішні регламенти та договори. Це стосується як договорів з клієнтами, так і з ІТ-підрядниками та сервісами (наприклад, CRM);

— переконатися, що обробка персональних даних ґрунтується на чітких правових підставах, таких як згода суб'єкта, виконання договору або законний інтерес;

— провести аудит усіх даних, які вони збирають, обробляють та зберігають. Особливу увагу варто приділити чутливим персональним даним (біометричні, генетичні, дані про стан здоров'я,

расу, політичні погляди) та визначити, чи відповідає їх обробка новим вимогам;

— підготуватися до реалізації таких прав, як право на забуття, мобільність даних та захист від автоматизованих рішень;

— розробити чітку процедуру повідомлення про витоки даних.

Загалом для українського бізнесу, особливо в IT-сфері, прийняття законопроєкту № 8153 спростить співпрацю з європейськими партнерами та клієнтами, оскільки Україна стане країною з адекватним рівнем захисту даних [32].

Відповідно до Звіту Європейської Комісії щодо прогресу України в межах Пакета розширення Європейського Союзу за 2025 рік щодо захисту персональних даних зазначено наступне: «Україна не досягла жодного прогресу у приведенні своєї правової бази щодо захисту персональних даних до законодавства ЄС. Остаточне прийняття законопроектів про захист персональних даних та про Національну комісію з питань захисту персональних даних та доступу до публічної інформації, зареєстровану у 2022 році, все ще очікується» [33].

6. Висновки

Підсумовуючи можна зазначити наступне:

1. Статистичні дані останніх років свідчать про експонціальне зростання обсягів використання штучного інтелекту в світі. Україна застосовує штучний інтелект перш за все в таких сферах публічних відносин як державне управління (govtech), правосуддя, соціальна сфера, податки та митниця, публічні закупівлі, освіта та охорона здоров'я тощо. Для цього створено основні законодавчі рамки. Уряд проголосив про певний часовий проміжок, коли публічна сфера та бізнес будуть мати можливість запровадження технологій штучного інтелекту на фоні м'якого правового регулювання. Разом з цим необхідно розуміти, що євроінтеграційний напрямок розвитку України вимагає приведення національного законодавства

у відповідність до законодавства ЄС, яке характеризується більш жорсткими вимогами щодо використання ШІ. Окреме стратегічне значення має використання ШІ в сфері оборони.

2. Правове визначення терміну «штучний інтелект» ускладняється тим, що за своїм змістом він не є спеціально-юридичним, а скоріше має універсальний характер та включає в себе технічні, філософські, соціальні аспекти. Через це, надана дефініція поняття «штучний інтелект» має бути однаково зрозумілою для представників будь-яких політичних, наукових та бізнесових кіл, верств населення, сфер соціального життя тощо.

Визначення поняття штучного інтелекту ускладнюється також тим, що ШІ інтерпретується через виконання функцій, які вимагають наявності інтелектуальних здібностей, що характерні виключно для людини, як живої біологічної істоти. В правових відносинах людина виступає суб'єктом, однак суспільство не готове до правового регулювання ШІ як окремого суб'єкта правовідносин.

3. Початком правового регулювання ШІ можна вважати розробку етичних правил та принципів його використання, зокрема першими були прийняті Азіломарські принципи ШІ, які були розроблені на міжнародній конференції в Азіломарі (Каліфорнія, США) в 2017 р. та Пекінські принципи ШІ, опубліковані в травні 2019 р. Пекінською академією штучного інтелекту

Окрім загальних правил та принципів, були розроблені також етичні принципи використання ШІ в окремих сферах, наприклад Європейська Етична хартія щодо використання штучного інтелекту в судовій системі та її середовищі 2018 р. (Рада Європи, Європейська Комісія з Ефективності Правосуддя), Рекомендації щодо етики та управління великими мультимодальними моделями (LMM) 2024 р. (Всесвітня організація охорони здоров'я) та ін.

Першим нормативно-правовим актом став Закон ЄС про ШІ, який надає розробникам і розгортачам систем чіткі вимоги

та зобов'язання щодо конкретного використання штучного інтелекту, класифікує ризики залежно від функції, яку виконує система штучного інтелекту, а також від конкретної мети та способів, для яких використовується система.

Загалом, правове регулювання ШІ здійснюється на національному рівні окремих країн, об'єднань (ЄС), міждержавному рівні тощо.

4. На даний момент спостерігається жорстка конкуренція між виробниками штучного інтелекту, що має безпосередній вплив і на безпекові питання його використання. Адже ситуація складається таким чином, що США для прискорення темпів росту свідомо обмежила державний вплив на ШІ і повністю віддала контроль над ним самим розробникам ШІ. ЄС та окремі європейські країни запроваджують більш жорстке правове регулювання ШІ, що безперечно негативно впливає на темпи розробки. Китай здійснює державне регулювання ШІ як на рівні етичних норм та принципів, так і на рівні законодавства, однак завдяки своїм ресурсам створює безпосередню конкуренцію США.

Список використаних джерел:

1. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Версія для консультацій. Єдиний веб-портал органів виконавчої влади України. Міністерство цифрової трансформації України, опубліковано 26 червня 2024 р. URL: https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuie-bilu-knyhu (дата звернення: 10.03.2026 р.).

2. Авдєєва Т. Дії та Мрії: штучний інтелект у публічному секторі. Аналітичне дослідження. Лабораторія цифрової безпеки, Міжнародний Фонд Відродження, 2024. URL: https://dslua.org/wp-content/uploads/2024/02/Mrii_ta_dii_kopiia.pdf (дата звернення: 17.03.2026 р.).

3. Цифрова трансформація економіки України. Січень 2026 року. Національний Інститут Стратегічних Досліджень. URL: https://niss.gov.ua/

news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-sichen-2026-roku (дата звернення: 17.03.2026 р.).

4. Підвищення стійкості шляхом прискорення цифрової трансформації бізнесу в Україні. Організація Економічного Співробітництва та Розвитку. 22 травня 2024 р. URL: https://www.oecd.org/uk/publications/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50.html (дата звернення: 17.03.2026 р.).

5. Історія штучного інтелекту. Вікіпедія. URL: https://uk.wikipedia.org/wiki/ (дата звернення: 10.03.2026 р.).

6. Європейська Комісія з Ефективності Правосуддя. Європейська Етична хартія щодо використання штучного інтелекту в судовій системі та її середовищі. Страсбург, 3–4 грудня 2018 року. URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4 (дата звернення: 10.03.2026 р.).

7. Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і Право*. 2023 р. № 1(44). С. 32–49. URL: https://ippi.org.ua/sites/default/files/5_28.pdf (дата звернення: 11.03.2026).

8. Kurzweil R. The Age of Intelligent Machines. Cambridge (Massachusetts, USA): MIT Press, 1990. 565 p. URL: https://www.kurzweilai.net/the-age-of-intelligent-machines-can-machines-think (дата звернення: 11.03.2026).

9. Patrick Henry Winston. Artificial Intelligence (3d Ed.) Addison-Wesley, 1992, 737 p. URL: https://courses.csail.mit.edu/6.034f/ai3/rest.pdf (дата звернення: 11.03.2026).

10. Bellman R. E. An Introduction to Artificial Intelligence: Can Computers Think? San Francisco : Boyd & Fraser Publishing Company ; Thomson Course Technology, 1978. 146 p. (дата звернення: 11.03.2026).

11. Намясенко О. К., Ратушний С. М. Штучний інтелект: у пошуках моделі правового регулювання. *Успіхи і досягнення у науці* : журнал. 2024. № 6(6) 2024. С. 128–141 (дата звернення: 13.03.2026).

12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial

intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). *Official Journal of the European Union*. L series, 2024/1689, 12.7.2024 URL : https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 13.03.2026).

13. Artificial Intelligence Strategy. Court of Justice of the European Union. *Directorate-General for Information*. 2023. P. 1–25. URL: https://curia.europa.eu/site/upload/docs/application/pdf/2023-11/cjeu_ai_strategy.pdf (дата звернення: 13.03.2026).

14. Asilomar AI Principles. 2017. URL: https://www.jstor.org/stable/pdf/resrep12564.12.pdf (дата звернення: 13.03.2026).

15. Beijing AI Principles. 2019. URL: https://link.springer.com/content/pdf/10.1007/s11623-019-1183-6.pdf (дата звернення: 13.03.2026).

16. Recommendation on the ethics of artificial intelligence. UNESCO. Adopted on 23 Nov. 2021. URL: https://digitallibrary.un.org/record/4062376?v=pdf#files (дата звернення: 13.03.2026).

17. Guidance for generative AI in education and research. United Nations Educational, Scientific and Cultural Organization. 2023. URL: https://unesdoc.unesco.org/ark:/48223/pf0000386693/pdf/386693eng.pdf.multi (дата звернення: 13.03.2026).

18. The OECD. AI Index. Technical paper. DSTI/DPC/AIGO(2025)1/FINAL OECD. 2026. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/oecd-ai-observatory-index_8f5fa0f2/32c01014-en.pdf (дата звернення: 13.03.2026).

19. Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. World Health Organization. 25 March 2025. URL: https://www.who.int/publications/i/item/9789240084759 (дата звернення: 13.03.2026).

20. Olha Petriv. Personal data protection in the age of artificial intelligence: international approaches and challenges. January 23, 2025. URL: https://cedem.org.ua/en/consultations/ai-data-protection/ (дата звернення: 16.03.2026).

21. Авдєєва Т. Рамкова конвенція Ради Європи про штучний інтелект: перемога чи поразка? Лабораторія цифрової безпеки. 27 березня 2024. URL: https://dslua.org/publications/ramkova-konventsiia-rady-yevropy-pro-shtuchnyy-intelekt-peremoha-chy-porazka/ (дата звернення: 16.03.2026).

22. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження КМУ від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 13.03.2026).

23. Регулювання штучного інтелекту в Україні: презентуємо дорожню карту: Міністерство цифрової трансформації України, 07 жовтня 2023 р. URL: https://thedigital.gov.ua/news/technologies/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu (дата звернення: 13.03.2026).

24. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року : Розпорядженням Кабінету Міністрів України від 13.04.2024 за № 320-р (втратила чинність). URL: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text (дата звернення: 13.03.2026).

25. Звіт про наслідки штучного інтелекту, Інтернету речей та робототехніки для безпеки та відповідальності. Європейська Комісія. Брюссель, 19.02.2020. COM (2020) 64 остаточна версія. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064 (дата звернення: 16.03.2026).

26. Marina M. Matić Bošković. Implications of EU AI Regulation for criminal justice. Institute of Criminological and Sociological Research, Belgrade, Serbia. P. 111–120. URL: http://institutecsr.iksi.ac.rs/1040/1/08-Matic-Boskovic.pdf (дата звернення: 16.03.2026).

27. Наказ Адміністрації Держспецзв'язку від 23.02.2026 № 154 «Про затвердження Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту» URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-23-02-2026-154-pro-zatverdzhennya-rekomendacii-z-kiberzakhistu-informaciino-komunikaciinikh-sistem-yaki-vikoristovuyut-tekhnologiyi-shtuchnogo-intelektu (дата звернення: 16.03.2026).

28. Баловсяк Н. Епоха позбавлення ілюзій та відповідального ШІ: яким буде 2026-й технологічний рік. Український Тиждень. 30 Грудня 2025. URL: https://tyzhden.ua/epokha-pozbavlennia-iliuzij-ta-vidpovidalnoho-shi-iakym-bude-2026-j-tekhnolohichnyj-rik/ (дата звернення: 16.03.2026).

29. Загальний регламент про захист даних (GDPR). Офіційний переклад українською мовою. URL: kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf, https://gdpr-text.com/uk/ (дата звернення: 16.03.2026).

30. Яворська О. С. Захист персональних даних у цифровому середовищі: досвід ЄС. *Юридичний науковий електронний журнал*. № 9/2024. С. 117-119. (дата звернення: 16.03.2026).

31. Про захист персональних даних : Проєкт Закону від 25.10.2022. № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення: 17.03.2026)

32. Дмитро Слободянюк. Захист персональних даних (GDPR / Директива ЄС): що змінюють нові законопроєкти в Україні. *Юридична Газета*. 13 жовтня 2025. URL: https://yur-gazeta.com/dumka-eksperta/zahist-personalnih-danih-gdpr--direktiva-es-shcho-zminyuyut-novi-zakonoproekti-v-ukrayini.html (дата звернення: 16.03.2026).

33. Commission Staff Working Document. Ukraine. Report. 2025 Communication on EU enlargement policy. Brussels, 4.11.2025. SWD(2025) 759 final. URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/EU-enlargement-.pdf (дата звернення: 16.03.2026).

References:

1. Bila knyha z rehulyuvannya SHI v Ukrayini: bachennya Mintsyfry. Versiya dlya konsul'tatsiy. Yedynyy veb-portal orhaniv vykonavchoyi vlady Ukrayiny. Ministerstvo tsyfrovoyi transformatsiyi Ukrayiny, opublikovano 26 chervnya 2024 r. URL: https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuie-bilu-knyhu (in Ukrainian).

2. Avdyeyeva, T. Diyi ta Mriyi: shtuchnyy intelekt u publichnomu sektori. Analitychne doslidzhennya. Laboratoriya tsyfrovoyi bezpeky, Mizhnarodnyy Fond Vidrodzhennya, 2024. URL: https://dslua.org/wp-content/uploads/2024/02/Mrii_ta_dii_kopiia.pdf (in Ukrainian).

3. Tsyfrova transformatsiya ekonomiky Ukrayiny. sichnya 2026 roku. Natsional'nyy instytut stratehichnykh doslidzhen'. URL: https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-sichen-2026-roku (in Ukrainian).

4. Pidvyshchennya stiykosti shlyakhom pryskorennya tsyfrovoyi transformatsiyi biznesu v Ukrayini. Orhanizatsiya Ekonomichnoho Spivrobitnytstva ta Rozvytku. 22 travnya 2024 r. URL: https://www.oecd.org/uk/publications/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50.html (in Ukrainian).

5. Istoriya shtuchnoho intelektu. Vikipediya. URL: https://uk.wikipedia.org/wiki/ (in Ukrainian).

6. Yevropeys'ka komisiya z efektyvnosti Pravosuddya. Yevropeys'ka Etychna Khartiya vykorystannya shtuchnoho intelektu v sudoviy systemi ta yiyi seredovyshchi. Strasburh, 3-4 hrudnya 2018 roku. URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4 (in Ukrainian).

7. Baranov, O. A. Vyznachennya terminu "shtuchnyy intelekt". *Informatsiya i Pravo*. № 1(44)/2023 r. S. 32-49. URL: https://ippi.org.ua/sites/default/files/5_28.pdf (in Ukrainian).

8. Kurzweil, R. The Age of Intelligent Machines. Cambridge (Massachusetts, USA): MIT Press, 1990. 565 p.

URL: https://www.kurzweilai.net/the-age-of-intelligent-machines-can-machines- think (дата звернення: 11.03.2026).

9. Winston, Patrick Henry. Artificial Intelligence (3d Ed.) Addison-Wesley, 1992, 737 p. URL: https://courses.csail.mit.edu/6.034f/ai3/rest.pdf (дата звернення: 11.03.2026).

10. Bellman, R. E. An Introduction to Artificial Intelligence: Can Computers Think? San Francisco: Boyd & Fraser Publishing Company; Thomson Course Technology, 1978. 146 p. (дата звернення: 11.03.2026).

11. Namyasenko, O. K., Ratushnyy, S. M. Shtuchnyy intelekt: u poshukakh modeli pravovoho rehulyuvannya. Uspikhy i dosyahnennya v nautsi: zhurnal. 2024. № 6(6) 2024. S. 128–141. (in Ukrainian).

12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). *Official Journal of the European Union*, L series, 2024/1689, 12.7.2024 URL : https://eur-lex.europa.eu/eli/reg/2024/1689/oj

13. Artificial Intelligence Strategy. Court of Justice of the European Union. Directorate-General for Information. 2023. P. 1–25. URL: https://curia.europa.eu/site/upload/docs/application/pdf/2023-11/cjeu_ai_strategy.pdf

14. Asilomar AI Principles, 2017, URL: https://www.jstor.org/stable/pdf/resrep12564.12.pdf (дата звернення: 13.03.2026).

15. Beijing AI Principles, 2019, URL: https://link.springer.com/content/pdf/10.1007/ s11623-019-1183-6.pdf

16. Recommendation on the ethics of artificial intelligence. UNESCO. Adopted on 23 Nov. 2021. URL: https://digitallibrary.un.org/record/4062376?v=pdf#files

17. Guidance for generative AI in education and research. United Nations Educational, Scientific and Cultural Organization. 2023. URL: https://unesdoc.unesco.org/ark:/48223/pf0000386693/pdf/386693eng.pdf.multi

18. The OECD. AI Index. Technical paper. DSTI/DPC/AIGO (2025) 1 / FINAL OECD. 2026. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/oecd-ai-observatory-index_8f5fa0f2/32c01014-en.pdf

19. Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. World Health Organization. 25 March 2025. URL: https://www.who.int/publications/i/item/9789240084759

20. Petriv, Olha. Personal data protection in the age of artificial intelligence: international approaches and challenges. January 23, 2025. URL: https://cedem.org.ua/en/consultations/ai-data-protection/

21. Avdyeyeva, T. Ramkova konventsiya Rady Yevropy pro shtuchnyy intelekt: peremoha chy porazka? Laboratoriya tsyfrovoyi bezpeky. 27 bereznya 2024. URL: https://dslua.org/publications/ramkova-konventsiia-rady-yevropy-pro-shtuchnyy-intelekt-peremoha-chy-porazka/ (in Ukrainian).

22. Pro skhvalennya Kontseptsiyi rozvytku shtuchnoho intelektu v Ukrayini: ROZPORYADZHENNYA KMU vid 2 hrudnya 2020 r. № 1556-r. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text (in Ukrainian).

23. Rehulyuvannya shtuchnoho intelektu v Ukrayini: prezentuyemo dorozhnyu kartu: Ministerstvo tsyfrovoyi transformatsiyi Ukrayiny, 07 zhovtnya 2023 r. URL: https://thedigital.gov.ua/news/technologies/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu (in Ukrainian).

24. Pro skhvalennya Kontseptsiyi Derzhavnoyi tsil'ovoyi naukovo-tekhnichnoyi prohramy z vykorystannya tekhnolohiy shtuchnoho intelektu v priorytetnykh haluzyakh ekonomiky na period do 2026 roku: Rozporyadzhennyam Kabinetu Ministriv Ukrayiny vid 13.04.2024 za № 320-r (vtratyla chynnist'). URL: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text (in Ukrainian).

25. Zvit pro doslidzhennya shtuchnoho intelektu, Internet rechey ta robototekhniky dlya bezpeky ta vidpovidal'nist'. Yevropeys'ka Komisiya. Bryussel', 19.02.2020. COM (2020) 64 ostatochna versiya. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064 (in Ukrainian).

26. Marina, M. Matić, Bošković. Implications of EU AI Regulation for criminal justice. Institute of Criminological and Sociological Research, Belgrade, Serbia. P. 111–120. URL: http://institutecsr.iksi.ac.rs/1040/1/08-Matic-Boskovic.pdf

27. Pro zatverdzhennya Rekomendatsiy z kiberzakhystu informatsiyno-komunikatsiynykh system, yaki zabezpechuyut' tekhnolohiyi shtuchnoho intelektu : Nakaz Administratsiyi Derzhspetszv'yazku vid 23.02.2026. № 154. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-23-02-2026-154-pro-zatverdzhennya-rekomendacii-z-kiberzakhistu-informaciino-komunikaciinikh-sistem-yaki-vikoristovuyut-tekhnologiyi-shtuchnogo-intelektu (in Ukrainian).

28. Balovsyak, N. Epokha oformlennya ilyuziy ta vidpovidnoho SHI: yakym bude 2026-y tekhnolohichnyy rik. Ukrayins'kyy Tyzhden'. 30 hrudnya 2025. URL: https://tyzhden.ua/epokha-pozbavlennia-iliuzij-ta-vidpovidalnoho-shi-iakym-bude-2026-j-tekhnolohichnyj-rik/ (in Ukrainian).

29. Zahal'nyy rehlament pro zakhyst danykh (GDPR). Ofitsiynyy pereklad ukrayins'koyu movoyu. URL: kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf, https://gdpr-text.com/uk/ (in Ukrainian).

30. Yavors'ka, O. S. Zakhyst personal'nykh danykh u tsyfrovomu seredovyshchi: dosvid YES. Yurydychnyy naukovyy elektronnyy zhurnal. № 9. 2024. S. 117–119. (in Ukrainian).

31. Pro zakhyst personal'nykh danykh. Proekt Zakonu vid 25.10.2022. № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (in Ukrainian).

32. Slobodyanyuk, Dmytro. Zakhyst personal'nykh danykh (GDPR / Dyrektyva YES): shcho zminyuyut' novi zakonoproyekty v Ukrayini. Yurydychna Hazeta. 13 zhovtnya 2025. URL: https://yur-gazeta.com/dumka-eksperta/zahist-personalnih-danih-gdpr--direktiva-es-shcho-zminyuyut-novi-zakonoproekti-v-ukrayini.html (in Ukrainian).

33. Commission Staff Working Document. Ukraine. Report. 2025 Communication on EU enlargement policy. Brussels, 4.11.2025. SWD (2025) 759 final. URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/EU-enlargement-.pdf

ОСОБИСТА БЕЗПЕКА ЯК ЧИННИК НАЦІОНАЛЬНОЇ БЕЗПЕКИ

PERSONAL SAFETY AS A PSYCHOPHYSICAL FACTOR OF NATIONAL SECURITY

Petryk D. P.,
Senior Lecturer Department of Special Physical Training,
Penitentiary Academy of Ukraine,
Chernihiv, Ukraine

Abstract. Subject of the study: The research focuses on the system of personal security for citizens, specifically university students and adults, as a fundamental component of the national security architecture. The study examines the psychophysical mechanisms of human response to threats and the methodology of forming sustainable readiness for safe behavior within modern social and educational environments. It explores the interaction between individual psychophysiological stability and state security stability. **Methodology:** The research is based on a multidisciplinary approach, integrating theories of national security, psychology of extreme situations, pedagogy, and physical education. The methodological framework includes a comprehensive theoretical analysis of scientific literature and legal acts. The synthesis of pedagogical experience and physiological modeling of stress responses were used to develop practical recommendations. Systemic analysis was applied to establish the link between individual victimhood and the general level of public safety. Empirical observation and comparative analysis of existing training practices for civilians were conducted to identify systemic errors

and optimization paths. **Purpose:** The purpose of the study is the scientific substantiation of personal security as a psychophysical factor of national security and the definition of the specific features of forming psychological readiness and basic psychophysical skills for safe behavior in students and adults under the conditions of modern security challenges. **Results:** The study establishes that in the face of modern hybrid threats, personal security is the primary element of national security. It is proved that state resilience directly correlates with the individual preparedness of each citizen. The author identifies that the key destructive factor in critical situations is unmanaged emotional stress, which leads to "cognitive narrowing" and motor dysfunction. Therefore, psychophysical readiness is defined as an integral characteristic combining situational awareness, emotional self-regulation, and controlled motor responses. The research substantiates that for the civilian population, the training model must prioritize prevention and de-escalation over physical confrontation. A significant result is the confirmation of the effectiveness of "simple motor models" based on gross motor skills, which remain reliable under high adrenaline pressure. These movements perform a "psychophysical grounding" function, stabilizing the heart rate and restoring a sense of subjective control. The study also systemizes typical errors in civilian training, such as the overestimation of physical strength and the neglect of psychological stability. **Conclusions:** The study concludes that forming psychophysical readiness is a continuous process of developing a safety culture. Integrating such training into the higher education system (specifically physical education) is a strategic tool for reducing victimhood and strengthening national security. The findings provide a scientific and practical basis for modernizing the civil protection system. The implementation of these results ensures sustainable social development by educating

responsible and protected individuals, which serves as a guarantee of Ukraine's national security in the long term.

Keywords: Personal Security, National Security, Individual Security, Public Interests, Human Rights Protection, Security Policy.

1. Вступ

У сучасних умовах розвитку українського суспільства проблема національної безпеки дедалі частіше розглядається не лише крізь призму військових, політичних або правових механізмів, а й через призму безпеки особистості. Зростання рівня соціальної напруги, поширення насильницьких злочинів, наслідки збройного конфлікту, міграційні процеси та урбанізація формують нове безпекове середовище, в якому кожен громадянин змушений самостійно приймати рішення щодо власної безпеки у повсякденному житті.

Особливо вразливою категорією у цьому контексті є студенти та повнолітні особи, які не мають спеціальної фізичної або силової підготовки, але щоденно стикаються з потенційно небезпечними ситуаціями у громадських місцях, транспорті, освітньому середовищі та побуті. Саме ця категорія населення найчастіше демонструє низький рівень психологічної готовності до дій у стресових умовах, що підвищує ризик віктимної поведінки та негативних наслідків для особистої і громадської безпеки.

У зв'язку з цим актуалізується необхідність наукового осмислення особистої безпеки громадян як складової національної безпеки держави. У сучасних наукових дослідженнях дедалі більше уваги приділяється психофізичним чинникам, що визначають здатність людини адекватно реагувати на загрози, зберігати самоконтроль, приймати раціональні рішення та здійснювати безпечні дії в умовах ризику. Психологічна готовність, рівень усвідомленості, стресостійкість та базові психофізичні навички стають важливими

елементами системи публічної безпеки поряд із правовими та організаційними механізмами.

Особиста безпека в даному дослідженні розглядається не як сукупність бойових або силових дій, а як комплекс психофізичних характеристик особистості, що забезпечують здатність запобігати небезпечним ситуаціям, знижувати рівень ризику та діяти відповідально у межах правового поля. Такий підхід є особливо важливим у роботі зі студентською молоддю та повнолітніми громадянами, для яких пріоритетом має бути не протистояння, а збереження життя, здоров'я та психологічної стабільності.

Метою даного дослідження є наукове обґрунтування особистої безпеки громадян як психофізичного чинника національної безпеки та визначення особливостей формування психологічної готовності й базових психофізичних навичок безпечної поведінки у студентів і повнолітніх осіб в умовах сучасних безпекових викликів.

Для досягнення поставленої мети у роботі використано загальнонаукові методи аналізу, синтезу та узагальнення наукових джерел, а також методи систематизації практичного досвіду психофізичної підготовки осіб без спеціальної силової підготовки. Логіка подання матеріалу передбачає послідовний перехід від теоретичного осмислення поняття особистої безпеки до аналізу психофізичних механізмів реагування на загрозу та узагальнення практичних підходів до формування культури безпеки у студентському та дорослому середовищі.

Наукова новизна дослідження полягає у розгляді особистої безпеки громадян як психофізичного чинника національної безпеки з акцентом на освітній та профілактичний потенціал психофізичної підготовки студентів і повнолітніх осіб. Практичне значення роботи полягає у можливості використання отриманих висновків у системі вищої освіти, програмах з фізичного виховання, громадянської та особистої безпеки, а також у профілактичній діяльності, спрямованій на зниження рівня насильства та формування відповідальної безпечної поведінки.

1.1. Поняття та зміст національної і публічної безпеки

У сучасній науковій думці національна безпека розглядається як складна багаторівнева система, що забезпечує захищеність життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз [1, с. 52]. Традиційно у центрі уваги досліджень перебували військові, політичні та економічні аспекти безпеки, однак упродовж останніх десятиліть відбувається суттєве розширення безпекової парадигми у бік людиноцентричного підходу. У межах цього підходу особистість розглядається не лише як об'єкт захисту, а і як активний суб'єкт системи національної безпеки, де людина, її життя і здоров'я визнаються найвищою соціальною цінністю [2, с. 3].

Публічна безпека є важливою складовою національної безпеки та охоплює сферу захищеності громадян у повсякденному соціальному просторі. Вона формується на перетині діяльності державних інституцій, місцевих громад та індивідуальної поведінки громадян, що вимагає трансформації правових механізмів її забезпечення [3, с. 124]. На відміну від суто державних механізмів безпеки, публічна безпека значною мірою залежить від рівня правової культури, соціальної відповідальності та здатності громадян адекватно діяти у потенційно небезпечних ситуаціях.

Варто зауважити, що в науковому дискурсі безпека розглядається не лише як відсутність загроз, а як динамічний стан захищеності життєво важливих інтересів особистості, суспільства та держави. У цьому контексті особиста безпека громадян виступає фундаментом національної безпеки, оскільки саме рівень захищеності та психофізичної готовності окремого індивіда визначає загальну стійкість соціуму до зовнішніх і внутрішніх викликів [1, с. 45].

У сучасних умовах публічна безпека дедалі частіше розглядається як динамічна система, що змінюється під впливом соціальних, психологічних та інформаційних чинників. Урбанізація, інтенсифікація соціальних контактів, зростання інформаційного

навантаження та загальний рівень стресу в суспільстві створюють нові виклики, які не можуть бути ефективно нейтралізовані виключно адміністративними або силовими засобами. У цьому контексті особливого значення набуває поведінковий та психофізичний аспект безпеки громадян.

Для студентів і повнолітніх осіб, які перебувають у процесі активної соціалізації або професійної реалізації, публічна безпека безпосередньо пов'язана з умінням орієнтуватися в соціальному середовищі, оцінювати рівень ризику та приймати відповідальні рішення у межах правового поля. Саме ця категорія населення найчастіше взаємодіє з відкритими публічними просторами, транспортною інфраструктурою та освітнім середовищем, що підвищує актуальність формування у них культури безпечної поведінки.

Таким чином, національна та публічна безпека перебувають у тісному взаємозв'язку, де ефективність державних і суспільних механізмів значною мірою визначається рівнем особистої безпеки громадян як фундаментального публічного інтересу [4, с. 47].

1.2. Особиста безпека в системі держави

Сучасний етап розбудови української державності характеризується переосмисленням ролі індивіда в системі захисту національних інтересів. Держава перестає бути єдиним монополістом у сфері безпеки, натомість формується модель партнерства, де особиста безпека громадянина є не лише об'єктом захисту, а й необхідною умовою стабільності всієї країни. Чинна Стратегія національної безпеки України чітко визначає найвищою цінністю людину, її життя, здоров'я, честь і гідність, що підтверджує перехід до моделі безпеки, орієнтованої на індивіда [5, с. 4].

У системі державних пріоритетів особиста безпека розглядається як багатогранне явище, що охоплює правові, соціальні та психологічні аспекти, а концепція «безпеки людини» (human security)

передбачає створення умов за яких громадянин відчуває захищеність не лише від фізичного насильства, а й має гарантії стабільності свого повсякденного життя, що є основою для його продуктивної діяльності [6, с. 88]. Таким чином, індивідуальний рівень безпеки стає індикатором ефективності роботи всього державного апарату.

У системі національної безпеки особиста безпека громадян виконує базову функцію, оскільки саме на рівні повсякденної життєдіяльності формується загальний рівень стійкості суспільства до кризових явищ. Низький рівень особистої безпеки окремих соціальних груп сприяє зростанню соціальної напруги, підвищенню рівня віктимності та ускладнює реалізацію державної політики у сфері публічної безпеки. Водночас сформована культура безпечної поведінки громадян здатна суттєво знизити навантаження на правоохоронні та соціальні інституції. Варто наголосити, що держава виступає головним гарантом особистої безпеки, створюючи відповідну правову базу та забезпечуючи функціонування інституцій, здатних оперативно реагувати на загрози інтересам приватних осіб [7, с. 115]. Проте в умовах гібридних загроз та воєнного стану особливого значення набуває здатність громадян до самозахисту та адекватної оцінки ризиків. Таким чином, інтеграція особистої безпеки в загальну систему державної безпеки вимагає не лише посилення правоохоронних функцій держави, а й активної підготовки самого населення до дій у небезпечних ситуаціях. Це створює підґрунтя для переходу до аналізу психофізичних механізмів, які визначають поведінку людини в момент безпосередньої загрози.

Особливого значення проблема особистої безпеки набуває у контексті студентської молоді та повнолітніх осіб, які перебувають у середовищі активної соціальної взаємодії. Освітні заклади, громадські простори, транспортна інфраструктура та цифрове середовище створюють широкий спектр потенційних ризиків, нейтралізація яких значною мірою залежить від рівня підготовленості

самих громадян. У цьому контексті особиста безпека виступає не лише індивідуальною потребою, а й соціально значущим ресурсом.

Особиста безпека громадян у даному дослідженні розглядається як комплексна система, що включає психологічну готовність до дій у стресових умовах, усвідомленість, здатність до самоконтролю та сформовані поведінкові моделі безпечної взаємодії з навколишнім середовищем. Такий підхід дозволяє відійти від вузького трактування безпеки як реакції на загрозу та зосередитися на превентивному аспекті, що є особливо актуальним для освітнього та соціального середовища.

Теоретичний аналіз дає змогу стверджувати, що особиста безпека громадян займає проміжне положення між публічною та національною безпекою, виконуючи функцію зв'язувальної ланки між індивідуальною поведінкою людини та загальнодержавними безпековими процесами. Саме через рівень особистої безпеки реалізується вплив психофізичних характеристик особистості на загальну стійкість системи безпеки держави.

Узагальнюючи викладене, можна стверджувати, що особиста безпека громадян є не вторинним, а структуроутворювальним елементом системи національної безпеки. Її формування потребує комплексного підходу, що поєднує державні механізми, освітні програми та розвиток психофізичної готовності особистості. Це створює підґрунтя для подальшого аналізу сучасних безпекових загроз та особливостей формування культури безпеки у студентів і повнолітніх осіб.

1.3. Сучасні загрози повсякденного життя

Трансформація безпекового середовища в Україні зумовила появу нових викликів, які мають комплексний та динамічний характер. Сучасні безпекові виклики характеризуються високим рівнем непередбачуваності та поєднанням прямих фізичних ризиків із потужним психологічним тиском на цивільне населення,

що вимагає розробки нових підходів до формування індивідуальної стійкості особистості [8, с. 210]. У межах повсякденної життєдіяльності громадян ці загрози вже не обмежуються лише кримінальними проявами чи техногенними аваріями, а охоплюють широкий спектр гібридних впливів.

На відміну від традиційних уявлень про безпеку, що зосереджувалися переважно на макрорівні державних ризиків, сучасні виклики дедалі частіше проявляються у звичних соціальних просторах — освітньому середовищі, громадських місцях, транспорті, сфері міжособистісної комунікації та цифровому просторі.

Для студентів і повнолітніх осіб характерною є висока інтенсивність соціальних контактів, мобільність та активне перебування у відкритому середовищі, що підвищує ймовірність потрапляння у потенційно небезпечні ситуації. При цьому значна частина ризиків не має яскраво вираженого кримінального характеру, а пов'язана з психологічною напругою, конфліктною взаємодією, інформаційним перевантаженням та недостатнім рівнем усвідомленості власної поведінки. Особливе місце серед чинників, що дестабілізують особисту безпеку, посідає хронічний стрес, спричинений тривалою воєнною агресією. Тривале перебування у стані безпекової невизначеності призводить до поступового виснаження адаптаційних ресурсів організму. Це безпосередньо впливає на психофізичний стан індивіда, знижуючи його здатність до швидкої, раціональної та адекватної реакції у разі виникнення безпосередньої небезпеки [9, с. 56]. Для студентської молоді цей аспект є критичним, оскільки психоемоційна нестабільність заважає ефективному засвоєнню навичок безпечної поведінки.

Однією з характерних ознак сучасних безпекових загроз є їхня латентність. Багато ризиків не сприймаються громадянами як безпосередня небезпека, що ускладнює своєчасну реакцію та підвищує рівень віктимності. Недостатня уважність до навколишнього

середовища, звичка ігнорувати сигнали небезпеки, а також переоцінка власних можливостей створюють умови для виникнення небажаних наслідків навіть у формально безпечних ситуаціях. Поряд із фізичними загрозами, значну частину ризиків для молоді становлять кіберзагрози та цілеспрямовані інформаційні маніпуляції. Такі впливи здатні не лише спричиняти фінансові втрати, а й дестабілізувати психоемоційний стан, провокуючи панічні настрої та дезорієнтацію, що суттєво змінює безпекову поведінку людини в реальному світі [10, с. 142].

Окремої уваги заслуговує вплив інформаційного середовища на сприйняття безпеки. Постійний потік новин, повідомлень та візуального контенту формує підвищений рівень тривожності або, навпаки, притуплює відчуття небезпеки. Для студентської молоді та дорослих осіб, які активно користуються цифровими технологіями, це створює додаткові психологічні навантаження, що впливають на здатність адекватно оцінювати ризики та приймати зважені рішення у реальних ситуаціях.

У контексті повсякденного життя важливою характеристикою сучасних загроз є їхня комплексність. Соціальні, психологічні та поведінкові чинники часто взаємодіють між собою, формуючи ситуації підвищеного ризику без явних зовнішніх ознак небезпеки. Саме тому ефективне забезпечення особистої безпеки не може обмежуватися лише знанням правил або зовнішнім контролем, а потребує розвитку внутрішніх механізмів саморегуляції та усвідомленої поведінки.

Таким чином, сучасні безпекові загрози у повсякденному житті громадян мають багатовимірний характер і потребують комплексного наукового осмислення. Усвідомлення специфіки цих загроз створює необхідні передумови для формування культури безпеки та переходу до аналізу особливостей підготовки студентів і повнолітніх осіб до безпечної поведінки, що розглядатиметься у наступному підрозділі.

1.4. Культура безпеки студентів та дорослих

Формування культури безпеки особистості в освітньому середовищі є складним багатогранним процесом, що виходить за межі простого засвоєння правил поведінки. Культура безпеки розглядається як інтегративна характеристика особистості, яка включає систему знань, переконань та практичних умінь, що забезпечують збереження життя і здоров'я у складних ситуаціях. Ефективне навчання базується на поєднанні теоретичних знань із системним практичним відпрацюванням поведінкових алгоритмів, що дозволяє перетворити знання на стійку навичку, яка спрацьовує автоматично в умовах стресу [11, с. 74].

Для студентської молоді та дорослих осіб процес формування цієї культури має свої особливості, зумовлені високим рівнем рефлексії та необхідністю усвідомленої мотивації. Ефективність засвоєння безпекових навичок дорослими особами безпосередньо залежить від рівня їхньої здатності до аналізу власного психофізичного стану в момент імітації загрози [12, с. 102]. Психологічна готовність виступає тут внутрішнім стрижнем, який дозволяє людині не піддатися паніці, а діяти раціонально, використовуючи раніше вивчені моделі поведінки.

Важливою особливістю формування культури безпеки у студентів і дорослих осіб є поєднання когнітивного, психологічного та поведінкового компонентів. Лише інформування про можливі ризики або правила безпечної поведінки не забезпечує стійкого результату. Ефективна культура безпеки передбачає розвиток усвідомленості, навичок саморегуляції, відповідального ставлення до власних дій та здатності приймати рішення в умовах невизначеності та стресу. Окрім індивідуального захисту, розвиток культури безпеки у студентської молоді має значний соціальний ефект. Сформована культура безпечної поведінки сприяє зниженню загального рівня соціальної напруги та формуванню безпечного публічного

простору через усвідомлення колективної відповідальності та готовності до надання взаємодопомоги [13, с. 89]. Таким чином, освіта у сфері безпеки стає інструментом не лише особистого захисту, а й зміцнення публічних інтересів держави.

У контексті освітнього середовища формування культури безпеки має інтегрований характер і реалізується через навчальні дисципліни, фізичне виховання, виховну роботу та неформальні освітні практики. Для студентської молоді особливо важливим є формування розуміння особистої безпеки не як обмеження свободи, а як інструменту збереження здоров'я, психічної рівноваги та соціальної ефективності. Для повнолітніх осіб культура безпеки пов'язана з відповідальністю за власне життя та безпеку інших членів суспільства.

Значну роль у формуванні культури безпеки відіграє психофізичний аспект підготовки. Психологічна готовність до дій у складних ситуаціях, здатність контролювати емоційні реакції та підтримувати функціональний психофізичний стан є важливими передумовами безпечної поведінки. Саме тому культура безпеки не може бути сформована без урахування індивідуальних психофізичних особливостей особистості, що є особливо актуальним для осіб без спеціальної підготовки.

Таким чином, формування культури безпеки у студентів і повнолітніх осіб є багатовимірним процесом, що потребує комплексного підходу та наукового обґрунтування. Усвідомлення ролі психофізичних чинників у забезпеченні особистої безпеки створює логічне підґрунтя для подальшого аналізу психологічних і психофізичних механізмів реагування людини на загрозу, що становить предмет дослідження наступного розділу.

Висновки до Розділу 1

1. Встановлено, що особиста безпека громадян є фундаментальною складовою системи національної безпеки держави. Вона визначає рівень захищеності національних інтересів через стан

безпеки кожного окремого члена суспільства в умовах повсякденної життєдіяльності.

2. Визначено, що освітнє середовище та повсякденне життя виступають основними сферами формування культури безпеки. Це актуалізує необхідність розроблення інтегрованих підходів до підготовки студентів та дорослого населення.

3. Обґрунтовано поняття віктимності як чинника, що знижує рівень національної безпеки. Доведено, що цілеспрямована підготовка у сфері особистої безпеки є дієвим інструментом профілактики насильства та соціальної дестабілізації.

Список використаних джерел:

1. Ліпкан В. А. Національна безпека України: навчальний посібник. Київ: Кондор, 2008. 552 с.

2. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 18.02.2026).

3. Чижов Д. Правові засади розуміння прав людини у сфері національної безпеки України. *Baltic Journal of Legal and Social Sciences*. 2022. № 2. С. 122–128.

4. Сипріян В. О. Теоретико-правові засади національної безпеки України. *Юридичний науковий електронний журнал*. 2021. № 5. С. 46–49.

5. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 18.02.2026).

6. Резнікова О. О. Стратегічне планування у сфері національної безпеки: методологія та практика. Київ : НІСД, 2020. 252 с.

7. Когут Ю. І. Державне управління у сфері забезпечення національної безпеки України. Київ : СидКон, 2021. 340 с.

8. Горбулін В. П. Як перемогти Росію у війні майбутнього. Київ : Брайт Букс, 2022. 256 с.

9. Осадько О. Ю. Психологія життєстійкості особистості в умовах війни. *Науковий вісник Ужгородського національного університету. Серія: Психологія*. 2023. Вип. 77. С. 54–59.

10. Петрик В. В. Інформаційна безпека України у сучасних умовах : навч. посіб. Київ : КНТ, 2021. 280 с.

11. Вачевський М. В. Педагогічні основи формування культури безпеки життєдіяльності. *Педагогіка і психологія професійної освіти*. 2020. № 1. С. 70–78.

12. Кузнєцов О. В. Психологія безпеки особистості : навч. посіб. Київ : КНТ, 2021. 232 с.

13. Гевко Б. Р. Соціально-педагогічні аспекти формування безпечної поведінки молоді. *Інноваційна педагогіка*. 2022. Вип. 45. С. 87–91.

References:

1. Lipkan V. A. (2008). National security of Ukraine. Kyiv: Kondor. 552 p. (in Ukrainian).

2. Constitution of Ukraine. (1996). URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (in Ukrainian).

3. Chyzhov D. (2022). Legal basis of understanding human rights in the field of national security of Ukraine. *Baltic Journal of Legal and Social Sciences*, no. 2, pp. 122–128.

4. Sypriian V. O. (2021). Theoretical and legal foundations of national security of Ukraine. *Yurydychnyi naukovyi elektronnyi zhurnal*, no. 5, pp. 46–49. (in Ukrainian).

5. President of Ukraine (2020). On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine". Decree no. 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (in Ukrainian).

6. Reznikova O. O. (2020). Stratehichne planuvannia u sferi natsionalnoi bezpeky: metodolohiia ta praktyka [Strategic planning in the field of national security: methodology and practice]. Kyiv: NISD. 252 p. (in Ukrainian).

7. Kohut Yu. I. (2021). State administration in the field of ensuring national security of Ukraine. Kyiv: SydKon. 340 p. (in Ukrainian)

8. Horbulin V. P. (2022). How to defeat Russia in the war of the future. Kyiv: Bright Books. 256 p. (in Ukrainian).

9. Osadko O. Yu. (2023). Psychology of individual resilience in war conditions. *Scientific Bulletin of Uzhhorod National University. Series: Psychology*, no. 77, pp. 54–59. (in Ukrainian).

10. Petryk V. V. (2021). Information security of Ukraine in modern conditions. Kyiv: KNT. 280 p. (in Ukrainian).

11. Vachevskyi M. V. (2020). Pedagogical foundations of forming a culture of life safety. *Pedagogy and Psychology of Vocational Education*, no. 1, pp. 70–78. (in Ukrainian).

12. Kuznietsov O. V. (2021). Psychology of personal safety. Kyiv: KNT. 232 p. (in Ukrainian).

13. Hevko B. R. (2022). Socio-pedagogical aspects of forming safe behavior of youth. *Innovative Pedagogy*, no. 45, pp. 87–91. (in Ukrainian).

2. Психологічні реакції людини в умовах небезпеки

Реагування людини на ситуацію загрози є складним психологічним процесом, що відбувається в умовах дефіциту часу, інформації та підвищеного емоційного напруження. Страх у ситуації небезпеки може виконувати як адаптивну, так і дезадаптивну функцію. За умови помірної інтенсивності він сприяє підвищенню уваги, мобілізації ресурсів організму та швидкому прийняттю рішень [14, с. 42]. Водночас надмірний рівень страху призводить до порушення когнітивних процесів, зниження здатності до аналізу ситуації та виникнення станів ступору або хаотичної поведінки.

Однією з типових психологічних реакцій на загрозу є «тунельний зір» або звуження свідомості, що проявляється у фокусуванні уваги на одному стимулі та ігноруванні інших важливих факторів

ситуації. Такий стан ускладнює просторову орієнтацію та знижує здатність до прогнозування подальшого розвитку подій [15, с. 95].

Для студентів і повнолітніх осіб, які не мають спеціальної підготовки, характерною є тенденція до автоматичних реакцій, що формуються під впливом життєвого досвіду та соціальних установок. У таких умовах рішення часто приймаються неусвідомлено, а поведінка визначається домінуючими емоціями, а не раціональною оцінкою ризиків. Це підкреслює критичну необхідність формування навичок саморегуляції, що дозволяють зберігати адекватність сприйняття навіть в умовах раптової небезпеки [16, с. 118].

Однією з типових психологічних реакцій на загрозу є звуження свідомості, що проявляється у фокусуванні уваги на одному стимулі та ігноруванні інших факторів ситуації. Такий стан ускладнює просторову орієнтацію та знижує здатність до прогнозування подальшого розвитку подій. У контексті особистої безпеки це підкреслює важливість формування навичок усвідомленого сприйняття та психологічної готовності до дій у стресових умовах.

Таким чином, психологічні реакції людини в умовах небезпеки є ключовим чинником, що визначає ефективність або неефективність поведінки у критичній ситуації. Усвідомлення закономірностей цих реакцій створює основу для подальшого аналізу когнітивних і психофізичних механізмів реагування на загрозу та обґрунтовує необхідність цілеспрямованої підготовки студентів і повнолітніх осіб у сфері особистої безпеки.

2.1. Когнітивні та поведінкові механізми оцінки загрози

Когнітивна оцінка ситуації є центральною ланкою у процесі реагування людини на загрозу. Саме на цьому етапі відбувається інтерпретація зовнішніх сигналів, формування уявлення про рівень небезпеки та вибір подальшої моделі поведінки [17, с. 112].

Когнітивні механізми реагування на загрозу тісно пов'язані з індивідуальним досвідом. Студенти й повнолітні особи часто покладаються на автоматизовані поведінкові шаблони («система 1» за термінологією когнітивістики), які не завжди є адекватними в умовах небезпеки. У таких ситуаціях рішення приймаються інтуїтивно, без повноцінного аналізу, що суттєво знижує ефективність безпечної поведінки [18, с. 64].

Однією з ключових характеристик когнітивного реагування на загрозу є здатність до ситуаційної оцінки, яка включає усвідомлення просторових умов та можливих варіантів дій. Порушення цього процесу проявляється у звуженні поля уваги або у загальній дезорієнтації, що призводить до імпульсивних або пасивних дій [19, с. 145].

Поведінкові механізми реагування формуються як результат взаємодії когнітивних процесів та емоційного стану особистості. У контексті особистої безпеки поведінка людини часто визначається не раціональним вибором, а домінуючою емоційною реакцією. Відсутність навичок усвідомленої саморегуляції призводить до імпульсивних або пасивних дій, що знижує здатність до ефективного уникнення небезпеки.

Для студентів і повнолітніх осіб важливим чинником є сформованість відповідальної поведінки, що ґрунтується на розумінні власних можливостей та обмежень. Усвідомлення того, що безпека починається з правильного сприйняття ситуації та прийняття зважених рішень, є передумовою зниження рівня віктимності та підвищення ефективності особистої безпеки.

Таким чином, когнітивні та поведінкові механізми оцінки загрози відіграють визначальну роль у формуванні безпечної поведінки. Розвиток усвідомленості, навичок ситуаційного аналізу та контролю власних реакцій є необхідною умовою підготовки студентів і повнолітніх осіб до дій у потенційно небезпечних умовах. Це створює

логічне підґрунтя для подальшого аналізу психофізіологічних змін і ролі рухової активності у процесі реагування на загрозу.

2.2. Психофізіологічні зміни та роль рухової активності у ситуації загрози

Реагування людини на ситуацію загрози супроводжується комплексом психофізіологічних змін, що охоплюють нервову, м'язову та серцево-судинну системи. Ці зміни мають адаптивний характер і спрямовані на мобілізацію ресурсів організму, проте за умови відсутності спеціальної підготовки вони призводять до дезорганізації поведінки та порушення функціонального стану [20, с. 156].

У стресових умовах відбувається різке підвищення м'язового тонусу, що змінює звичну рухову організацію людини. Для студентів і повнолітніх осіб без системної психофізичної підготовки надмірна м'язова напруга стає чинником, що обмежує амплітуду рухів, знижує точність дій та суттєво ускладнює просторову орієнтацію [21, с. 78].

Водночас рухова активність у ситуації загрози виконує важливу регуляторну функцію. Рух сприяє зниженню надлишкової психоемоційної напруги, відновленню контролю над тілом та поверненню відчуття керованості власним станом. З позицій психофізіології навіть прості, усвідомлені рухи здатні стабілізувати стан нервової системи та підвищити ефективність подальших рішень.

Особливого значення у контексті особистої безпеки набуває координація рухів і здатність підтримувати функціональний психофізичний стан в умовах стресу. Порушення координації, характерні для станів сильного емоційного збудження, знижують здатність людини адекватно взаємодіяти з навколишнім середовищем. Формування навичок базової рухової стабільності та усвідомленого контролю тіла є важливим чинником підвищення рівня особистої безпеки.

Дихання виступає одним із ключових механізмів регуляції психофізіологічного стану. У стресових ситуаціях спостерігається

тенденція до поверхневого та прискореного дихання, що посилює відчуття тривоги. Усвідомлене регулювання дихального ритму сприяє зниженню психоемоційного напруження та відновленню контролю над рухами, що має критичне значення для прийняття зважених рішень [22, с. 92].

Таким чином, психофізіологічні зміни в умовах загрози виступають природною реакцією організму на стрес. Ефективність особистої безпеки значною мірою залежить від здатності людини використовувати рухову активність і регуляцію дихання як засоби стабілізації стану. Це обґрунтовує необхідність формування психофізичної готовності як складової культури безпеки.

2.3. Формування психофізичної готовності студентів і повнолітніх осіб до дій у небезпечних ситуаціях

Психофізична готовність є інтегральною характеристикою особистості, що відображає здатність людини зберігати функціональний стан в умовах стресу. У контексті особистої безпеки вона визначає ефективність реагування на потенційні загрози та безпосередньо впливає на характер поведінки у критичних ситуаціях [23, с. 142].

Для студентів і повнолітніх осіб, які не мають спеціальної підготовки у сфері безпеки, формування психофізичної готовності набуває особливого значення. Саме ця категорія громадян найчастіше стикається з небезпечними або конфліктними ситуаціями у повсякденному житті, при цьому не володіючи достатніми навичками саморегуляції та контролю психофізичного стану. У таких умовах вирішальним чинником стає не рівень фізичної сили, а здатність зберігати ясність мислення, керованість рухів і емоційну стабільність.

Формування психофізичної готовності доцільно розглядати як поетапний процес, що поєднує розвиток психологічної усвідомленості, навичок саморегуляції та базових рухових умінь.

Усвідомленість дозволяє своєчасно розпізнавати зміни власного стану, сигнали зовнішнього середовища та рівень загрози. Саме на цьому рівні закладається здатність до адекватної когнітивної оцінки ситуації та прийняття зважених рішень.

Важливим компонентом психофізичної готовності є здатність до регуляції психоемоційного стану через дихання та рухову активність. Усвідомлене дихання і прості рухові дії сприяють зниженню надмірного м'язового напруження, відновленню координації та поверненню відчуття контролю над тілом. Для осіб без спеціальної підготовки такі засоби є доступними, безпечними та ефективними у повсякденних умовах.

Особливе місце у формуванні такої готовності займає принцип простоти та мінімізації складності дій. В умовах високого психоемоційного напруження складні рухові або поведінкові алгоритми втрачають ефективність, оскільки потребують надмірної концентрації. Натомість базові, зрозумілі дії забезпечують вищий рівень надійності та передбачуваності поведінки людини [24, с. 56].

Формування психофізичної готовності студентів і дорослих осіб доцільно реалізовувати у межах освітніх програм та міждисциплінарних курсів. У цьому контексті підготовка виступає не як навчання силових дій, а як засіб підвищення рівня усвідомленої, відповідальної та безпечної поведінки, що дозволяє суттєво знизити рівень віктимності особистості [25, с. 215].

Психофізична готовність у контексті особистої безпеки доцільно розглядати не лише як характеристику цивільної поведінки, а як універсальну основу реагування людини на ситуації підвищеного ризику. Незалежно від соціального статусу чи професійної належності, механізми психофізіологічної реакції на загрозу мають спільні закономірності, що визначають ефективність подальших дій.

Умови невизначеності, дефіциту часу та підвищеного емоційного напруження активізують типові реакції організму, пов'язані

з мобілізацією ресурсів нервової та м'язової систем. За відсутності сформованої психофізичної готовності такі реакції можуть набувати дезорганізуючого характеру, що проявляється у втраті координації, звуженні уваги та зниженні здатності до прийняття зважених рішень.

З огляду на це психофізична готовність виступає базовим чинником безпеки, який поєднує усвідомлення ситуації, контроль психоемоційного стану та здатність до керування власними руховими діями. У цивільному середовищі вона забезпечує зниження рівня віктимності та підвищення адаптивності поведінки, тоді як у професійній діяльності — створює передумови для ефективного виконання функціональних завдань в умовах підвищеного ризику.

Таким чином, формування психофізичної готовності є складним багаторівневим процесом, що дозволяє не лише стабілізувати стан особистості в момент загрози, а й системно знизити рівень її віктимності через виховання впевненості та керованості поведінки. Саме цей теоретичний фундамент стає базою для розробки практичних методик підготовки, що розглядаються у наступному розділі.

Висновки до Розділу 2

1. Досліджено психофізіологічні механізми реагування на загрозу, де ключовим деструктивним фактором визначено некерований емоційний стрес та страх. З'ясовано, що без спеціальної підготовки ці стани призводять до дезорганізації рухової активності та когнітивного звуження.

2. Обґрунтовано роль ситуаційної уважності та когнітивної оцінки ризиків як базису безпечної поведінки. Встановлено, що здатність до швидкого аналізу обставин дозволяє приймати ефективні рішення ще до переходу ситуації у фазу фізичного зіткнення.

3. Визначено психофізичну готовність як інтегральну характеристику особистості, що поєднує психологічну стійкість, здатність до саморегуляції через дихання та контроль м'язового тонусу.

Список використаних джерел:

1. Плющ С. М. Психологія безпеки та ризику : навч. посіб. Київ : КНУ імені Тараса Шевченка, 2021. 190 с.

2. Корольчук М. С., Крайнюк В. М. Психологія стресостійкості особистості : монографія. Київ : Ніка-Центр, 2019. 516 с.

3. Блінов О. А. Психологія бойової психічної травми : монографія. Київ : Талком, 2020. 254 с.

4. Савченко О. В. Психологія когнітивного оцінювання стресових подій. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Психологія*. 2021. Вип. 70. С. 110–116.

5. Канеман Д. Мислення швидке й повільне / пер. з англ. М. Яковлєв. Київ : Наш Формат, 2017. 480 с.

6. Тімченко О. В. Синдром посттравматичного стресу: психологічні аспекти : монографія. Харків : Вид-во НУЦЗУ, 2019. 210 с.

7. Макаренко М. В., Лизогуб В. С. Психофізіологічні основи професійного відбору та адаптації фахівців. Київ : Черкаси, 2011. 464 с.

8. Мунтян В. С. Психофізична підготовка студентів у системі вищої освіти: монографія. Харків : ХНПУ, 2020. 185 с.

9. Оськіна В. О. Психофізіологічні методи саморегуляції в екстремальних умовах. *Науковий часопис НПУ імені М. П. Драгоманова*. 2019. Вип. 11. С. 89–95.

10. Оніщенко Н. В. Психологічна готовність до дій в екстремальних ситуаціях: теорія та практика. Київ : Освіта України, 2021. 284 с.

11. Осьодло В. І. Психологія професійного становлення особистості у складних умовах життєдіяльності: монографія. Київ : Золоті ворота, 2019. 312 с.

12. Бойчук Ю. Д. Безпека життєдіяльності: формування культури безпеки молоді: навч. посіб. Харків : ХНПУ, 2022. 320 с.

References:

1. Pliushch S. M. (2021). Psychology of security and risk. Kyiv: Taras Shevchenko National University of Kyiv. 190 p. (in Ukrainian).

2. Korolchuk M. S., Krainiuk V. M. (2019). Psychology of individual stress resistance. Kyiv: Nika-Tsentr. 516 p. (in Ukrainian).

3. Blinov O. A. (2020). Psychology of combat psychic trauma. Kyiv : Talkom. 254 p. (in Ukrainian).

4. Savchenko O. V. (2021). Psychology of cognitive assessment of stressful events. *The Journal of V. N. Karazin Kharkiv National University. A Series of Psychology*, no. 70, pp. 110–116. (in Ukrainian).

5. Kahneman D. (2017). Thinking, Fast and Slow. Trans. M. Yakovliev. Kyiv: Nash Format. 480 p. (in Ukrainian).

6. Timchenko O. V. (2019). Post-traumatic stress syndrome: psychological aspects. Kharkiv: NUTSZU. 210 p. (in Ukrainian).

7. Makarenko M. V., Lyzohub V. S. (2011). Psychophysiological foundations of professional selection and adaptation of specialists. Kyiv: Cherkasy. 464 p. (in Ukrainian).

8. Muntian V. S. (2020). Psychophysical training of students in the higher education system. Kharkiv: KhNPU. 185 p. (in Ukrainian).

9. Oskina V. O. (2019). Psychophysiological methods of self-regulation in extreme conditions. *Scientific Journal of NPU named after M. P. Drahomanov*, no. 11, pp. 89–95. (in Ukrainian).

10. Onishchenko N. V. (2021). Psychological readiness for actions in extreme situations: theory and practice. Kyiv: Osvita Ukrainy. 284 p. (in Ukrainian).

11. Osodlo V. I. (2019). Psychology of professional development of personality in difficult life conditions. Kyiv: Zoloti vorota. 312 p. (in Ukrainian).

12. Boichuk Yu. D. (2022). Life safety: forming the safety culture of youth. Kharkiv: KhNPU. 320 p. (in Ukrainian).

3. Особливості практичної підготовки студентів та дорослих

Практична підготовка у сфері особистої безпеки студентів і повнолітніх осіб має низку специфічних особливостей, зумовлених

віковими, соціальними та психофізичними характеристиками цієї цільової аудиторії. На відміну від професійних груп, діяльність яких пов'язана з підвищеним рівнем ризику, цивільні особи зазвичай не мають системної підготовки до дій у небезпечних ситуаціях і не володіють стійкими навичками психофізичної саморегуляції.

Однією з ключових особливостей такої підготовки є її профілактичний характер. Метою роботи є не формування навичок протидії, а розвиток здатності розпізнавати загрози та підтримувати контроль над власним станом у стресових умовах [26, с. 210].

Практичний досвід свідчить, що значна частина труднощів у засвоєнні матеріалу пов'язана з психологічними бар'єрами: страхом, соціальними стереотипами та хибними уявленнями про безпеку. Це зумовлює необхідність поєднання фізичних вправ із корекцією поведінкових установок [27, с. 45].

Важливою умовою ефективності є адаптованість підготовки до реальних умов повсякденного життя. Пріоритет надається універсальним підходам, які можуть бути легко інтегровані у систему фізичного виховання та неформальної освіти без спеціального обладнання [28, с. 115]. Саме тому у практичній роботі зі студентами і дорослими особами пріоритет надається простим, універсальним і безпечним підходам, які можуть бути інтегровані у систему фізичного виховання та неформальної освіти.

Таким чином, практична підготовка студентів і повнолітніх осіб у сфері особистої безпеки має будуватися на принципах профілактики, усвідомленості та психофізичної доступності. Узагальнення цього досвіду створює основу для визначення принципів побудови занять з психофізичної підготовки, які будуть розглянуті у наступному підрозділі.

3.1. Принципи побудови занять з психофізичної підготовки

Побудова занять з психофізичної підготовки студентів і повнолітніх осіб у сфері особистої безпеки потребує дотримання низки

принципів, що забезпечують ефективність, безпечність та практичну доцільність освітнього процесу. Першим базовим принципом є принцип усвідомленості. Психофізична підготовка передбачає не механічне виконання рухових дій, а формування здатності розуміти власний стан, відчувати напругу та своєчасно її регулювати [29, с. 134]. Усвідомленість забезпечує інтеграцію психологічних і фізичних компонентів підготовки та створює основу для адекватної поведінки у стресових ситуаціях.

Другим принципом є принцип простоти та доступності. Практичний досвід свідчить, що у ситуаціях психоемоційного напруження ефективними залишаються лише ті дії, які є простими за структурою та не потребують складної координації. Саме тому заняття мають ґрунтуватися на базових рухових моделях, доступних для осіб без спеціального обладнання [30, с. 88].

Важливе значення має принцип функціональної доцільності рухів. Рухові дії мають відповідати реальним умовам повсякденного життя та бути спрямованими на підтримання рівноваги, просторової орієнтації та загальної координації. Такий підхід сприяє перенесенню сформованих навичок у реальні ситуації потенційної небезпеки.

Принцип поступовості та адаптації передбачає поетапне ускладнення психофізичних навантажень з урахуванням індивідуальних можливостей учасників. Надмірне або передчасне ускладнення завдань може призводити до зростання тривожності та зниження мотивації, що негативно впливає на формування психофізичної готовності. Адаптація змісту занять дозволяє забезпечити стійкий і безпечний розвиток необхідних навичок.

Принцип безпечності та контролю навантаження є визначальним у роботі зі студентами та повнолітніми особами. Заняття з психофізичної підготовки не повинні створювати додаткових ризиків для здоров'я або провокувати надмірне психоемоційне напруження. Контроль інтенсивності та тривалості навантажень

забезпечує позитивний адаптаційний ефект і сприяє формуванню довіри до навчального процесу.

Завершальним є принцип інтеграції у систему фізичного виховання та освіти. Така інтеграція дозволяє формувати культуру безпеки як складову загальної культури рухової активності та здорового способу життя [31, с. 52].

Таким чином, дотримання зазначених принципів створює методологічну основу для ефективної підготовки. Вони забезпечують узгодженість між теоретичними положеннями та практичним досвідом, що є умовою формування стійкої та усвідомленої безпечної поведінки.

3.2. Роль простих рухових моделей у формуванні безпечної поведінки

Рухова активність є одним із базових механізмів адаптації людини до змін умов середовища, зокрема до ситуацій потенційної небезпеки. У контексті особистої безпеки рух розглядається не як інструмент силового впливу, а як засіб підтримання психофізичної стабільності, просторової орієнтації та керованості поведінки.

Практичний досвід підготовки студентів і повнолітніх осіб свідчить, що у стресових ситуаціях ефективними залишаються лише прості рухові моделі, які не потребують складної координації. Наукові дослідження підтверджують, що під впливом адреналіну відбувається блокування дрібної моторики, тому лише великомоторні, природні рухи зберігають свою функціональність [32, с. 74]. Складні рухи в умовах емоційного напруження часто втрачають керованість, що призводить до дезорганізації поведінки.

Прості рухові моделі виконують стабілізуючу функцію, оскільки сприяють збереженню рівноваги та відчуття опори. Вони дозволяють людині швидше адаптуватися до змін обстановки, знижують рівень м'язового напруження. З позицій психофізіології, ритмічні

та контрольовані рухи сприяють відновленню балансу між процесами збудження і гальмування в корі головного мозку, що підвищує загальну стійкість до стресу [33, с. 112].

Важливою характеристикою простих рухових моделей є їхня універсальність. Саме можливість перенесення сформованих рухових навичок із навчального середовища у реальні умови повсякденного життя визначає цінність підготовки. Успішна реалізація таких моделей базується на створенні стійких динамічних стереотипів, які спрацьовують автоматично навіть за умови значного когнітивного звуження [34, с. 82].

З позицій психофізіології прості рухові дії сприяють зниженню надмірної активації нервової системи та відновленню балансу між збудженням і гальмуванням. Ритмічні та контрольовані рухи позитивно впливають на дихальний ритм і серцево-судинну діяльність, що у сукупності підвищує рівень психофізичної стійкості людини.

У процесі формування безпечної поведінки прості рухові дії створюють базу для усвідомленого керування власним тілом. Саме через них формується відчуття контролю та впевненості у власних діях, що є критично важливим для зниження рівня віктимності.

Аналіз практичного досвіду підготовки у сфері особистої безпеки підтверджує, що надійність дій людини в умовах стресу безпосередньо пов'язана з простотою та функціональною доцільністю використовуваних рухових моделей. У ситуаціях психоемоційного напруження організм схильний до спрощення рухової активності, що обумовлює перевагу базових, добре засвоєних рухів над складними координаційними діями.

Прості рухові моделі характеризуються високим рівнем відтворюваності, стабільності та керованості, що дозволяє зберігати контроль над тілом навіть за умов часткового порушення уваги або підвищеного рівня збудження нервової системи. Саме ці властивості роблять їх ефективним інструментом як у цивільних ситуаціях

потенційної небезпеки, так і в діяльності, пов'язаній із підвищеними фізичними та психологічними навантаженнями.

Використання простих рухових моделей сприяє формуванню відчуття опори, стабільності та передбачуваності власних дій, що має важливе значення для зниження рівня тривожності та підвищення впевненості у поведінці. У професійному контексті це дозволяє мінімізувати вплив стресових чинників на якість виконання функціональних завдань і зменшити ймовірність помилок у критичних ситуаціях.

Отже, орієнтація на прості рухові моделі є методологічно обґрунтованим підходом до підготовки як цивільних осіб, так і фахівців силових та безпекових структур, діяльність яких потребує високого рівня психофізичної надійності. Таким чином, використання простих рухових моделей у психофізичній підготовці студентів і повнолітніх осіб є обґрунтованим підходом, що забезпечує доступність та ефективність формування навичок безпечної поведінки у потенційно небезпечних ситуаціях.

3.3. Аналіз практичного досвіду та типових помилок у підготовці до дій у небезпечних ситуаціях

Незважаючи на науково обґрунтовану доцільність використання простих рухових моделей, реальна практика підготовки студентів і повнолітніх осіб часто стикається із низкою деструктивних чинників та методичних прорахунків. Аналіз практичного досвіду свідчить, що ефективність навчального процесу значною мірою залежить не лише від змісту занять, а й від здатності розпізнавати та усувати типові помилки, які часто мають системний характер і пов'язані з неправильним розумінням сутності особистої безпеки, способами подання матеріалу та сформованими очікуваннями учасників.

Однією з найбільш поширених помилок є переоцінка значення фізичної сили та окремих технічних дій. У свідомості багатьох студентів і дорослих осіб безпека ототожнюється суто з умінням

застосовувати силові прийоми, що не відповідає реальним умовам повсякденного життя. Такий підхід ігнорує психологічні та психофізичні чинники реагування на загрозу і може створювати хибне відчуття захищеності.

Іншою типовою проблемою є недооцінка ролі психоемоційного стану у критичних ситуаціях. У процесі підготовки часто зосереджуються на зовнішніх аспектах поведінки, залишаючи поза увагою внутрішні реакції людини на стрес. Відсутність навичок саморегуляції призводить до того, що навіть добре засвоєний матеріал не реалізується у ситуації реальної загрози.

Практичний досвід також виявляє помилки, пов'язані з надмірною складністю навчального матеріалу. Складні рухові моделі, багатокомпонентні алгоритми дій та перевантаження інформацією знижують рівень засвоєння та ефективність підготовки. В умовах стресу такі моделі не відтворюються або реалізуються фрагментарно, що підвищує ризик неадекватної поведінки.

Ще одним проблемним аспектом є ігнорування індивідуальних відмінностей учасників підготовки. Різний рівень фізичної підготовленості, попередній досвід, психологічні особливості та мотивація потребують диференційованого підходу. Уніфіковані програми без урахування цих чинників знижують ефективність формування психофізичної готовності.

Водночас узагальнення позитивного практичного досвіду свідчить, що найбільш ефективними є підходи, орієнтовані на розвиток усвідомленості, простоти дій та реалістичності сценаріїв. Навчальний процес, побудований на принципах безпечності, доступності та поступовості, сприяє формуванню стійких моделей поведінки та зниженню рівня тривожності у потенційно небезпечних ситуаціях.

Таким чином, аналіз типових помилок у підготовці студентів і повнолітніх осіб дозволяє визначити ключові напрями підвищення ефективності формування навичок особистої безпеки. Усунення

зазначених недоліків сприяє розвитку психофізичної готовності, підвищенню рівня усвідомленої поведінки та формуванню культури безпеки у повсякденному житті.

Висновки до Розділу 3

1. Охарактеризовано принципи практичної підготовки, де пріоритет надається профілактиці, простоті та функціональній доцільності дій. Встановлено, що для цивільних осіб найбільш ефективною є стратегія уникнення конфлікту та деескалації.

2. Доведено перевагу простих рухових моделей над складними технічними діями в умовах високого рівня стресу. Прості рухи на базі великої моторики є надійнішими та легше відтворюються непідготовленими особами.

3. Систематизовано типові помилки у навчанні безпеці, зокрема переоцінку фізичної сили та ігнорування психологічного аспекту. Обґрунтовано доцільність інтеграції такої підготовки в систему фізичного виховання закладів вищої освіти.

Список використаних джерел:

1. Коцан І. Я. Психофізіологічні та методичні аспекти безпеки життєдіяльності: монографія. Луцьк : Вежа-Друк, 2020. 340 с.

2. Маляр Е. І. Педагогічні умови формування готовності студентів до самозахисту в екстремальних ситуаціях. *Інноваційна педагогіка*. 2021. Вип. 32. Т. 2. С. 43–47.

3. Пилипко О. О. Організація самостійних занять студентів з фізичного виховання та безпеки життєдіяльності. Харків : ХДАФК, 2019. 160 с.

4. Петровський В. В. Психофізичне виховання молоді: методичні засади. Київ : Олімпійська література, 2020. 215 с.

5. Гітін В. Г. Психофізична підготовка людини до екстремальних умов. Харків : Торсінг, 2019. 192 с.

6. Зайцев В. П. Педагогіка безпеки: формування навичок самозахисту в системі вищої освіти. *Теорія та методика фізичного виховання*. 2022. № 1. С. 50–57.

7. Петров М. П. Алгоритми безпечної поведінки в міському середовищі: психолого-педагогічний аспект. Київ : Фенікс, 2021. 140 с.

8. Сидоров Ю. В. Методика проведення тренінгів з особистої безпеки для цивільних осіб. Львів : Світ, 2022. 180 с.

9. Яковенко С. І. Психологія безпеки особистості: теорія та практика. Київ : Видавничий дім «Слово», 2020. 232 с.

References:

1. Kotsan, I. Ya. (2020). Psychophysiological and methodical aspects of life safety. Lutsk: Vezha-Druk. 340 p. (in Ukrainian).

2. Maliar, E. I. (2021). Pedagogical conditions for forming students' readiness for self-defense in extreme situations. *Innovative Pedagogy*, no. 32, pp. 43–47. (in Ukrainian).

3. Pylypko, O. O. (2019). Organization of independent classes for students on physical education and life safety. Kharkiv: KhDAFK. 160 p. (in Ukrainian).

4. Petrovskyi, V. V. (2020). Psychophysical education of youth: methodological foundations. Kyiv: Olimpiiska literatura. 215 p. (in Ukrainian).

5. Hitin, V. H. (2019). Psychophysical training of a person for extreme conditions. Kharkiv: Torsinh. 192 p. (in Ukrainian).

6. Zaitsev, V. P. (2022). Safety pedagogy: formation of self-defense skills in the higher education system. Theory and Methodology of Physical Education, no. 1, pp. 50–57. (in Ukrainian).

7. Petrov, M. P. (2021). Safe behavior algorithms in the urban environment: psychological and pedagogical aspect. Kyiv: Feniks. 140 p. (in Ukrainian).

8. Sydorov, Yu. V. (2022). Methodology of conducting personal safety trainings for civilians. Lviv: Svit. 180 p. (in Ukrainian).

9. Yakovenko, S. I. (2020). Psykholohiia bezpeky osobystosti: teoriia ta praktyka [Psychology of personal security: theory and practice]. Kyiv: Slovo. 232 p. (in Ukrainian).

3. Висновки

1. Аргументовано, що в умовах сучасних глобальних та гібридних загроз особиста безпека людини виступає первинною та невід'ємною ланкою в загальній архітектурі національної безпеки. Встановлено, що загальний стан захищеності національних інтересів безпосередньо корелює із індивідуальною підготовленістю кожного громадянина. Доведено, що формування культури безпечної життєдіяльності серед студентської молоді та повнолітніх осіб є стратегічним ресурсом зміцнення державної стійкості, що дозволяє змінити парадигму сприйняття безпеки з пасивного очікування захисту на активну стратегію системного зниження віктимності суспільства.

2. Досліджено та систематизовано психофізіологічні механізми реагування людини на загрозу в умовах гострого стресу. З'ясовано, що ключовим деструктивним детермінантом поведінки є некероване психоемоційне напруження, яке спричиняє когнітивне звуження, порушення дрібної моторики та дезорганізацію рухової активності. Обґрунтовано, що подолання цих факторів можливе лише через формування стійкої психофізичної готовності, яка базується на синергії ситуаційної уважності, емоційного самоконтролю та здатності до усвідомленого керування власним станом через дихальні та м'язові алгоритми регуляції.

3. Визначено, що концепція підготовки цивільних осіб має ґрунтуватися на принципах усвідомленості, профілактики та деескалації. Встановлено, що основною метою такої підготовки є не розвиток спеціалізованих навичок силового протистояння, а виховання здатності до ідентифікації небезпеки на ранніх етапах її виникнення. Психофізична готовність розглядається як інтегральна характеристика особистості, що дозволяє зберігати ясність мислення та фізичну керованість у ситуаціях високої невизначеності, мінімізуючи ризики для життя і здоров'я у повсякденному житті.

4. Обґрунтовано та практично підтверджено, що використання простих рухових моделей, заснованих на великій моториці та природних рухових патернах, є найефективнішим інструментом забезпечення безпеки в умовах «адреналінового тиску». Оскільки складні технічні дії втрачають надійність під час стресу, саме прості, функціонально доцільні рухи дозволяють людині зберігати просторову орієнтацію та контроль над дистанцією. Доведено, що такі моделі виконують функцію «психофізичного заземлення», сприяючи стабілізації стану та відновленню відчуття суб'єктивного контролю над ситуацією.

5. Виявлено та проаналізовано типові системні помилки у підготовці цивільних осіб, серед яких найбільш критичними визначено переоцінку ролі фізичної сили та ігнорування внутрішнього психоемоційного стану. Встановлено, що ефективність навчання значно підвищується за умови інтеграції психофізичних вправ у загальноосвітній простір та систему фізичного виховання ЗВО. Застосування диференційованого підходу, орієнтованого на формування реалістичних поведінкових установок учасників, дозволяє перетворити теоретичні знання на стійку навичку безпечної поведінки.

6. Узагальнено, що формування психофізичної готовності особистості є безперервним процесом розвитку загальної культури безпеки. Запропоновані у монографії методичні підходи створюють наукове підґрунтя для модернізації системи безпекової освіти та цивільного захисту. Впровадження результатів дослідження дозволить не лише знизити рівень індивідуальної віктимності громадян, а й забезпечити сталий розвиток суспільства через виховання відповідальної та захищеної особистості, що є запорукою зміцнення національної безпеки України в довгостроковій перспективі.

КОГНІТИВНА БЕЗПЕКА ТА МЕДІАТЕХНОЛОГІЇ В СИСТЕМІ ЗАХИСТУ ПУБЛІЧНИХ ІНТЕРЕСІВ УКРАЇНИ

COGNITIVE SECURITY AND MEDIA TECHNOLOGIES IN THE SYSTEM OF PROTECTION OF PUBLIC INTERESTS OF UKRAINE

Pekhnyk A. V.,
Candidate of Political Sciences, Associate Professor,
Head of the Department of Journalism, Advertising
and Media Communications,
I. I. Mechnikov ONU,
Odesa, Ukraine

Інформаційна зброя є зброєю масового ураження —
вона вражає не тіла, а розуми й волю.

Abstract. This article examines cognitive security as a systemic and autonomous dimension of public interest protection in Ukraine. The subject of research encompasses the mechanisms, typology, and structural conditions of cognitive threats operating through media-technological infrastructure, together with the institutional, normative, and educational instruments available for their mitigation. The study is situated at the intersection of cognitive science, media studies, security studies, and public administration. Particular attention is devoted to the Ukrainian context: a society simultaneously undergoing democratic consolidation and Euro-Atlantic integration while

enduring the most extensively documented campaign of information-psychological warfare in modern history, conducted by the Russian Federation since 2014 and intensified dramatically following the full-scale invasion of February 24, 2022. The article argues that cognitive security cannot be reduced to traditional information security: its core concern is the protection of cognitive processes themselves — perception, attention, memory, judgment, and decision-making — from targeted external manipulation deployed through media-technological means. This reframing positions cognitive security as a foundational public good indispensable to the epistemic conditions of democratic self-governance, since authentic democratic participation presupposes citizens capable of forming unmanipulated preferences and exercising informed choice.

The study employs a multi-method, interdisciplinary framework. At the theoretical level it draws on cognitive science (bounded rationality, dual-process theory, cognitive biases), media and communication studies (agenda-setting, framing theory, cultivation theory), security studies (hybrid threats, non-kinetic warfare, strategic communication), and regulatory theory (public interest, proportionality, democratic governance). At the empirical level the methodology integrates: systematic content analysis of documented disinformation campaigns coded with the DISARM framework — a standardised taxonomy of information operations tactics, techniques, and procedures modelled on MITRE ATT&CK; comparative normative-legal analysis of Ukrainian legislation and EU regulatory instruments, including the Digital Services Act (2022) and the EU Code of Practice on Disinformation; case-study analysis of verified Russian cognitive operations against Ukraine (2014–2024) drawing on EUvsDisinfo, EU DisinfoLab, and Digital Security Lab Ukraine data; and critical synthesis of experimental and survey-based literature on disinformation susceptibility and the

effectiveness of prebunking and media literacy interventions. The overarching methodological principle is triangulation: qualitative depth of discourse and case analysis is complemented by the breadth of comparative legal analysis and the causal insights of experimental research.

The purpose of the article is to develop a comprehensive conceptual framework for cognitive security in the context of public interest protection in Ukraine and to analyse the key dimensions of its practical realisation through the prism of the contemporary media-technological environment. Specific objectives include: establishing the operational definition of cognitive security distinct from adjacent concepts; constructing a typology of cognitive threats; analysing technological mechanisms — algorithmic manipulation, synthetic media, deepfakes, coordinated inauthentic behaviour, and microtargeting; examining the normative-legal architecture in Ukraine and the EU; verifying propositions through case analysis; and formulating strategic directions for a national cognitive security system.

The research yields six principal findings. First, cognitive security constitutes an autonomous and indispensable dimension of public interest protection, irreducible to information or psychological security. Second, Ukraine faces an unprecedented cognitive threat landscape in which disinformation operations, algorithmic manipulation, synthetic media, and coordinated inauthentic behaviour mutually reinforce one another — a challenge continuously amplified by generative artificial intelligence. Third, Ukraine's normative system has advanced substantially through the Law on Media (2022) and Euro-integration obligations, yet systemic gaps persist: institutional fragmentation, absence of a framework law on cognitive security, de facto non-regulation of Telegram, and underdeveloped real-time response mechanisms. Fourth, an unresolved normative tension between effective protection and the preservation of fundamental rights — free

speech, free thought, free information — requires clear proportionality standards and independent oversight. Fifth, the most durable foundation of any cognitive security system is societal resilience built through systematic media literacy education and democratic culture; technological and regulatory measures are necessary but insufficient without a cognitively competent citizenry. Sixth, an effective national cognitive security system requires a coordinated approach spanning five dimensions: institutional consolidation (a National Cognitive Security Centre), technological development (early-warning systems, Ukrainian-language AI models, deepfake detectors), legislative reform (a framework law and DSA implementation), systemic media education, and deepened international partnership with EDMO and NATO Centres of Excellence.

Keywords: cognitive security, media technologies, public interest protection, disinformation, information operations, hybrid warfare, algorithmic manipulation, synthetic media, deepfakes, media literacy, digital sovereignty, coordinated inauthentic behaviour, prebunking, Ukraine, democratic resilience.

1. Вступ

Сучасна епоха характеризується безпрецедентним злиттям фізичного, цифрового та когнітивного просторів, що породжує якісно нові форми загроз публічним інтересам. Якщо класичне безпекознавство зосереджувалося на захисті територій, інституцій та критичної інфраструктури, то сьогодні до цього переліку невід'ємно додається захист самої здатності громадян і суспільства адекватно сприймати реальність, критично мислити й приймати автономні рішення. Ця нова площина безпеки постає ключовим фронтом сучасних гібридних конфліктів [19, с. 5; 25, с. 8].

Україна перебуває в унікальній — і трагічній — позиції держави, яка одночасно є об'єктом повномасштабної збройної агресії та

найбільш масштабної задокументованої кампанії інформаційно-психологічних операцій в історії сучасних конфліктів [12; 36]. Відтак питання когнітивної безпеки набуває для України не абстрактно-теоретичного, а вкрай практичного і невідкладного характеру: від ефективності системи захисту когнітивного суверенітету громадян залежить і мобілізаційний потенціал суспільства, і стійкість демократичних інститутів, і успішність євроінтеграції.

Водночас науковий і управлінський дискурс щодо когнітивної безпеки в Україні перебуває на початковому етапі формування. Попри значний масив досліджень у суміжних галузях — інформаційної безпеки [19], медіакомунікацій [25], психологічної безпеки — системного, міждисциплінарного аналізу когнітивної безпеки як самостійного виміру захисту публічних інтересів бракує.

Слід відзначити той факт, що сучасний етап розвитку інформаційного суспільства характеризується якісною трансформацією природи загроз публічним інтересам: поряд із традиційними формами збройної, економічної та кіберагресії дедалі більшого стратегічного значення набувають цілеспрямовані впливи на когнітивні процеси громадян — їхню здатність адекватно сприймати реальність, критично мислити й приймати автономні рішення. Ця тенденція є глобальною, однак для України вона набуває особливої гостроти та невідкладності.

По-перше, Україна перебуває в умовах повномасштабної збройної агресії рф, невід'ємним складником якої є безпрецедентна за масштабом і задокументованістю кампанія інформаційно-психологічних операцій. За оцінками EU East StratCom Task Force, Росія здійснює системні дезінформаційні операції проти України, ЄС і міжнародної спільноти щонайменше з 2014 року, і після 24 лютого 2022 р. їх інтенсивність та технологічна складність зросли кардинально. Питання когнітивної безпеки тому є не абстрактно-теоретичним, а безпосередньо пов'язаним із мобілізаційним потенціалом

суспільства, стійкістю демократичних інститутів і успішністю євроінтеграції.

По-друге, технологічний прогрес у сфері штучного інтелекту та генеративних медіа суттєво розширює арсенал когнітивного впливу. Розповсюдження дипфейків, великих мовних моделей, систем мікротаргетингу та координованої неавтентичної поведінки переводить маніпуляцію суспільною свідомістю на якісно новий рівень масштабованості, персоналізованості й правдоподібності, для якого чинні правові та інституційні механізми захисту виявляються структурно недостатніми.

По-третє, євроінтеграційний курс України актуалізує необхідність приведення вітчизняної системи захисту когнітивної безпеки у відповідність до стандартів ЄС — передусім Акту про цифрові послуги (DSA, 2022), Кодексу поведінки щодо дезінформації (2022) та відповідних вимог щодо регулювання великих платформ. Гармонізація у цій сфері є одночасно євроінтеграційним зобов'язанням і практичною безпековою необхідністю.

По-четверте, в умовах воєнного стану загострюється фундаментальна нормативна напруга між ефективністю захисту когнітивного простору та збереженням гарантій свободи слова, думки й інформації. Відсутність системного наукового опрацювання цієї напруги в українському контексті унеможливлює вироблення збалансованих регуляторних рішень, що відповідають стандартам демократичного врядування.

Відтак актуальність дослідження визначається одночасно трьома взаємопов'язаними чинниками: практичною безпековою нагальністю в умовах гібридної агресії; технологічною динамікою, що постійно генерує нові форми загроз; та нормативно-інституційними вимогами євроінтеграційного процесу.

Тема когнітивної безпеки в контексті захисту публічних інтересів України є новою для українського наукового дискурсу з кількох

взаємопов'язаних причин. У концептуальному відношенні поняття «когнітивна безпека» як самостійна наукова категорія лише нещодавно сформувалося на перетині когнітивної науки, безпекознавства та медіадосліджень і досі не отримало системного опрацювання в українській науці. Наявні вітчизняні дослідження оперують переважно суміжними поняттями — «інформаційна безпека», «інформаційно-психологічна безпека», «медіабезпека» — не виокремлюючи специфічно когнітивного виміру захисту як самостійного об'єкта аналізу. Відтак тема є новою не лише як конкретний предмет дослідження, а й як концептуальна рамка, що потребує розробки.

У проблемному відношенні поєднання трьох визначальних для сучасної України чинників — повномасштабна збройна агресія з безпрецедентним компонентом когнітивних операцій, стрімка технологічна еволюція інструментів маніпуляції (генеративний ШІ, дипфейки, мікротаргетинг) та євроінтеграційні зобов'язання щодо регулювання цифрового простору — утворює якісно нову проблемну ситуацію, якої не існувало на момент формування наявного масиву досліджень із суміжних тем. Ця ситуація потребує принципово нового концептуального інструментарію, а не лише застосування наявних підходів до нових емпіричних матеріалів.

У міждисциплінарному відношенні тема є новою як спроба синтезу, що досі не здійснювався: поєднання аналітичного апарату когнітивної науки, теорії медіакомунікацій, безпекознавства і публічного управління стосовно єдиного об'єкта — системи захисту когнітивних процесів як публічного інтересу. Кожна з цих дисциплін досліджує окремі аспекти проблеми, однак їх інтегрована міждисциплінарна рамка в українському науковому просторі відсутня.

У прикладному відношенні тема є новою як предмет публічно-управлінського проєктування: питання про те, якою має бути національна система когнітивної безпеки України — з якими інституційними, нормативними, технологічними та освітніми

компонентами — в науковій літературі системно не ставилося і не досліджувалося.

Метою дослідження є розроблення системної концептуальної рамки когнітивної безпеки в контексті захисту публічних інтересів України та аналіз ключових аспектів її практичної реалізації через призму медіатехнологічного середовища. Відповідно до мети визначено такі науково-дослідницькі завдання:

— обґрунтувати концептуальні засади когнітивної безпеки;

— систематизувати типологію когнітивних загроз у сучасному медіасередовищі;

— проаналізувати технологічні механізми реалізації цих загроз;

— дослідити нормативно-правову базу захисту когнітивної безпеки;

— верифікувати теоретичні положення на матеріалі конкретних кейсів;

— сформулювати стратегічні напрями розбудови національної системи когнітивної безпеки.

Теоретико-методологічну основу дослідження формує міждисциплінарна рамка, що свідомо інтегрує концептуальний апарат чотирьох дисциплінарних традицій, жодна з яких окремо не є достатньою для повноцінного аналізу феномену когнітивної безпеки.

Когнітивна наука забезпечує розуміння механізмів, через які стають можливими цілеспрямовані маніпуляції людським мисленням. Фундаментальним є відкриття обмеженої раціональності (Г. Саймон) [28, с. 99]: людські когнітивні агенти не є оптимізаторами в раціонально-економічному сенсі, а використовують евристики — спрощені правила прийняття рішень, що є адаптивними в більшості ситуацій, але систематично вразливими до маніпуляцій у специфічних умовах. Дослідження когнітивних упереджень (Д. Канеман і А. Тверські) [16, с. 20–24] показали, що ці відхилення від

нормативної раціональності є не випадковими помилками, а стійкими, відтворюваними і передбачуваними закономірностями — що і робить їх ефективними «векторами атаки». Двосистемна теорія мислення (Система 1 — швидке, інтуїтивне, емоційне; Система 2 — повільне, аналітичне, свідоме) [16, с. 20–22] пояснює, чому маніпулятивний контент, що активує Систему 1 через емоційне й образне подання, є ефективнішим, ніж раціональне спростування через Систему 2. Концепція «архітектури вибору» (R. Thaler, C. Sunstein) [30, с. 5–8] додає розуміння того, що когнітивне середовище — контекст, в якому здійснюється вибір — принципово визначає його зміст незалежно від усвідомлених преференцій агента, що є теоретичним обґрунтуванням регуляторних заходів щодо дизайну інформаційного середовища.

Теорія медіакомунікацій забезпечує розуміння того, як медіасистема конституює суспільне сприйняття реальності — а не лише відображає її. Теорія встановлення порядку денного (Maxwell McCombs, Donald Shaw) [21, с. 176] емпірично верифікувала, що медіа визначають не лише те, «що думати», але й «про що думати» — формуючи ієрархію суспільної уваги, яка в умовах систематичної маніпуляції стає інструментом відволікання від справді важливого. Теорія фреймінгу (Erving Goffman, Robert Entman) [10, с. 52] описує механізм, через який одні й ті самі факти, подані в різних інтерпретаційних рамках, призводять до кардинально різних суджень і рішень — без будь-якої фальсифікації самих фактів. Теорія культивації (George Gerbner) [14, с. 43] встановила довгостроковий накопичувальний ефект медіаспоживання: систематична експозиція до певних образів і наративів поступово «культивує» специфічне сприйняття соціальної реальності, що стає «природним» для аудиторії. Критичний дискурс-аналіз (Norman Fairclough, Teun van Dijk) [13; 32] забезпечує інструментарій для виявлення прихованих владних відносин і маніпулятивних стратегій

у медіатекстах — включно з тими, що не містять явно хибної інформації.

Безпекознавство забезпечує концептуальну рамку для розуміння когнітивних операцій як форми агресії та системного ризику. Теорія гібридних загроз описує сучасні конфлікти як поєднання кінетичних і некінетичних інструментів впливу, де когнітивний домен є окремим і рівноправним полем бою поряд із фізичним, кіберпросторовим та інформаційним. Концепція стратегічної комунікації (НАТО, ЄС) визначає принципи державного реагування на когнітивні операції — передбачення, швидкість, автентичність, координація — і є безпосереднім практичним інструментарієм для аналізу кейсів протидії. Теорія «м'якої сили» та публічної дипломатії (Joseph Nye) забезпечує розуміння довгострокових механізмів формування сприйняття через культурні й ціннісні наративи, що є важливим для аналізу операцій на міжнародну аудиторію.

Публічне управління забезпечує нормативно-аналітичну рамку для оцінки регуляторних відповідей на когнітивні загрози. Регуляторна теорія (market failure, public goods) обґрунтовує, чому когнітивна безпека є сферою, де ринкові механізми є структурно недостатніми і де виникнення «провалів ринку» — зокрема, в контексті алгоритмічної оптимізації на залученість на шкоду якості інформаційного середовища — є системним, а не випадковим. Теорія публічного інтересу визначає нормативні підстави для державного втручання у сферу медіа й цифрових платформ: коли й на яких умовах обмеження свободи інформаційного обміну є виправданим в інтересах суспільства. Теорія демократичного врядування встановлює конституційні межі регуляторних заходів — вимоги необхідності, пропорційності й підзвітності — що є принципово важливим для уникнення ризиків, за яких система «захисту» когнітивної безпеки сама стає інструментом обмеження когнітивної автономії.

Системний аналіз застосовується для розробки інтегрованої концептуальної моделі когнітивної безпеки та виявлення системних зв'язків між її компонентами — загрозами, механізмами реалізації, нормативними інструментами і суспільною стійкістю. Порівняльно-правовий аналіз забезпечує зіставлення нормативних систем України та ЄС, виявлення прогалин і формулювання рекомендацій щодо гармонізації. Контент-аналіз медіаматеріалів і верифікованих кейсів здійснено на основі баз EUvsDisinfo і Digital Security Lab Ukraine з метою реконструкції типових патернів когнітивних операцій. Синтез емпіричних досліджень (систематичний огляд) використовується для верифікації теоретичних положень на основі наявних рандомізованих і квазіекспериментальних досліджень у галузі медіаосвіти, дезінформації та когнітивних ефектів медіаспоживання.

Інтеграція цих методів у єдину дослідницьку стратегію обґрунтована принципом методологічної тріангуляції: кожне ключове положення статті отримує підтвердження через щонайменше два незалежні методологічні підходи, що підвищує надійність висновків і знижує ризики методологічної упередженості.

1. Когнітивна безпека: концептуальні засади та системна рамка

Когнітивна безпека як самостійна наукова категорія формувалась на перехресті кількох дисциплінарних традицій, відображаючи зрослу усвідомленість того, що сучасні загрози безпеці систематично спрямовані не лише проти фізичних чи кіберфізичних об'єктів, але й проти людської здатності розуміти реальність і діяти в ній.

З боку когнітивної науки фундаментальними є відкриття обмеженої раціональності (Г. Саймон) [28, с. 99–100], систематичних когнітивних упереджень (Д. Канеман і А. Тверські) [16, с. 20–35] та нейропластичності. Когнітивна наука продемонструвала, що людське мислення системно відхиляється від нормативно-раціональних стандартів у передбачуваний і відтворюваний

спосіб — а це означає, що ці відхилення можна використовувати як вектори атаки. Концепція «архітектури вибору» (R. Thaler, C. Sunstein) [30, с. 5–8] додала розуміння того, що когнітивне середовище принципово визначає зміст самого вибору, незалежно від усвідомлених преференцій агента.

З боку досліджень безпеки вирішальним є переосмислення загрози від традиційних «кінетичних» до «некінетичних» форм. Концепція «когнітивного домену» (cognitive domain) як окремого виміру поля бою з'явилася в натовській доктрині у 2010-х роках поряд із традиційними фізичним, інформаційним і кіберпросторовим. НАТО офіційно включила когнітивний домін до своєї доктрини в документах 2021–2023 років.

З боку медіадосліджень ключовим є розуміння медіасистеми не як нейтрального каналу трансмісії інформації, а як конститутивного середовища. Теорія встановлення порядку денного (agenda-setting, Maxwell McCombs, Donald Shaw) [21, с. 176–177], теорія фреймінгу (Erving Goffman, Robert Entman) [10, с. 51–58] та теорія культивації (George Gerbner) [14, с. 43–68] емпірично верифікували, що медіасистема не просто відображає реальність, але активно конструює те, яким чином аудиторія цю реальність сприймає.

В українській науковій традиції близькою концептуальною рамкою є «інформаційно-психологічна безпека» [19, с. 12–18; 25, с. 35–42; 2, с. 7–11], що охоплює захист від інформаційних впливів на психологічний стан суспільства. Ця традиція є продуктивним контекстом для інтеграції концепту когнітивної безпеки, хоча остання акцентує специфічно когнітивні механізми маніпуляції та вимагає чіткого операціонального визначення.

Когнітивна безпека визначається як стан захищеності індивідуальних і колективних когнітивних процесів — сприйняття, уваги, пам'яті, судження, прийняття рішень — від цілеспрямованих зовнішніх впливів, що прагнуть порушити їхню адекватність, автономність або цілісність через технологічні, медіаційні та

соціально-психологічні механізми. Це визначення підкреслює: орієнтацію на процеси, а не лише стани; охоплення як індивідуального, так і колективного рівня; акцент на цілеспрямованості загрози; багатоканальність засобів реалізації загроз.

Структурно концепт когнітивної безпеки включає три взаємопов'язані виміри. По-перше, захищеність — відсутність активних когнітивних атак або ефективна нейтралізація їх впливу. По-друге, стійкість — здатність індивідів і спільнот зберігати когнітивну автономію в умовах систематичного маніпулятивного тиску, що включає критичне мислення, медіаграмотність та соціальну довіру. По-третє, адаптивність — спроможність системи когнітивного захисту розвиватися в міру еволюції загроз [20, с. 41–45].

Публічний вимір когнітивної безпеки реалізується через два рівні. Перший — рівень публічного блага: когнітивна безпека суспільства є благом, що потребує колективної (державної) організації — аналогічно до санітарного захисту чи освіти. Другий — рівень демократичної легітимності: маніпулятивний вплив на масову свідомість підриває епістемічні умови демократії, адже колективне самоврядування передбачає здатність громадян формувати автентичні, неманіпульовані преференції.

Когнітивна безпека перебуває в складних відносинах перетину і розрізнення з рядом суміжних понять. Інформаційна безпека традиційно охоплює захист цілісності, доступності й конфіденційності інформації та інформаційних систем: загроза інформаційній безпеці — це злам системи, загроза когнітивній безпеці — маніпуляція людським розумом через технічно легальний інформаційний вплив. Психологічна безпека охоплює ширший спектр психічних станів — не лише когнітивних, але й емоційних та ідентифікаційних. Медіабезпека є необхідною, але не достатньою умовою когнітивної безпеки. Цифровий суверенітет становить одне з ключових обґрунтувань для регуляторних інструментів у цій сфері [32, с. 55].

2. Сучасний ландшафт когнітивних загроз у медіатехнологічному середовищі

Систематизація когнітивних загроз, що реалізуються через медіатехнологічну інфраструктуру, є методологічно необхідним кроком для подальшого аналізу. Пропонована типологія (Таблиця 1) ґрунтується на трьох критеріях: характер контенту; технологічний механізм реалізації; цільовий когнітивний ефект.

Таблиця 1 — Типологія когнітивних загроз у медіатехнологічному середовищі

Тип загрози	Механізм	Платформа	Цільовий ефект
Дезінформація	Фабрикація фактів, підроблені документи	Новинні сайти, Telegram	Хибні переконання
Маніпулятивний фреймінг	Вибіркова подача, акцентування	ТБ, онлайн-медіа	Упереджені судження
Пропаганда	Систематичні наративи, символи	Мас-медіа, соцмережі	Ідеологічне підпорядкування
Алгоритмічна маніпуляція	Персоналізація, ехо-камери	Facebook, YouTube, TikTok	Поляризація, радикалізація
Синтетичні медіа (deepfake)	ШІ-генерація відео / аудіо	Відеоплатформи, месенджери	Дискредитація, паніка
Інформаційне перевантаження	Потоки контенту, «шум»	Всі платформи	Апатія, дезорієнтація

Важливою аналітичною рамкою є DISARM-фреймворк [9], розроблений Digital Security Lab Ukraine та міжнародними партнерами на основі матриці кіберзагроз MITRE ATT&CK. DISARM систематизує тактики, техніки і процедури (ТТП) інформаційних операцій. Станом на 2024 рік фреймворк включає понад 200 задокументованих технік у межах чотирьох стадій: планування, підготовка, виконання й закріплення ефекту.

Дезінформація — навмисне поширення хибної або оманливої інформації з метою заподіяти шкоду — є найбільш дослідженим

типом когнітивної загрози. Аналіз ускладнюється концептуальними нюансами, ігнорування яких призводить до неточних висновків. По-перше, важливо розрізняти тріаду [34, с. 5], запропоновану C. Wardle і H. Derakhshan: *disinformation* (навмисно хибна), *misinformation* (хибна без умислу) та *malinformation* (достовірна, але використовується з метою заподіяти шкоду).

Фундаментальне значення має «ілюзія правди» [15, с. 107–108]: повторювана експозиція до твердження підвищує суб'єктивну оцінку його достовірності незалежно від об'єктивної верифікованості. Цей ефект, добре встановлений у лабораторних умовах [16, с. 62–64], має принципові наслідки для розуміння довгострокового накопичувального ефекту пропаганди.

Кількісний масштаб проблеми вражає. Дослідження MIT Media Lab (Vosoughi, Roy, Aral, 2018) [33, с. 1146] встановило на матеріалі 126 000 новинних каскадів у Twitter за 2006–2017 роки, що хибні новини поширюються швидше, далі й ширше, ніж правдиві. Ймовірність ретвіту для хибних новин виявилася на 70 % вищою порівняно з правдивими: ключовий пояснювальний фактор — новизна й емоційне забарвлення. Ці результати підтверджуються і для контенту про COVID-19 [6, с. 1–5].

Маніпулятивний фреймінг є одним із найбільш тонких і водночас ефективних механізмів когнітивного впливу. Теорія фреймінгу (Entman, 1993) [10, с. 52] описує фрейм як «відбір певних аспектів сприйнятої реальності та надання їм більшої ваги в комунікативному тексті» у спосіб, що просуває певне визначення проблеми, причинну інтерпретацію, моральну оцінку чи рекомендацію щодо дії. Ключова особливість фреймінгу — він не потребує хибної інформації: одні й ті самі факти, подані в різних фреймах, призводять до кардинально різних суджень.

Класичний приклад у релевантному для України контексті — різні способи представлення протестів Майдану 2013–2014 рр.:

«демократична революція», «антиурядовий заколот», «нацистський путч», «народне повстання проти корупції». Кожен із цих фреймів [13, с. 26–35] апелює до реальних подій, але формує принципово різне їх розуміння. Ефект фреймінгу посилюється повторюваністю: систематичне відтворення одного фрейму через множину медіаканалів поступово формує «природне» сприйняття, що суб'єкт вже сприймає не як фрейм, а як «саму реальність».

Окремим типом є цілеспрямоване інформаційне перевантаження. На відміну від класичної пропаганди, стратегія «потопу в інформації» орієнтована на досягнення когнітивного виснаження й апатії. Нейрокогнітивна основа цього ефекту — «виснаження его» [3, с. 1252–1254]: когнітивні ресурси є обмеженими, і тривале критичне опрацювання великих обсягів інформації систематично знижує здатність до якісного аналізу та підвищує сприйнятливість до маніпуляцій.

3. Технологічні механізми реалізації когнітивних загроз

Найбільш системним технологічним чинником є алгоритмічна медіація — визначення алгоритмами платформ, який контент бачить кожен користувач. Сучасні алгоритми рекомендаційних систем (Facebook, YouTube, TikTok, Twitter/X) оптимізовані передусім на максимізацію залученості — часу, проведеного на платформі, та кількості взаємодій.

Ця оптимізаційна ціль є структурно небезпечною з точки зору когнітивної безпеки. Емпіричні дослідження [4, с. 7313–7316; 27, с. 131–135] демонструють, що емоційно забарвлений — зокрема, морально обурливий — контент отримує значно вищу органічну залученість. Алгоритми «дізналися», що поляризуючий контент є найбільш «ефективним» з точки зору залученості, й систематично підсилюють його поширення. Таким чином, когнітивна загроза закладена в самій архітектурі платформ.

Феномен «ехо-камер» і «фільтрувальних бульбашок» [23, с. 9–12] описує сформовані алгоритмами інформаційні середовища, в яких користувач переважно отримує контент, що відповідає його наявним переконанням. Когнітивним наслідком є посилення ефекту підтвердження й наростаюча поляризація: різні групи населення живуть у різних «інформаційних реальностях», що ускладнює демократичний дискурс і підвищує вразливість до маніпулятивних операцій.

Розвиток генеративних систем штучного інтелекту (GANs, дифузійні моделі, великі мовні моделі) відкрив якісно нову епоху — епоху синтетичних медіа. Дипфейки — реалістичні синтетичні аудіовізуальні матеріали, в яких особа, голос чи контекст сфабриковані засобами ШІ. Спектр синтетичних медіа включає: відеодипфейки, аудіодипфейки, ШІ-генеровані текстові матеріали, синтетичні зображення, а також маніпульовані «дешевфейки» — контент, змінений простими засобами (уповільнення, обрізання, зміна контексту).

Для когнітивної безпеки синтетичні медіа є принциповою загрозою. По-перше, вони підривають базову епістемічну установку: що аудіовізуальні матеріали є достовірними свідченнями реальності. По-друге, навіть виявлені й спростовані дипфейки можуть виконати свою функцію — вкинути сумнів. Це явище, що психологи називають *liar's dividend* (R. Chesney, D. Citron) [5, с. 1756–1762]: спростована підробка ретроспективно підриває довіру до справжніх матеріалів.

Резонансним кейсом для України стало поширення у березні 2022 р. дипфейк-відео, в якому начебто Президент Зеленський закликає солдатів скласти зброю. Попри технічну недосконалість, відео було стрімко поширене в соціальних мережах до виявлення й публічного спростування [36]. Цей кейс ілюстрував потенціал синтетичних медіа в умовах гострої інформаційної кризи, коли аудиторія перебуває в стані підвищеної когнітивної вразливості.

Координована неавтентична поведінка — систематичне використання мереж неавтентичних акаунтів для штучного підсилення,

координованого поширення чи маніпулятивного впливу — є однією з найбільш масштабних операційних форм когнітивних загроз. Функції ботних мереж охоплюють: «накачування» контенту через масові лайки й шери для алгоритмічного просування; штучне створення ілюзії суспільного консенсусу; harassment-кампанії проти журналістів і активістів; дестабілізацію коментарних секцій.

Масштаб CIB-операцій є вражаючим. Дослідження Oxford Internet Institute [22] зафіксувало організовані кампанії CIB у 81 країні станом на 2020 р. EU DisinfoLab задокументував мережі з десятків тисяч акаунтів, координованих у рамках операцій проти України [11].

Технологія мікротаргетингу — використання детальних психографічних і демографічних профілів для гіперперсоналізованої доставки повідомлень конкретним сегментам аудиторії — є найбільш досконалою формою технологічно опосередкованої когнітивної маніпуляції. Скандал навколо Cambridge Analytica (2018) публічно продемонстрував потенціал цієї технології у виборчому контексті. Базуючись на психографічних моделях OCEAN/Big Five [16, с. 298–302], рекламні системи здатні ідентифікувати осіб з конкретними когнітивними вразливостями та доставляти їм відповідний маніпулятивний контент. Приховуваність мікротаргетингу є додатковою загрозою для когнітивної безпеки й демократичного дискурсу: мікротаргетований контент не є публічно видимим і не підлягає колективному критичному обговоренню.

4. Когнітивні операції проти україни: аналіз кейсів

Інформаційні операції росії проти України є безпрецедентними за масштабом і задокументованістю [12; 36]. Починаючи з подій 2014 року і посилившись після 24 лютого 2022 р., вони формують найбільш масштабне задокументоване застосування когнітивної зброї в сучасній історії. Системна архітектура охоплює п'ять взаємопов'язаних рівнів: наративний, медіаканальний, технологічний (ботні мережі, мікротаргетинг), інституційний (підставні «медіа»,

«аналітичні центри», НКО) й аудиторний (диференційований таргетинг на внутрішню аудиторію РФ, українців і міжнародну спільноту).

Аналіз бази EUvsDisinfo [12] — проєкту EU East StratCom Task Force, що з 2015 р. збирає верифіковані кейси дезінформації — дозволяє реконструювати типову матрицю наративів (Таблиця 2):

Таблиця 2 — Матриця основних дезінформаційних наративів проти України (за EUvsDisinfo, 2015–2024)

Наратив	Цільова аудиторія	Механізм впливу
«Нацизм в Україні»	Міжнародна спільнота, внутрішня рф	Делегітимація держави через хибну аналогію, апеляція до антифашизму
«Громадянська війна»	Глобальний Південь, ЄС	Нейтралізація підтримки через моральну рівнозначність сторін
«НАТО-агресія»	Антизахідні аудиторії	Переосмислення агресора через розширення каузального ланцюга
«Небратній народ»	росіяни, прокремлівські аудиторії	Деперсоналізація жертв через заперечення ідентичності
«Біолабораторії»	Конспірологічна аудиторія	Активація конспірологічних схем, розсіювання відповідальності

Примітна стратегічна логіка цієї матриці: різні наративи адресовані різним аудиторіям і реалізують різні цілі, але всі разом спрямовані на делегітимацію України як держави, підрив міжнародної підтримки й дезорієнтацію внутрішньої аудиторії. Це ілюструє принцип «лінкових атак» (linkage attacks) в когнітивних операціях: взаємопов'язані наративи підсилюють один одного й формують стійкий когнітивний простір [26, с. 12–18].

Telegram зайняв особливе місце в медіасистемі України — і особливо значущу роль в інформаційних операціях в контексті повномасштабної агресії. За різними оцінками, станом на 2023–2024 рр. Telegram є основним або одним з основних джерел новин для близько 70 % активних інтернет-користувачів України [36].

Специфіка Telegram як середовища когнітивних операцій визначається структурними характеристиками: відсутність систематичної модерації контенту; анонімність каналів — значна частина впливових каналів не має верифікованого авторства; можливість необмеженого поширення без алгоритмічної фільтрації; відсутність прозорості рекламного таргетингу. Дослідження Digital Security Lab Ukraine [36] задокументувало функціонування мереж скоординованих Telegram-каналів, що систематично поширюють проросійський контент або контент, спрямований на деморалізацію українців.

Показовим кейсом є кампанія «мобілізаційних наративів» у 2023–2024 рр.: серія Telegram-публікацій, що систематично перебільшували масштаб мобілізаційних порушень і цілеспрямовано дестабілізувала суспільні настрої. DSL задокументував скоординований характер кампанії через аналіз тимчасових патернів публікацій і семантичну кластеризацію повідомлень [36].

Паралельно з атаками на внутрішньоукраїнську аудиторію, Росія здійснює масштабні операції з формування сприйняття серед міжнародної аудиторії. Аналіз задокументованих операцій EU DisinfoLab [11] — зокрема, доповіді "Indian Chronicles" (2020) — розкриває мережу понад 750 фіктивних медіаорганізацій, залучених до просування проросійських наративів більш ніж у 116 країнах. Метод «інституційного маскування» є особливо ефективним: наратив, поширений «незалежною аналітичною організацією», сприймається аудиторією як більш достовірний.

На Глобальному Півдні росія просуває наратив «неоколоніальної агресії Заходу», що апелює до антиколоніального досвіду африканських, азійських і латиноамериканських суспільств. Когнітивна ефективність цього наративу визначається апеляцією до реального (або сприйнятого) досвіду та рефреймінгом агресора в захисника — класична техніка DARVO (Deny, Attack, Reverse Victim and Offender) [13, с. 18–22].

Система верифікації в Україні представлена відносно скоординованою мережею організацій: StopFake (заснований 2014), VoxCheck, Texty.org.ua, Detector Media. Їхня діяльність охоплює верифікацію тверджень, аналіз дезінформаційних кампаній і медіаосвітню роботу в рамках міжнародних мереж IFCN і EDMO.

Стратегічна комунікація держави суттєво еволюціонувала з лютого 2022 р. Ключовою інновацією став принцип «прозорості і передбачення»: офіційні органи — передусім ЦПД — систематично попереджали про наступаючі дезінформаційні операції до їх розгортання, позбавляючи їх ефекту несподіванки. Цей підхід, оснований на дослідженнях «інокуляції» [31, с. 1–4; 7, с. 1–5], є одним з найбільш науково верифікованих методів протидії дезінформації.

5. Нормативно-правова база захисту когнітивної безпеки в Україні та ЄС

Нормативно-правова база України у сфері захисту когнітивної безпеки формувалася поступово. Ключові акти систематизовані в Таблиці 3.

Стратегія національної безпеки України 2020 р. [29, с. 8–10] вперше закріпила інформаційну безпеку і захист інформаційного простору як окремий стратегічний пріоритет. Доктрина інформаційної безпеки 2017 р. [35] детальніше окреслила загрози — зокрема, «пропаганду, дезінформацію, маніпуляцію суспільною свідомістю» — і механізми їх нейтралізації.

Закон України «Про медіа» (2022) [17] є найбільш значущою недавньою законодавчою інновацією. Він поширює регуляторні вимоги на онлайн-медіа, передбачає механізми блокування контенту, що загрожує публічним інтересам, і вводить посилений контроль над прозорістю власності медіа. Регулятором виступає Національна рада з розширеними повноваженнями. Разом з тим закон критикується рядом медіаорганізацій за ризики надлишкового обмеження свободи слова.

Таблиця 3 — Нормативно-правова база захисту когнітивної безпеки в Україні та ЄС

Акт / Документ	Рік	Ключові положення
Стратегія національної безпеки України	2020	Інформаційна безпека як складова нац. безпеки
Закон України «Про медіа»	2022	Регулювання онлайн-медіа, боротьба з дезінформацією
Доктрина інформаційної безпеки України	2017	Захист від іноземних інформаційних операцій
Стратегія кібербезпеки України	2021	Захист критичної інформаційної інфраструктури
DSA (ЄС, імплементація Україною)	2022/2025	Відповідальність платформ, прозорість алгоритмів
Закон «Про основи національного спротиву»	2021	Інформаційний спротив як форма оборони

Закон «Про основи національного спротиву» (2021) [18] вперше нормативно визначив «інформаційний спротив» як форму оборони держави, закріпивши участь громадянського суспільства в захисті інформаційного суверенітету. Конституційний вимір є ключовим: Конституція України гарантує свободу слова й інформації (ст. 34) та захист від цензури (ст. 15). Будь-які заходи когнітивного захисту мають відповідати принципам необхідності й пропорційності у демократичному суспільстві.

Акт про цифрові послуги (Digital Services Act, DSA, 2022) [8] встановлює нові вимоги для великих платформ (VLOP) щодо: прозорості алгоритмічних рекомендаційних систем; аудиту системних ризиків, включаючи «навмисне маніпулювання послугою»; механізмів подачі скарг; особливих вимог щодо захисту від ризиків у кризових ситуаціях (стаття 36), що може бути задіяна в умовах збройного конфлікту. DSA є першим у світі обов'язковим регуляторним актом, що прямо адресує проблему системних когнітивних ризиків з боку платформ.

Кодекс поведінки щодо дезінформації ЄС (Code of Practice on Disinformation, оновлений 2022) є добровільним механізмом саморегулювання платформ, що передбачає зобов'язання щодо: боротьби з монетизацією дезінформації, підвищення прозорості політичної реклами, підтримки верифікаційних організацій. Для України імплементація цих стандартів [8, с. 45–48] є вимогою євроінтеграційного процесу і водночас практичною необхідністю.

Попри значні досягнення, нормативна система захисту когнітивної безпеки в Україні зберігає ряд системних прогалин, усунення яких є умовою її практичної ефективності.

По-перше, відсутній спеціальний рамковий акт щодо когнітивної безпеки як такої. Відповідні норми розпорошені між Законом «Про медіа», Стратегією національної безпеки, Доктриною інформаційної безпеки, Законом «Про основи національного спротиву» та кількома десятками підзаконних актів — без системної координації, єдиних визначень і механізмів міжвідомчої взаємодії. Така фрагментованість унеможливлює як стратегічне планування, так і ефективне правозастосування: в разі системної когнітивної атаки різні відомства діють за різними повноваженнями, різними процедурами і часто з різними пріоритетами. Прийняття рамкового закону про когнітивну безпеку, що визначав би поняття, суб'єктів захисту, повноваження, процедури й гарантії прав, є першочерговим законодавчим завданням.

По-друге, регулювання Telegram як домінуючого новинного середовища фактично залишається поза ефективним правовим контролем — і це є найбільш гострою структурною вразливістю. Станом на 2023 рік 72 % українських інтернет-користувачів отримували новини через Telegram, тоді як у 2021 р. цей показник складав лише 20 % — безпрецедентне зростання, зумовлене повномасштабним вторгненням. При цьому ані Telegram як платформа, ані автори анонімних Telegram-каналів не несуть жодної

медіавідповідальності і не обмежені вимогами щодо достовірності інформації.

Проблема поглиблюється структурними характеристиками самої платформи. Представник ГУР Андрій Юсов описав Telegram як «легалізований даркнет», де можна знайти все — від продажу наркотиків до груп ухильників від призову. Офіційні заяви про зв'язки платформи з російськими спецслужбами зробили начальник ГУР генерал-лейтенант Кирило Буданов та інші керівники безпекових структур, охарактеризувавши платформу як «однозначно проблемну з точки зору національної безпеки».

Спроби законодавчого врегулювання натрапляють на структурні перешкоди. Зареєстрований у березні 2024 р. законопроєкт передбачав вимоги щодо створення місцевого представництва, розкриття структури власності, дотримання вимог щодо спростувань та реагування на запити Нацради. Законопроєкт підтримали окремі депутати, зокрема колишній секретар РНБО Олексій Данілов, однак він мав мало шансів на ухвалення через відсутність підтримки з боку президентського офісу. У квітні 2024 р. Telegram тимчасово заблокував декілька державних чат-ботів — СБУ, Міноборони та ГУР — після того, як Україна звернулася до Apple з проханням натиснути на платформу. Українські офіційні особи розцінили цей крок як невисловлену погрозу: тиск на компанію може коштувати доступу до офіційних каналів.

У вересні 2024 р. Україна заборонила використання Telegram для державних службовців, військових і працівників критичної інфраструктури, посилаючись на загрози національній безпеці. Однак ця заборона є лише частковим заходом: вона не вирішує проблему анонімних проросійських каналів, не регулює цивільне використання і не встановлює жодних зобов'язань для самої платформи. Парадокс полягає в тому, що держава, яка забороняє своїм службовцям використовувати Telegram, одночасно не може ні зобов'язати

платформу блокувати дезінформаційні канали, ні отримати доступ до даних про їхніх операторів.

Telegram в умовах воєнного стану потребує комплексного підходу: законодавчого визначення платформи як суб'єкта медійної відповідальності; вимоги де-анонімізації каналів із понад 10 000 підписників; зобов'язання щодо реагування на запити регулятора протягом встановлених строків; координації з ЄС для забезпечення екстериторіального тиску через механізми DSA.

По-третє, механізми швидкого реагування на когнітивні атаки в режимі реального часу залишаються недостатньо розвиненими. Існуюча система передбачає кілька послідовних кроків — виявлення, аналіз, верифікація, прийняття рішення, реагування, — кожен з яких відповідає окремому відомству й потребує координації. Натомість сучасні когнітивні операції розгортаються за лічені години: дипфейк вірально поширюється до того, як завершується процедура верифікації; мобілізаційна паніка охоплює аудиторію Telegram до того, як виходить офіційне спростування. Мінімально необхідними є: цілодобовий оперативний штаб моніторингу з повноваженнями щодо термінового реагування; стандарт часу реакції (не більше 2 годин від виявлення до першого публічного спростування); протоколи взаємодії з платформами для прискореного блокування явно маніпулятивного контенту в умовах воєнного стану.

6. Суспільна стійкість до когнітивних загроз: вимірювання і фактори

Поряд із захисними (регуляторними й технологічними) заходами, фундаментальним виміром когнітивної безпеки є суспільна стійкість — здатність індивідів і спільнот зберігати когнітивну автономію в умовах систематичного маніпулятивного тиску. Когнітивна стійкість не є природженою рисою: вона формується через освіту, соціальний досвід і культурні практики.

Когнітивна стійкість включає кілька взаємопов'язаних складників: критичне мислення — здатність аналізувати аргументи і виявляти логічні маніпуляції [24, с. 2521–2522]; медіаграмотність — розуміння того, як функціонують медіасистеми і алгоритми; інформаційна гігієна — практичні навички верифікації інформації і диверсифікації джерел; епістемічна скромність — усвідомлення меж власного знання; соціальна довіра — як колективний ресурс стійкості: суспільства з вищим рівнем соціальної довіри демонструють вищу опірність дезінформації [1, с. 212–215].

Ефективність медіаосвітніх втручань підтверджена рядом рандомізованих контрольованих досліджень. Зокрема, "Go Viral!" — онлайн-гра, розроблена Університетом Кембриджа і ЮНІСЕФ, — продемонструвала статистично значущий ефект зниження сприйнятливості до COVID-дезінформації навіть після короткого (5-хвилинного) ігрового сесії. Дослідження "policylab" Джона Кука (2023) [7, с. 1–4] верифікувало, що «пребункінг» — попередження про маніпулятивні техніки до зустрічі з конкретним маніпулятивним контентом — є значно ефективнішим за «дебункінг» — спростування вже засвоєної дезінформації [31, с. 1–3].

В Україні система медіаосвіти розвивається інтенсивно, але нерівномірно. Серед ключових акторів: Академія Української преси, ГО «Детектор медіа», проєкт «Фільтр» Міністерства культури та інформаційної політики, «Медіаграмотність» МОН. Системна інтеграція медіаграмотності в шкільні навчальні програми залишається недостатньою.

Досвід Фінляндії, який з 2017 року незмінно займає перше місце в Індексі медіаграмотності серед 35 європейських країн, є унікальним за своєю системністю та свідомою стратегічною спрямованістю. Результат не є випадковим — він є продуктом кількох десятиліть цілеспрямованої публічної політики, побудованої на усвідомленій безпековій логіці. Це системна інтеграція критичного

мислення і медіаграмотності в навчальні програми з початкової школи, розроблена ще в 1990-х, яка сформувала суспільство з виключно високою стійкістю до маніпуляцій. Фінські дослідники й урядовці відкрито кажуть, що це є свідомою відповіддю на досвід тривалого сусідства з росією. Безпосереднім каталізатором реформи став 2014 рік, коли під час національних і європейських виборів в країні зафіксувалося різке зростання потоків російської пропаганди, медичної дезінформації та кліматичного заперечення в цифровому просторі. У 2016 р. фінансова навчальна програма була переглянута, щоб пріоритетизувати навички, необхідні учням для виявлення саме такого типу дезінформації. Для окремої підготовки державних службовців до протидії фейкам Фінляндія запросила міжнародних спеціалістів, зокрема з Гарвардського університету. Сі-Ен-Ен. Сьогодні медіаграмотність є наскрізною компетентністю у фінансовій системі освіти: поняття дезінформації та маніпуляції є частиною шкільних програм від дитячого садка до вищої школи, включаючи вивчення класичних пропагандистських досвідів, реклами й техніки маніпулювання статистикою.

Принциповим є педагогічний механізм цієї системи. Усі фінські вчителі — від дитячого садка до старшої школи, незалежно від предмету — зобов'язані інтегрувати медіаграмотність у свій навчальний процес. З 1980-х років стандарт підготовки вчителів став обов'язковим ступенем магістра, що формує культуру дослідницького підходу в класі. Учителі зводять складні методики перевірки до трьох базових питань: хто стоїть за повідомлення? Яким є доказ? Що кажуть інші джерела?

Разом із тим фінська модель не є безпроблемною, а саме критичне осмислення її меж є корисним для України. Фінансові дослідження (проєкт CRITICAL) фіксують, що 40 % дванадцятирічних учнів не можуть чітко відрізнити комерційну інформацію від фактичної інформації, а старші школярі знають труднощі з розпізнаванням маніпулятивних графіків. D+C — Розвиток + СпівпрацяЦе

працює про те, що навіть системна медіасвіта не забезпечує абсолютного захисту, і вимагає постійного вдосконалення методик.

Фінансова резистентність до маніпуляцій є частково культурним феноменом, однак вона була цілеспрямовано сформована протягом останніх десятиліть — і фінські дослідники відкрито визнають, що освіта розглядається там як склад колективної цивільної оборони, а не лише педагогічного процесу. Саме ця ідея — медіаграмотність як елемент системи національної безпеки — є ключовим уроком для України.

Для системного управління когнітивною безпекою необхідні верифіковані методи вимірювання стану стійкості суспільства. Пропонується система індикаторів у трьох вимірах: *компетентнісні* — вимірювання рівня медіаграмотності через стандартизовані тести, здатності до розпізнавання маніпулятивних технік; *поведінкові* — практики верифікації інформації, диверсифікація джерел; *суспільно-когнітивні* — рівень соціальної довіри, довіра до медіасистеми, рівень поляризації суспільних поглядів. Регулярні обстеження медіаграмотності [1, с. 232–233] мають бути інституціоналізовані як елемент національного моніторингу.

7. Стратегічні напрями розбудови національної системи когнітивної безпеки України

Ефективна система когнітивної безпеки потребує інституційної інфраструктури, що забезпечує координацію між різними акторами. Нині ця інфраструктура в Україні є фрагментованою: відповідні повноваження розподілені між Міністерством культури та інформаційної політики, РНБО, СБУ, Нацрадою, ЦПД та рядом інших органів без чіткої координаційної системи.

Пропонується формування міжвідомчого координаційного органу з чіткими функціями: моніторинг когнітивних загроз у режимі реального часу; координація між державними органами, медіаорганізаціями, платформами і громадянським суспільством; розробка і впровадження стандартів медіаграмотності; верифікація

й публічна комунікація щодо когнітивних операцій; дослідницька функція і оновлення методологічної бази. Принципово важливою є незалежність такого органу від органів виконавчої влади — для запобігання ризикам інструменталізації системи когнітивної безпеки з метою обмеження опозиційних голосів.

Технологічна складова системи включає пріоритетні напрями: система раннього попередження — автоматизований моніторинг медіапростору для ідентифікації нових когнітивних операцій на ранніх стадіях; підтримка україномовних ШІ-моделей — розробка якісних NLP-моделей для аналізу тексту, аудіо й відео; дипфейк-детектори [5, с. 1801–1810] — фінансування і розробка верифікованих інструментів виявлення синтетичних медіа у партнерстві з DARPA і Partnership on AI; платформа публічного верифікаційного реєстру — загальнодоступна база верифікованих і спростованих тверджень із відкритим API.

Системна медіаосвіта є найбільш довгостроковим, але водночас найбільш фундаментальним інструментом. Пропонується повна інтеграція медіаграмотності й критичного мислення в Державний стандарт базової і повної середньої освіти — не як окремого предмету, а як наскрізної компетентності (досвід Фінляндії і Естонії [1, с. 224–228]); система неформальної освіти для дорослих з особливою увагою до вразливих груп (люди похилого віку, мешканці малих міст, користувачі Telegram); підготовка медіапрофесіоналів і публічних службовців.

Когнітивні загрози є транснаціональними за своєю природою й потребують транснаціональних відповідей. Жодна держава не здатна ефективно протистояти скоординованим когнітивним операціям в ізоляції від міжнародних партнерів, оскільки самі платформи, через які ці операції реалізуються, є транснаціональними суб'єктами з глобальною інфраструктурою та юрисдикційним імунітетом від будь-якої окремої держави. Для України міжнародна

інтеграція у цій сфері є водночас безпековою необхідністю і євроінтеграційним зобов'язанням.

Перший напрям: система EDMO. Спеціально для підтримки України та Молдови у протидії російській дезінформації в рамках EDMO створено окремий регіональний хаб FACT, що довів загальну кількість хабів мережі до 15 і забезпечив охоплення країн-кандидатів. EDMO об'єднує верифікаторів і дослідників, підтримує програми медіаграмотності та надає аналітичну підтримку органам влади в оцінці імплементації Кодексу поведінки щодо дезінформації ЄС. Принципово важливою є інституційна незалежність мережі від будь-яких публічних органів влади — що забезпечує суспільну довіру до результатів верифікації.

Другий напрям: партнерство з технологічними платформами. Meta, Google/YouTube і TikTok є одночасно основним середовищем реалізації когнітивних операцій і потенційно найбільш ефективними партнерами у їх нейтралізації. Наявна практика є суперечливою. На позитивному боці: Meta задокументувала і ліквідувала кампанію Doppelganger — мережу сайтів, що імітують легітимні медіа, атрибутовану російським компаніям, що згодом потрапили під санкції ЄС і США; Google у першому кварталі 2023 р. припинив роботу понад 400 каналів YouTube, пов'язаних з Internet Research Agency. Разом з тим структурні обмеження є суттєвими: акаунти, виявлені на одній платформі, мігрують на інші; X (Twitter) після публікації Meta переліку загрозливих акаунтів заблокував більшість із них лише через 12 днів після медійного розголосу. Єврокомісія у 2025 р. встановила, що TikTok і Meta порушили зобов'язання щодо доступу дослідників до даних відповідно до DSA — що ілюструє принципову межу добровільних партнерств.

Третій напрям: НАТО. NATO StratCom CoE (Рига) є провідним аналітичним і навчальним центром у сфері стратегічних комунікацій і протидії дезінформації, для якого співпраця з Україною

є пріоритетним фокусом. У 2022–2023 рр. StratCom CoE разом із Hybrid CoE організував для України, Молдови та Грузії практичні «Wargames з протидії дезінформації» — симуляційні ігри з розбудови спроможностей. Hybrid CoE (Гельсінкі) акумулює досвід протидії гібридним загрозам у ширшому значенні і є важливою ресурсною базою для євроатлантичної інтеграції України.

Четвертий напрям: G7. У Капрійському комюніке G7 (квітень 2024 р.) міністри закордонних справ закріпили захист інформаційного середовища від іноземних маніпуляцій як спільний пріоритет. Для України ця рамка відкриває канали технічної допомоги та дипломатичного тиску на платформи і держави-агресори поза вузькими рамками НАТО і ЄС.

Ключовим принципом стратегії міжнародного партнерства має бути взаємодоповнюваність, а не дублювання: EDMO забезпечує верифікаційну інфраструктуру; StratCom CoE і Hybrid CoE — безпекову методологію і навчання; платформи — операційний доступ до даних; G7 — дипломатичний і регуляторний тиск на глобальному рівні. Завдання України — ефективно інтегруватися в кожен із цих рівнів, зберігаючи при цьому стратегічну автономію.

8. Висновки

Проведене дослідження дозволяє сформулювати ряд концептуальних і прикладних висновків.

По-перше, когнітивна безпека є самостійним і невід'ємним виміром системи захисту публічних інтересів, що принципово відрізняється від традиційних понять інформаційної й психологічної безпеки [19; 25]. В умовах гібридних конфліктів і глибокої цифровізації захист когнітивних процесів громадян є умовою і фундаментом демократичного врядування.

По-друге, сучасний ландшафт когнітивних загроз в Україні є безпрецедентним за масштабом і складністю [12; 36]. Він включає

системні дезінформаційні операції [33; 34], алгоритмічну маніпуляцію [4; 23], синтетичні медіа [5], координовану неавтентичну поведінку [22] і цілеспрямований мікротаргетинг. При цьому технологічна еволюція постійно розширює арсенал доступних засобів когнітивного впливу.

По-третє, нормативна система захисту когнітивної безпеки в Україні суттєво удосконалилася — особливо з прийняттям Закону «Про медіа» (2022) [17] і в рамках євроінтеграційних зобов'язань. Разом з тим зберігаються системні прогалини: фрагментованість інституційної архітектури, відсутність рамкового законодавства, де-факто нерегульованість Telegram.

По-четверте, нерозв'язаною залишається принципова нормативна напруга між ефективністю захисту й збереженням фундаментальних прав. Вирішення цієї напруги потребує чітких правових стандартів необхідності й пропорційності, незалежного судового контролю та активної участі громадянського суспільства.

По-п'яте, найбільш стійкою основою системи когнітивної безпеки є суспільна стійкість, що формується через системну медіаосвіту [7; 31], соціальну довіру й демократичну культуру. Технологічні й регуляторні заходи є необхідними, але недостатніми — без когнітивно компетентного суспільства жодна зовнішня система захисту не забезпечить надійного захисту від маніпуляцій.

По-шосте, ефективна система когнітивної безпеки України потребує збалансованого і координованого підходу, що охоплює: інституційну консолідацію, технологічний розвиток, законодавчу реформу (рамковий закон, імплементація DSA [8]), системну медіаосвіту і міжнародне партнерство (EDMO, НАТО, Meta/Google-партнерства). Лише системний підхід може відповісти на безпрецедентний виклик, що стоїть перед Україною.

Перспективами подальших досліджень є: розроблення методологічних стандартів моніторингу когнітивної безпеки;

порівняльний аналіз ефективності різних моделей медіарегулювання; дослідження специфічних вразливостей різних аудиторних груп і розробка цільових заходів когнітивного захисту; правовий аналіз конституційних меж регулювання когнітивного середовища.

Список використаних джерел:

1. Allcott H., Gentzkow M. Social media and fake news in the 2016 election. *Journal of Economic Perspectives*. 2017. Vol. 31. № 2. P. 211–236.

2. Баровська А. В. Інформаційна безпека України: сучасний стан та перспективи. Київ : НІСД, 2016. 48 с.

3. Baumeister R. F., Bratslavsky E., Muraven M., Tice D. M. Ego depletion: Is the active self a limited resource? *Journal of Personality and Social Psychology*. 1998. Vol. 74. № 5. P. 1252–1265.

4. Brady W. J. et al. Emotion shapes the diffusion of moralized content in social networks. *Proceedings of the National Academy of Sciences*. 2017. Vol. 114. № 28. P. 7313–7318.

5. Chesney R., Citron D. Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*. 2019. Vol. 107. P. 1753–1819.

6. Cinelli, M. et al. The COVID-19 social media infodemic. *Scientific Reports*. 2020. Vol. 10. 16598.

7. Cook J., Ellerton P., Kinkead D. Deconstructing climate misinformation to identify reasoning errors. *Environmental Research Letters*. 2023. Vol. 13. 024018.

8. Digital Services Act : Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services / European Parliament and Council of the EU. *Official Journal of the European Union*. 2022. L 277. P. 1–102.

9. DISARM Foundation. The DISARM Framework. 2024. URL: https://www.disarm.foundation

10. Entman R. M. Framing: Toward clarification of a fractured paradigm. *Journal of Communication*. 1993. Vol. 43. № 4. P. 51–58.

11. EU DisinfoLab. Indian Chronicles: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests. 2020. URL: https://www.eu-disinfolab.eu/stories/indian-chronicles

12. EUvsDisinfo. Disinformation database / East StratCom Task Force. 2024. URL: https://euvsdisinfo.eu/disinformation-cases

13. Fairclough, N. Critical Discourse Analysis: The Critical Study of Language. London : Longman, 1995. 265 p.

14. Gerbner G. et al. Growing up with television: Cultivation processes. Media Effects: Advances in Theory and Research / eds. J. Bryant, D. Zillmann. Hillsdale : Lawrence Erlbaum, 2002. P. 43–68.

15. Hasher L., Goldstein D., Toppino T. Frequency and the conference of referential validity. *Journal of Verbal Learning and Verbal Behavior*. 1977. Vol. 16. № 1. P. 107–112.

16. Kahneman, D. Thinking, Fast and Slow. New York : Farrar, Straus and Giroux, 2011. 499 p.

17. Про медіа : Закон України від 13 грудня 2022 р. № 2849-IX / Верховна Рада України. *Відомості Верховної Ради України*. 2023. № 8. Ст. 52.

18. Про основи національного спротиву : Закон України від 16 липня 2021 р. № 1702-IX / Верховна Рада України. *Відомості Верховної Ради України*. 2021. № 43. URL: https://zakon.rada.gov.ua/laws/show/1702-20

19. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції. Київ : КНТ, 2006. 280 с.

20. Luhmann N. The Reality of the Mass Media. Stanford : Stanford University Press, 2000. 154 p.

21. McCombs M., Shaw D. The agenda-setting function of mass media. *Public Opinion Quarterly*. 1972. Vol. 36. № 2. P. 176–187.

22. Oxford Internet Institute. Computational Propaganda Project: Country Reports 2017–2021. Oxford : University of Oxford, 2021. URL: https://demtech.oii.ox.ac.uk

23. Pariser E. The Filter Bubble: What the Internet Is Hiding from You. New York : Penguin Press, 2011. 304 p.

24. Pennycook G., Rand D. G. Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences*. 2019. Vol. 116. № 7. P. 2521–2526.

25. Почепцов Г. Г. Інформаційні війни. Київ : Ваклер, 2000. 576 с.

26. Pomerantsev P. Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia. New York : PublicAffairs, 2014. 256 p.

27. Ribeiro M. H. et al. Auditing radicalization pathways on YouTube. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAccT '20), New York, January 27–30, 2020. New York : ACM, 2020. P. 131–141.

28. Simon H. A. A behavioral model of rational choice. *The Quarterly Journal of Economics*. 1955. Vol. 69. № 1. P. 99–118.

29. Про затвердження Стратегії національної безпеки України : Указ Президента України від 14 вересня 2020 р. № 392/2020 / Президент України. *Офіційний вісник України*. 2020. № 75. Ст. 476.

30. Thaler R. H., Sunstein C. R. Nudge: Improving Decisions About Health, Wealth, and Happiness. New Haven : Yale University Press, 2008. 293 p.

31. Van der Linden S. et al. Inoculating the public against misinformation about climate change. *Global Challenges*. 2017. Vol. 1. № 2. 1600008.

32. Van Dijk T. A. Discourse and Power. New York : Palgrave Macmillan, 2008. 308 p.

33. Vosoughi S., Roy D., Aral S. The spread of true and false news online. *Science*. 2018. Vol. 359. № 6380. P. 1146–1151.

34. Wardle, C., Derakhshan, H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Strasbourg : Council of Europe, 2017. 100 p.

35. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 р. № 47/2017 / Президент України. *Офіційний вісник України*. 2017. № 20. Ст. 566.

36. Digital Security Lab Ukraine. Звіти про дезінформаційні кампанії 2022–2024. 2024. URL: https://dslua.org

References:

1. Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31(2), 211–236. https://doi.org/10.1257/jep.31.2.211.

2. Barovska, A. V. (2016). Information security of Ukraine: Current state and prospects [in Ukrainian]. NISD.

3. Baumeister, R. F., Bratslavsky, E., Muraven, M., & Tice, D. M. (1998). Ego depletion: Is the active self a limited resource? *Journal of Personality and Social Psychology*, 74(5), 1252–1265. https://doi.org/10.1037/0022-3514.74.5.1252.

4. Brady, W. J., Wills, J. A., Jost, J. T., Tucker, J. A., & Van Bavel, J. J. (2017). Emotion shapes the diffusion of moralized content in social networks. P*roceedings of the National Academy of Sciences*, 114(28), 7313–7318. https://doi.org/10.1073/pnas.1618923114.

5. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753–1819. https://doi.org/10.15779/Z38RV0D15J.

6. Cinelli, M., Quattrociocchi, W., Galeazzi, A., Valensise, C. M., Brugnoli, E., Schmidt, A. L., Zola, P., Zollo, F., & Scala, A. (2020). The COVID-19 social media infodemic. *Scientific Reports*, 10, 16598. https://doi.org/10.1038/s41598-020-73510-5.

7. Cook, J., Ellerton, P., & Kinkead, D. (2023). Deconstructing climate misinformation to identify reasoning errors. *Environmental Research Letters*, 13, 024018. https://doi.org/10.1088/1748-9326/aaa49f.

8. Digital Services Act. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services. *Official Journal of the European Union*, L 277, 1–102.

9. DISARM Foundation. (2024). The DISARM framework. Retrieved from https://www.disarm.foundation

10. Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x.

11. EU DisinfoLab. (2020). Indian Chronicles: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests. https://www.eu-disinfolab.eu/stories/indian-chronicles

12. EUvsDisinfo. (2024). Disinformation database. East StratCom Task Force. https://euvsdisinfo.eu/disinformation-cases

13. Fairclough, N. (1995). Critical discourse analysis: The critical study of language. Longman.

14. Gerbner, G., Gross, L., Morgan, M., Signorielli, N., & Shanahan, J. (2002). Growing up with television: Cultivation processes. In J. Bryant & D. Zillmann (Eds.), Media effects: Advances in theory and research (pp. 43–68). Lawrence Erlbaum.

15. Hasher, L., Goldstein, D., & Toppino, T. (1977). Frequency and the conference of referential validity. *Journal of Verbal Learning and Verbal Behavior*, 16(1), 107–112. https://doi.org/10.1016/S0022-5371(77)80012-1.

16. Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.

17. Law of Ukraine "On Media" of December 13, 2022, No. 2849-IX. (2023). Bulletin of the Verkhovna Rada of Ukraine, 8, Art. 52 [in Ukrainian].

18. Law of Ukraine "On the Fundamentals of National Resistance" of July 16, 2021, No. 1702-IX. (2021). *Bulletin of the Verkhovna Rada of Ukraine*, 43 [in Ukrainian].

19. Lipkan, V. A. (2006). Information security of Ukraine under the conditions of European integration [in Ukrainian]. KNT.

20. Luhmann, N. (2000). The reality of the mass media. Stanford University Press.

21. McCombs, M., & Shaw, D. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly*, 36(2), 176–187. https://doi.org/10.1086/267990.

22. Oxford Internet Institute. (2021). Computational propaganda project: Country reports 2017–2021. University of Oxford. Retrieved from https://demtech.oii.ox.ac.uk

23. Pariser, E. (2011). The filter bubble: What the Internet is hiding from you. Penguin Press.

24. Pennycook, G., & Rand, D. G. (2019). Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences,* 116(7), 2521–2526. https://doi.org/10.1073/pnas.1806781116.

25. Pocheptsov, H. H. (2000). Information wars [in Ukrainian]. Vakler.

26. Pomerantsev, P. (2014). Nothing is true and everything is possible: The surreal heart of the new Russia. PublicAffairs.

27. Ribeiro, M. H., Ottoni, R., West, R., Almeida, V. A. F., & Meira, W. (2020). Auditing radicalization pathways on YouTube. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (pp. 131–141). ACM. https://doi.org/10.1145/3351095.3372879

28. Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics,* 69(1), 99–118. https://doi.org/10.2307/1884852.

29. National Security Strategy of Ukraine, approved by Presidential Decree No. 392/2020 of September 14, 2020. (2020). *Ofitsiinyi visnyk Ukrainy [Official Gazette of Ukraine]*, 75. [in Ukrainian]

30. Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving decisions about health, wealth, and happiness. Yale University Press.

31. Van der Linden, S., Leiserowitz, A., Rosenthal, S., & Maibach, E. (2017). Inoculating the public against misinformation about climate change. *Global Challenges,* 1(2), 1600008. https://doi.org/10.1002/gch2.201600008

32. Van Dijk, T. A. (2008). Discourse and power. Palgrave Macmillan.

33. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science,* 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559.

34. Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.

35. Doctrine of Information Security of Ukraine, approved by Presidential Decree No. 47/2017 of February 25, 2017. (2017). *Official Gazette of Ukraine*, 20, Art. 566 [in Ukrainian].

36. Digital Security Lab Ukraine. (2024). Zvity pro dezinformatsiini kampanii 2022–2024 [Reports on disinformation campaigns 2022–2024] [in Ukrainian]. Retrieved from https://dslua.org

КОНСТИТУЦІЙНО-ПРАВОВИЙ ВИМІР ЦИФРОВИХ ПРАВ ЛЮДИНИ

CONSTITUTIONAL AND LEGAL DIMENSION OF DIGITAL HUMAN RIGHTS

Saparova A. O.,
Candidate of Legal Sciences,
Associate Professor at the Department of Legal Support
of Business Security,
State University of Trade and Economics,
Kyiv, Ukraine

Abstract. The section of the monograph is devoted to a comprehensive understanding of digital human rights in the constitutional and legal dimension as a phenomenon that is formed under the influence of the digital transformation of society. The main idea of the study is to prove that digital rights are not an isolated or temporary legal category, but constitute an evolutionary continuation of the classical system of human rights, integrated into the modern constitutional order. The digital environment changes not only the forms of realization of rights, but also the very logic of their guarantee, which requires rethinking the role of constitutional law as an instrument for ensuring a balance between individual freedom, public interests and technological development.

The subject of the study is the constitutional and legal nature of digital human rights, the mechanisms of their constitutionalization, guarantees of implementation and protection in the conditions of a digital society. Particular attention is paid to the transformation of traditional rights — privacy, freedom of expression, the right to

information, equality — in the digital space, as well as the emergence of new legal dimensions related to Internet access, personal data protection, algorithmic transparency and digital inclusion.

The purpose of section of the monograph is a comprehensive analysis of digital human rights in the constitutional and legal dimension, taking into account international standards, foreign experience and practice of constitutional justice, as well as substantiation of the need to develop an effective system of guarantees for their implementation in the context of digital transformation. The focus of the study is the search for an optimal model for combining innovative development of a digital society with the preservation of fundamental constitutional values.

The research methodology is based on a combination of general scientific and special legal approaches. The dialectical method was used to analyze the evolution of human rights in the context of technological change; the systemic approach — to consider digital rights as a component of a single system of constitutional values; the comparative legal method — to study international standards and national models of the constitutionalization of digital rights; formal legal and interpretative methods — to analyze the norms of constitutional law and judicial practice. The conceptual basis is the theory of digital constitutionalism, which allows us to consider the adaptation of the fundamental principles of the rule of law to the digital environment.

The conclusions substantiate that digital rights form a multidimensional segment of the modern system of human rights, which combines informational, technological and social elements. Their constitutionalization occurs in two complementary ways: through the interpretative expansion of traditional rights and through the normative consolidation of new guarantees. The effectiveness of the protection of digital rights depends on a complex

system of regulatory, institutional, procedural and socio-educational mechanisms. The study proves that the development of constitutional guarantees of digital rights is a continuous process aimed at ensuring the real realization of human dignity, freedom and legal certainty in the digital age. It is the integration of legal and technological approaches that creates the conditions for the stability of constitutional values in the transformed information society.

Keywords: Public Interests, National Security of Ukraine, Political and Legal Support, Sectoral Specificity, State Security Policy, Transformation of Security Governance.

1. Вступ

Цифрова трансформація сучасного суспільства є однією з ключових характеристик розвитку держави і права у XXI столітті. Впровадження інформаційно-комунікаційних технологій у всі сфери суспільних відносин — від публічного управління до приватної комунікації — зумовлює не лише технологічні зміни, а й глибоку трансформацію системи прав людини. У цифровому середовищі відбувається переосмислення змісту традиційних конституційних прав, формуються нові правові можливості особи та виникають принципово нові виклики для їх гарантування і захисту. За таких умов цифрові права поступово утверджуються як самостійний об'єкт конституційно-правового аналізу.

Актуальність дослідження зумовлена необхідністю теоретичного осмислення та нормативного забезпечення прав людини в умовах цифрової трансформації. Розвиток цифрових технологій впливає на реалізацію права на приватність, свободу вираження поглядів, доступ до інформації, рівність та участь у публічному управлінні.

Одночасно зростають ризики цифрового контролю, алгоритмічної непрозорості, порушення персональних даних і цифрової

нерівності. Це потребує вироблення сучасних наукових рішень щодо конституціоналізації цифрових прав, формування ефективних гарантій їх реалізації та забезпечення балансу між технологічним розвитком і фундаментальними конституційними цінностями. Особливої ваги набуває дослідження проблемних питань захисту прав людини в цифровому середовищі у контексті євроінтеграційних процесів та адаптації національного законодавства до міжнародних стандартів.

Наукова новизна дослідження полягає у комплексному розгляді цифрових прав людини як інтегративного елементу сучасної системи конституційних прав, що формується на перетині правових, технологічних і соціальних процесів. У розділі обґрунтовується підхід до цифрових прав не лише як похідних від інформаційних прав, а як багатовимірної категорії, що трансформує зміст конституційних гарантій. Запропоновано системне бачення конституціоналізації цифрових прав через поєднання інтерпретаційного та нормативного механізмів, а також розкрито роль цифрового конституціоналізму як теоретичної моделі адаптації принципів верховенства права до цифрового середовища.

Метою дослідження є з'ясування за результатами комплексного аналізу природи цифрових прав людини у конституційно-правовому вимірі та обґрунтування системи гарантій їх реалізації і захисту в умовах цифрової трансформації суспільства.

Для досягнення поставленої мети визначено такі **науково-дослідницькі завдання:** розкрити природу, поняття та еволюцію цифрових прав людини у системі конституційних цінностей; проаналізувати міжнародні стандарти та національні моделі конституціоналізації цифрових прав; дослідити взаємозв'язок цифрових прав із традиційними конституційними гарантіями.

Методологія дослідження базується на поєднанні загальнонаукових та спеціально-юридичних методів. Діалектичний метод

дозволив простежити становлення прав людини під впливом цифрових змін. Системний підхід застосовано для аналізу цифрових прав як складової єдиної системи конституційних цінностей. Порівняльно-правовий метод використано для дослідження міжнародних стандартів і зарубіжного досвіду. Формально-юридичний та інтерпретаційний методи забезпечили аналіз нормативних положень і судової практики. Концептуальною основою виступає теорія цифрового конституціоналізму, що дозволяє розглядати адаптацію фундаментальних правових принципів до цифрового середовища.

Логіка подання матеріалу зумовлена метою та завданнями дослідження. У першому параграфі розкриваються теоретико-правові засади цифрових прав людини, їх природа та становлення. Другий параграф присвячений аналізу міжнародних стандартів і національних моделей конституціоналізації цифрових прав. У третьому параграфі досліджуються конституційні гарантії реалізації та захисту цифрових прав у сучасному правопорядку. Така структура забезпечує послідовний перехід від теоретичного осмислення проблеми до аналізу практичних механізмів її вирішення.

2. Поняття, природа та еволюція цифрових прав людини у системі конституційних цінностей

Права людини — це визнані світовим співтовариством блага й умови життя, яких може домагатися особа від держави і суспільства, в яких вона живе, та забезпечення яких реальне в умовах досягнутого людством прогресу [8, с. 231].

Ідея прав людини, пройшовши крізь сторіччя людських страждань, зазіхань та масового насильства, складає основу сучасного світового правопорядку та, разом з цим, залишається основним викликом сьогодення.

Права людини разом з демократією та верховенством права складають ключові цінності європейського правового простору [7, с. 455].

Права людини, як зазначає Ю. Шемшученко, — історично мінлива категорія, яка еволюціонує разом із суспільством та державою [11, с. 5].

Права людини в цифрову епоху набувають дедалі більшої важливості й мають перебувати в епіцентрі уваги та дискусій як на рівні філософії права й загальнотеоретичного правознавства, так і в межах галузевих юридичних наук [22, с. 42].

Багатогранність людини породжує невичерпність її прав. Разом з людиною, її рівнем розвитку та значенням у соціумі постійно змінюються і її права, їх пріоритети [25, с. 729].

Права людини в умовах глобалізації — правові можливості людини здійснювати певні дії для задоволення своїх духовних і матеріальних інтересів, забезпечення існування й розвитку, які мають специфіку, що пов'язана з особливостями змісту процесу глобалізації [28, с. 603].

Одночасно з революцією в історії людства відбувається еволюція діджиталізації. Цифрове людство з'явилося не протягом однієї ночі, а формується останні 70 років [23, с. 26].

Глобалізація — як багатогранний, різнорівневий, нелінійний, диференційований, незворотний, суперечливий процес розширення, посилення й прискорення світової інтеграції державно-правових, економічно-фінансових і суспільно-політичних інститутів, ідей, принципів, цінностей, зв'язків, відносин має наслідком становлення ускладненого глобального мегасуспільства, істотні зміни в конкретних соціумах, характеризується об'єктивно-суб'єктивним характером, позитивними і негативними наслідками для людини, суспільства, держави, світової спільности [28, с. 604].

Погоджуємося з думкою Л. Г. Удовики, що «у сучасному світі права людини набувають нових форм, змісту, виявів» [28, с. 604].

При цьому сформувалося розуміння того, що стандарти прав людини мають зберігати свою універсальність незалежно від середовища їх реалізації — офлайн чи онлайн.

Особливого значення в умовах цифрової трансформації набуває конституційно-правовий вимір цифрових прав. Саме конституційне право формує базові принципи правового статусу особи, визначає межі допустимого втручання держави у сферу приватної автономії та встановлює підвищений рівень гарантій прав людини. Як зазначається у вітчизняній доктрині: «просування цифрових прав на шляху загального визнання логічно веде до пошуків визначення їх конституційно-правових гарантій і механізмів захисту, що наразі відбувається у двох форматах: 1) інтерпретаційному — як виведення певного цифрового права (як неявного права) з конституційних прав людини і, відповідно, доведення того, що це право охоплюється наявними конституційними гарантіями; 2) безпосереднього визначення цифрового права (як нового права) у текстах конституційних актів» [26, с. 146].

Тому розвиток цифрових прав неминуче приводить до необхідності пошуку нових моделей їх конституціоналізації — як шляхом інтерпретації традиційних конституційних норм, так і через пряме нормативне закріплення цифрових прав у текстах основних законів.

Водночас процес цифровізації впливає не лише на зміст прав людини, а й на саму природу конституціоналізму. У науковому дискурсі формується концепція цифрового конституціоналізму, що спрямована на адаптацію фундаментальних цінностей сучасного конституціоналізму — верховенства права, прав людини, поділу влади — до умов цифрового суспільства.

На думку Н. Кушакової-Костицької: «процес цифровізації має глобальний характер, однак постає питання, чи наявні в ньому національні особливості, які сприяють або гальмують його. Такі особливості мають місце й пов'язані з рівнем комп'ютерної / цифрової

грамотності населення, його менталітетом, інтелектуальним потенціалом, можливостями доступу до мережі Інтернет, а коли йдеться про цифровізацію правотворчості — з рівнем правосвідомості та правової культури безпосередньо правознавців і представників громадянського суспільства загалом» [9, с. 30].

Важливим напрямом сучасних наукових дискусій є проблема доцільності розширення системи прав людини шляхом включення «нових» цифрових прав.

Існує обґрунтована пересторога щодо надмірного розширення каталогу прав, оскільки це може призвести до знецінення фундаментального характеру прав людини та ускладнення механізмів їх реального забезпечення [26, с. 160].

Водночас інформаційна сфера демонструє об'єктивну необхідність розвитку нових правових інструментів, оскільки цифрові технології формують принципово нові умови реалізації людських свобод.

З цього погляду показовими є підходи, запропоновані Б. Кастерсом, який звертає увагу що «багато прав, які мають громадяни, зокрема фундаментальні права, що визначають ширшу картину, були розроблені в епоху, коли світ виглядав зовсім інакше. Отже, в сучасних дебатах та юридичних дослідженнях бракує ширшого обговорення того, які нові (фундаментальні та інші) права повинні мати громадяни в цифрову епоху. Це ставить питання про те, які (фундаментальні та інші) права можна було б придумати, якби нам довелося розробляти їх з чистого аркуша, а не бути прив'язаними до набору існуючих фундаментальних прав» [32, с. 2].

Такий підхід актуалізує необхідність концептуального переосмислення природи прав людини в умовах цифрової трансформації.

У цьому контексті цифрові права постають не лише як результат технічного прогресу, а як відповідь на глибинні соціальні зміни. Розвиток великих даних, інтернету речей, блокчейн-технологій та

алгоритмічного управління зумовлює появу нових форм соціальної взаємодії, що вимагають адекватних правових гарантій [32, с. 1].

Саме тому ідея «нових цифрових прав» не може розглядатися виключно як теоретичний експеримент, а має безпосереднє прикладне значення для формування майбутніх моделей правового регулювання.

Разом із тим значна частина дослідників наголошує на необхідності системного підходу до класифікації цифрових прав.

Так, у вітчизняній доктрині підкреслюється, що поняття «цифрові права» доцільно розглядати не як окрему групу прав людини, а як умовну категорію, що охоплює особливості реалізації та гарантії захисту фундаментальних прав людини в Інтернеті, зокрема свободи вираження поглядів та права на приватність онлайн. Зважаючи на величезну роль, яку відіграє Інтернет у сучасному житті, виокремлення такої категорії допомагає краще систематизувати та вивчати потреби захисту прав людини в онлайн-середовищі, окремі гарантії яких сьогодні розпорошені в рекомендаціях, резолюціях та інших актах міжнародних інституцій. Інші дослідники вважають цифрові права похідними від інформаційних, але не тотожними, і наголошують на необхідності їх виділення в окрему групу. Також цифрові права розуміють і як права громадян на доступ, використання, створення й публікацію цифрових творів, право на вільний доступ до мережі Інтернет (інших комунікаційних мереж) з використанням комп'ютерів та інших електронних пристроїв [5, с. 130].

О. Б. Братасюк та Н. Ф. Ментух цифрові права людини визначають як «окрему групу прав людини, які пов'язані з використанням та/або реалізовуються в мережі Інтернет за допомогою спеціальних пристроїв (комп'ютерів, смартфонів тощо)» [3].

О. Я. Мединська та Г. П. Синоруб також зазначають, що цифрові права є окремою категорією прав, це «права людей на доступ, використання, створення і публікацію цифрових творів, доступ

і використання комп'ютерів та інших електронних пристроїв, а також комунікаційних мереж, зокрема, мережі Інтернет» [10].

Ю. С. Размєтаєва вважає, що «до цифрових відносять і такі фундаментальні права, як свобода вираження думки і слова, приватність, право на інформацію, право на участь в управлінні державними справами тощо, і такі, як право бути забутим, право на анонімність чи, навіть, право на Інтернет» [16].

Цифрові права також перебувають у тісному зв'язку з інформаційними правами, однак не є з ними тотожними. Цифрові права мають ширший функціональний зміст, оскільки охоплюють не лише доступ до інформації, а й умови цифрової комунікації, безпеку цифрового простору, автономію особи у процесі обробки даних та використання цифрових платформ.

Таким чином, цифрові права формують окремий сегмент сучасної системи прав людини, що інтегрує інформаційний, технологічний та соціальний виміри.

Цифрова революція, що охопила світ, суттєво змінила спосіб спілкування, роботи та життя людей. Цей стрімкий технологічний розвиток несе з собою нові виклики для захисту прав людини [1, с. 111].

Досі технології були призначені для того, щоб робити все легше, швидше й ефективніше. Вони забезпечили нас можливостями особистого розвитку. Але вже зрозуміло, що й потенціал, і супутні ризики зростають. Ми перебуваємо на порозі докорінних системних змін, які вимагають від людини постійного пристосування [30, с. 86].

Окрему увагу в науковому дискурсі приділено проблемі взаємозв'язку цифрових прав із демократичними процесами. Перехід значної частини публічних сервісів у цифровий формат трансформує механізми участі громадян у публічному управлінні, доступу до адміністративних процедур та реалізації політичних прав.

У цьому аспекті цифрові права виступають не лише як інструмент індивідуальної свободи, а і як елемент інституційної стабільності демократичної держави.

Водночас цифровізація породжує нові ризики соціальної нерівності. Погоджуємося з В. І. Чалчинським, що «відсутність в окремих громадян доступу до цифрових технологій та мережі Інтернет, недостатній рівень цифрової грамотності та цифрових навичок призводить до порушення їх конституційних прав, зокрема права на інформацію, права на освіту, права на особистий та культурний розвиток. Особи, які користуються сучасними цифровими технологіями та інформаційними ресурсами, мають переваги над тими, хто позбавлений таких можливостей» [29, с. 114–115].

Обмежений доступ до цифрових технологій, низький рівень цифрової грамотності та нерівномірний розвиток інфраструктури формують так званий «цифровий розрив», що безпосередньо впливає на можливість реалізації конституційних прав.

З огляду на це, цифрові права набувають ознак соціальних прав, оскільки їх ефективне здійснення залежить від активної ролі держави у створенні відповідних умов.

Важливим аспектом розвитку цифрових прав є їх інтеграція у сферу освіти та формування цифрової компетентності населення. Дослідження, проведені Міністерством цифрової трансформації України, засвідчують, що хоча більшість громадян володіють базовими цифровими навичками, їх рівень часто є недостатнім для повноцінної реалізації можливостей цифрової економіки та електронних сервісів [31].

Це свідчить про необхідність розглядати цифрові права у взаємозв'язку з правом на освіту та доступом до цифрових знань.

Ситуація ускладнюється тим, що більшість прав людини концептуально розвинуті та нормативно закріплені ще до початку цифрової епохи. Зокрема, Загальна декларація прав людини, Міжнародний пакт про громадянські і політичні права, Міжнародний пакт про економічні, соціальні і культурні права, Конвенція про захист прав людини і основоположних свобод та низка інших документів були розроблені

для аналогового середовища. Хоча ці документи залишаються актуальними, вони часто не беруть до уваги специфіки цифрових викликів. Судова практика постійно актуалізує зміст прав людини в окремих сферах, проте таке приведення до сучасного розуміння викликів поки що є доволі точковим [4, с. 20].

Можна зробити висновок, що розвиток цифрових прав людини є не лише наслідком технологічного прогресу, а і результатом глибоких соціальних трансформацій. Вони формуються на перетині правових, технологічних та гуманітарних процесів, що зумовлює їх складну багаторівневу природу. Саме тому цифрові права доцільно розглядати як інтегративний елемент сучасної системи прав людини, який потребує подальшого теоретичного осмислення та нормативного розвитку.

3. Конституціоналізація цифрових прав людини: міжнародні стандарти, національні моделі

Міжнародний вимір конституціоналізації цифрових прав формується насамперед у межах діяльності Організації Об'єднаних Націй (далі — ООН) та Ради Європи (далі — РЄ). Одним із перших міжнародних документів, який заклав концептуальні засади визнання цифрових прав, стала резолюція Генеральної Асамблеї ООН щодо сприяння, захисту та забезпечення прав людини в Інтернеті. У ній було закріплено принцип рівності стандартів прав людини незалежно від середовища їх реалізації — онлайн чи офлайн [52].

Цей підхід фактично визнав цифровий простір повноцінною сферою реалізації прав людини.

Подальший розвиток міжнародних стандартів цифрових прав відбувався у європейському правовому просторі. Одним із перших системних кроків стало ухвалення у 2014 році Хартії цифрових прав, підготовленої мережею неурядових організацій EDRi. Цей документ сформулював комплекс принципів, серед яких прозорість

державних даних, участь громадян у законодавчих процесах, захист персональних даних, необмежений доступ до Інтернету, заохочення анонімності та шифрування, а також підтримка мультистейкхолдерного управління Інтернетом [48].

Наступним етапом стало прийняття Португалією у 2021 році Хартії прав людини в цифрову епоху та Лісабонської декларації принципів цифрової демократії, які розглядаються як підґрунтя для майбутньої загальноєвропейської Хартії цифрових прав [38].

У 2022 році Європейська комісія представила проєкт Європейської декларації про цифрові права та принципи цифрового десятиліття, що підтверджує тенденцію до формування наднаціонального стандарту цифрових прав людини [40].

Особливе місце у процесі конституціоналізації цифрових прав займає право на доступ до Інтернету. У сучасних умовах воно виступає базовою умовою реалізації інших прав у цифровому середовищі, оскільки позбавлення доступу до мережі фактично унеможливлює повноцінне здійснення багатьох соціальних, політичних та культурних прав. Погоджуємося з О. Тихомировим, що «саме тому право на доступ до Інтернету як таке, безвідносно комплексу цифрових прав, стало об'єктом міжнародного і національного правового регулювання» [26, с. 142].

Парламентська асамблея РЄ у резолюції 1987 (2014) прямо зазначила, що право на доступ до Інтернету включає можливість отримувати і поширювати інформацію без необґрунтованого втручання держави, а держави-члени повинні визнати це право в законодавстві та на практиці [53].

Водночас у доктрині триває дискусія щодо правової природи цього права — є воно фундаментальним, чи похідним, інструментальним щодо свободи слова та права на інформацію?

Застосування інтерпретаційного підходу до визнання цифрових прав чітко простежується у діяльності міжнародних органів. Так,

спеціальний доповідач ООН Ф. Ла Рю наголосив, що непропорційні обмеження доступу до Інтернету становлять порушення свободи вираження поглядів, гарантованої Міжнародним пактом про громадянські та політичні права [46].

Аналогічна логіка простежується у практиці Європейського суду з прав людини.

У справі "Ahmet Yildirim v. Turkey" Європейський суд з прав людини (далі — ЄСПЛ) визнав, що доступ до Інтернету є невід'ємним компонентом права на доступ до інформації та комунікації, яке вже захищене національними конституціями, і охоплює право кожної особи брати участь в інформаційному суспільстві та зобов'язання держав гарантувати доступ до Інтернету своїм громадянам [39].

Таким чином, судова практика поступово формує конституційні стандарти цифрових прав через тлумачення традиційних прав людини.

Турецька Республіка демонструє специфічний підхід до конституційного регулювання цифрових прав, який формується на перетині європейських стандартів та національних особливостей публічної безпеки. Конституція Туреччини 1982 року не містить прямої згадки про цифрові права, однак гарантує свободу вираження поглядів, право на приватність і таємницю комунікацій (статті 20, 22, 26) [36].

У практиці Конституційного суду Туреччини поступово формується доктрина цифрової пропорційності, відповідно до якої втручання держави у цифрові права допускається лише за умови суворого дотримання принципу необхідності та легітимної мети.

20 березня 2014 року, у відповідь на широку критику турецького уряду на Twitter.com, Президія телекомунікацій та зв'язку (TIB) видала заборону на вебсайт. Основним аргументом турецького уряду було те, що деякі коментарі, розміщені в Twitter, викликали занепокоєння щодо конфіденційності, безпеки та національної безпеки.

Через цю заборону кілька осіб звернулися до Конституційного суду Туреччини, стверджуючи, що заборона не має правових підстав. У своїх аргументах заявники посилалися на статті Конституції Туреччини щодо свободи слова, а також на прецедентне право ЄСПЛ. Вони також стверджували, що заборона не лише являє собою втручання в право доступу до інформації, але й у право на її поширення. Конституційний суд Туреччини відреагував на ці питання 2 квітня 2014 року у рішенні № 2014/3986, постановивши, що блокування Twitter з боку ТІВ дійсно є неконституційним, і наказав скасувати заборону.

Пізніше турецький парламент 10 вересня 2014 року ухвалив поправку до національного Закону про Інтернет № 5651, яка потенційно дозволяла ТІВ блокувати будь-який вебсайт без попереднього судового рішення з міркувань «національної безпеки, відновлення громадського порядку або запобігання скоєнню злочину». У відповідь на ці поправки Конституційний суд Туреччини 2 жовтня 2014 року у рішенні № 2014/149 постановив, що ці поправки, які дозволяли уряду блокувати певні вебсайти без судового рішення з міркувань «національної безпеки, відновлення громадського порядку або запобігання скоєнню злочину», є неконституційними. Прем'єр-міністр Туреччини розкритикував це рішення.

У рішенні Суду зазначено, що поправки до Закону про Інтернет № 5651 порушують статті 26, 27, 40 та 67 Конституції Туреччини. Головним обґрунтуванням для скасування заборони регулятора було те, що такі дії порушують права на недоторканність приватного життя та особисту свободу, які є гарантованими правами Конституцією Туреччини. Подібні обґрунтування обговорювалися як у рішенні Конституційного суду № 2014/3986 (2 квітня 2014 року), яке скасувало заборону Twitter.com, так і в рішенні № 2014/4705 (29 травня 2014 р.), який скасував заборону YouTube.com [51].

Турецькі науковці звертають увагу на напруженість між вимогами національної безпеки та захистом цифрових прав, що робить

турецьку модель показовою для аналізу меж допустимого конституційного обмеження цифрових свобод [44].

Окрім судової практики, важливим інструментом конституціоналізації цифрових прав є пряме нормативне закріплення у конституціях держав.

Конституцією Грузії визначено право на свободу переконань, інформації, засобів масової інформації та Інтернету, в межах якого акцентовано, що «всі мають право на доступ до Інтернету і вільне користування Інтернетом» [49].

Конституцію Греції доповнено ст. 5А(2), яка встановлює — «усі особи мають право брати участь в інформаційному суспільстві. Сприяння доступу до інформації, що передається в електронному вигляді, а також її виробництва, обміну та поширення є обов'язком держави» [50].

Конституція Португалії містить ст. 35 «Використання комп'ютерів», якою розкривається право на захист персональних даних та гарантується вільний доступ до комп'ютерних мереж загального користування [45].

Розмірковуючи про цифрові права та їх конституціоналізацію в Ірландії, Едоардо Селесте відзначає, що такі принципи як свобода інформації, захист даних та інформаційне самовизначення, доступ до Інтернету, навіть якщо визнані тільки на законодавчому рівні (не закріплені в тексті Конституції), походять із визнаних конституційних прав і часто включені в інші національні чи наднаціональні конституційні документи, а тому є «дуже близькими до конституційного кордону» [34].

Важливим етапом конституціоналізації цифрових прав стало також виокремлення права на захист персональних даних у Хартії основних прав Європейського Союзу, яке має тісний зв'язок із правом на приватність та розглядається як його похідний елемент [35].

Запровадження GDPR (General Data Protection Regulation) стало прикладом трансформації цього права у конкретний механізм правового захисту [41].

В Україні інфраструктура правової охорони та захисту цифрових прав формується в контексті євроінтеграційних зусиль. Так, Угодою про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (Угода про асоціацію з ЄС), передбачено, що одним із напрямів співробітництва є сприяння широкому доступу, поліпшенню безпеки мереж та широкому використанню інформаційно-телекомунікаційних технологій приватними особами, бізнесом та адміністративними органами шляхом розвитку локальних ресурсів Інтернет і впровадження онлайн-послуг, зокрема електронного бізнесу, електронного уряду, електронної охорони здоров'я і електронного навчання [27].

Так само, керівне значення має стаття 8 (1) Європейської конвенції з прав людини: «Кожен має право на невтручання у своє приватне і сімейне життя, у свою кореспонденцію». Проте це право на невтручання за статтею 8 (1) має застереження, що «його можна назвати винятком в інтересах спільноти, яке визнає, що права особи можна належним чином обмежувати в інтересах суспільства в цілому, якщо водночас виконано певні досить суворі умови» [2, с. 74].

Такими «суворими умовами», за словами Т. Бінгема, є інтереси національної безпеки, громадської убезпеченості або економічного добробуту країни, запобігання заворушенням або злочинам, захист здоров'я або моралі, захист прав і свобод інших осіб [2, с. 75].

При цьому, сама Європейська конвенція з прав людини може бути взірцем того, що в сучасній конституційній доктрині називають «парадигмою нормативної еквівалентності». Згідно останньої, завдяки використанню загальних термінологічних конструкцій, що відображають базові етичні та соціальні цінності, а не конкретні технологічні

обставини, ця Конвенція й подібні їй нормативно-правові акти залишаються актуальними в умовах змін, забезпечуючи гнучкість нормозастосування. Можна погодитися з висловленою в літературі думкою, що «саме завдяки цьому система захисту прав людини є актуальною впродовж тривалого часу. І саме цей аспект лежить в основі «парадигми нормативної еквівалентності», відповідно до якої наявні, передусім фундаментальні, права людини є достатніми для забезпечення захисту людей в онлайн-середовищі» [37].

В українському правопорядку конституціоналізація цифрових прав відбувається переважно шляхом інтерпретації традиційних прав Конституційним Судом України (далі — КСУ). Це обумовлено сутнісними відмінностями законодавчої й судової влади. Як вказується в літературі, «законодавчі органи займаються питаннями політики, яка спрямована на максимальне виконання інтересів чи уподобань громадян, тоді як суди — це принципові форуми, в яких права, що встановлюють обмеження на досягнення загального добробуту, визначаються, тлумачаться та застосовуються до конкретних обставин справи» [24, с. 205].

КСУ в Рішенні від 20 січня 2012 року № 2-рп/2012 наголосив, що збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручання в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини [19].

У Рішенні від 1 червня 2016 року № 2-рп/2016 КСУ зазначив, що у разі обмеження конституційного права або свободи законодавець зобов'язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію цього права або свободи і не порушувати сутнісний зміст такого права [17].

КСУ в Рішенні від 12 липня 2019 року № 5-р(I)/2019 також зазначив, що під правомірним обмеженням конституційних прав і свобод людини і громадянина слід розуміти передбачену Конституцією України можливість втручання держави за допомогою юридичних засобів у зміст та обсяг конституційних прав і свобод людини і громадянина, яке відповідає вимогам верховенства права, потрібності, доцільності та пропорційності у демократичному суспільстві; метою такого обмеження є охорона основоположних цінностей у суспільстві, до яких належать, зокрема, життя, свобода та гідність людини, здоров'я і моральність населення, національна безпека, громадський порядок [18].

КСУ у своєму рішенні від 22 січня 2020 року наголосив, що обмеження права на доступ до інформації мають здійснюватися з дотриманням принципу пропорційності та непорушності сутнісного змісту права [20].

Це рішення має безпосереднє значення для формування стандартів захисту цифрових прав в Україні. Його важливість суттєво зростає також з огляду на те, що, «практична реалізація більшості особистих, політичних, економічних і соціальних прав без доступу до сучасних інформаційно-комунікаційних технологій та їх безпосереднього використання є ускладненою, якщо взагалі можливою» [47].

Таким чином, право особи на доступ до інформації, гарантоване статтею 34 Конституції України, не є абсолютним і може підлягати обмеженням. Такі обмеження мають бути винятками, які передбачені законом, переслідувати одну або декілька законних цілей і бути необхідними у демократичному суспільстві. У разі обмеження права на доступ до інформації законодавець зобов'язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію вказаного права і не порушувати сутнісного змісту такого права.

Суттєвий вплив на розвиток конституційного виміру цифрових прав має концепція цифрового конституціоналізму, яка прагне відповісти на виклики правам і свободам людини в епоху цифрових технологій. Цифровий конституціоналізм структурно складається з трьох рівнів і їх загальної цілі. Рівнями є глобальний, суспільний та ліберальний. Ціллю — вироблення потенційного нормативного шляху подальшого розвитку, що є результатом взаємодії цих трьох рівнів. Глобальна, суспільна та ліберальна складові як три стовпи цифрового конституціоналізму звертаються до нормативного ядра конституціоналізму та пропонують структуру для переформатування захисту основних прав та обмежень людини в цифрову епоху. Ключ до розуміння цифрового конституціоналізму полягає у зв'язку між цими поглядами та становить нормативне розуміння наративу, яке забезпечує реалізацію цифрових прав та інформаційних потреб людини, дотримання принципу верховенства права та належне правове регулювання цих відносин, а також засоби правового захисту [9, с. 31].

Цифровий конституціоналізм спрямований на поступове впровадження ключових конституційних принципів у цифрове середовище. Його розвиток зумовлений не лише діяльністю держав, а й впливом приватних цифрових платформ, які дедалі більше визначають умови реалізації прав людини.

Як акцентує Е. Селесто, цифровий конституціоналізм визначає ідеологію, яка адаптує цінності сучасного конституціоналізму до особливостей цифрового суспільства, виступає за захист основних прав і збереження балансу влади в цифровому суспільстві [33].

Окремого аналізу потребує соціально-економічний вимір реалізації цифрових прав, насамперед права на доступ до Інтернету. Юридичне визнання цього права саме по собі не гарантує його ефективної реалізації. Реальний доступ до цифрових мереж можливий лише за умови створення відповідної інфраструктури, технологічної бази та економічних передумов.

На міжнародному рівні визнання цифрових прав людини знайшло відображення в резолюціях ООН, декларації Ради Європи та інших документах. Зокрема, у 2016 році ООН визнала право на доступ до Інтернету одним з базових прав людини [15].

Світовий досвід демонструє, що спектр державних зобов'язань у цій сфері є досить широким і включає сприяння цифровій грамотності, подолання гендерної нерівності, забезпечення доступності Інтернету для осіб з інвалідністю, зменшення інфраструктурної нерівності між регіонами, створення безкоштовних точок доступу у громадських місцях та підтримку соціально вразливих груп населення [26, с. 145].

Таким чином, конституціоналізація цифрових прав має супроводжуватися комплексною державною політикою у сфері цифрової інклюзії.

Особливе значення у цьому процесі має розвиток цифрової грамотності населення.

Важливим інституційним кроком у напрямі реалізації цифрових прав стало створення у 2019 році Міністерства цифрової трансформації України. До його повноважень віднесено формування та реалізацію державної політики у сфері розвитку цифрових навичок населення та забезпечення цифрових прав громадян [12].

Це стало інституційною відповіддю України на глобальну цифрову трансформацію як новий етап розвитку цивілізації, процес суспільно-економічної, гуманітарної та інформаційної модернізації.

Як слушно зазначає О. С. Гиляка, «в умовах цієї трансформації здійснюється глобальна електронізація даних, а значні обсяги персональних даних зберігаються у формі, доступній для передачі, поширення чи обміну на різних рівнях, в тому числі транснаціональному. Проте, такі процеси можуть бути ризикованими з погляду захисту персональних даних» [6, с. 19].

Запровадження цифрових платформ публічних послуг та розвиток електронного урядування сприяють практичній реалізації принципу доступності державних сервісів.

Разом із тим цифровізація державного управління супроводжується новими ризиками для прав людини. Зростання ролі автоматизованих систем та алгоритмічних рішень у публічному адмініструванні актуалізує проблему прозорості, підзвітності та недискримінаційного використання цифрових технологій.

Конституційні гарантії мають забезпечувати не лише доступ до цифрових сервісів, а й захист від зловживань цифровими інструментами.

Важливою складовою цифрового конституціоналізму є забезпечення балансу між свободою вираження поглядів та необхідністю протидії дезінформації, мові ворожнечі та кіберзагрозам. Цифрові технології створюють нові комунікативні можливості, але водночас спричиняють ризики політичного втручання, маніпуляцій громадською думкою та обмеження свободи слова, особливо в умовах авторитаризму та нестабільних демократій [26, с. 151].

Це потребує розроблення нових правових механізмів регулювання цифрового інформаційного простору.

Окремого значення набуває питання захисту персональних даних у контексті конституційних гарантій приватності. Конституційні права людини є фундаментом будь-якого демократичного суспільства, вони закріплюють можливості людини у різних сферах життя — приватній, політичній, соціально-економічній, культурній тощо. Відповідно, основними проблемами є забезпечення конфіденційності та безпеки особистих даних, регулювання використання штучного інтелекту та автоматизованих систем, а також забезпечення доступу до цифрових технологій для всіх верств суспільства. Українське законодавство, яке станом на сьогодні є недосконалим у цій сфері, повинно адаптуватися до нових викликів, визначаючи

чіткі рамки та принципи захисту прав громадян у цифровому просторі [29, с. 110].

Впровадження Загального регламенту з захисту даних (GDPR) та дотримання Європейської Конвенції з прав людини (ЄКПЛ) в українському правовому просторі є ключовими кроками в напрямку гарантування захисту приватності та прав громадян. Україна, бажаючи зблизити свої законодавчі акти з європейськими, прийняла ряд законів, які гармонізують внутрішні норми з вимогами GDPR. Наприклад, Закон України «Про захист персональних даних» [13] враховує ключові принципи GDPR та встановлює правила обробки та захисту персональних даних громадян.

GDPR визначає права і обов'язки відповідальних осіб щодо обробки персональних даних. Українське законодавство також враховує ці принципи, забезпечуючи високий стандарт захисту прав споживачів в сфері обробки їхніх персональних даних.

GDPR передбачає значні штрафи за порушення вимог щодо захисту персональних даних. Українське законодавство також встановлює відповідальність за порушення правил обробки особистої інформації, сприяючи формуванню ефективної системи відшкодування збитків [21].

Суттєвим викликом для сучасного конституційного права є вплив алгоритмічних систем і штучного інтелекту на процес реалізації прав людини. Використання автоматизованих систем прийняття рішень у публічному адмініструванні, фінансовому секторі, системах безпеки та соціального забезпечення створює нові ризики дискримінації, непрозорості управлінських процесів та порушення принципу рівності перед законом.

Тому конституціоналізація цифрових прав має включати гарантії алгоритмічної справедливості, прозорості та підзвітності державних і приватних суб'єктів, що використовують цифрові технології.

Водночас цифрові технології дедалі активніше використовуються в процесах політичної комунікації та демократичного врядування. Електронні петиції, онлайн-консультації, цифрові платформи участі громадян у прийнятті управлінських рішень розширюють можливості реалізації політичних прав. Однак така трансформація породжує й нові загрози — маніпуляцію інформаційними потоками, втручання у виборчі процеси, поширення дезінформації та використання персональних даних у політичних цілях.

Тому цифровий конституціоналізм повинен забезпечувати баланс між відкритістю цифрового простору та необхідністю захисту демократичних інститутів.

Особливу увагу у цьому контексті слід приділити ролі приватних цифрових платформ. Соціальні мережі, пошукові системи та онлайн-платформи фактично виконують функції «приватних регуляторів» інформаційного простору, визначаючи правила доступу до контенту, модерації інформації та алгоритмічного ранжування.

Це зумовлює необхідність переосмислення традиційної моделі конституційних правовідносин, у якій держава є основним суб'єктом гарантування прав людини. У цифрову епоху значна частина владних повноважень де-факто реалізується приватними корпораціями, що створює нові виклики для забезпечення верховенства права.

У цьому зв'язку в науковому дискурсі підкреслюється необхідність багаторівневого підходу до цифрового конституціоналізму. Йдеться не лише про державний рівень регулювання, а й про формування глобальних стандартів, саморегулювання цифрових платформ та участь громадянського суспільства у розробці цифрових політик.

Такий підхід відповідає сучасним тенденціям розвитку інформаційного суспільства та дозволяє врахувати транснаціональний характер цифрових відносин.

Значущим аспектом конституціоналізації цифрових прав є також проблема екстратериторіальності їх захисту. Цифрові платформи

діють у глобальному масштабі, тоді як механізми правового захисту залишаються переважно національними. Це створює ситуації, коли порушення прав людини відбуваються поза межами юрисдикції конкретної держави, що ускладнює доступ до ефективних засобів правового захисту [16].

У цьому контексті посилюється роль міжнародних стандартів та наднаціональних механізмів правового регулювання.

Окремої уваги заслуговує питання інформаційної безпеки як елементу конституційних гарантій цифрових прав. Стратегія кібербезпеки України визначає інформаційну безпеку як складову національної безпеки, що безпосередньо пов'язана із захистом прав і свобод людини в цифровому середовищі [14].

У підсумку можна констатувати, що процес конституціоналізації цифрових прав є складним і багатовекторним. Він поєднує міжнародні стандарти, судову практику, національні моделі конституційного закріплення та розвиток цифрового конституціоналізму як нової теоретичної парадигми. Саме ця багаторівнева модель створює передумови для формування ефективної системи гарантій прав людини в цифрову епоху.

4. Конституційні гарантії реалізації та захисту цифрових прав людини

Важливою складовою системи гарантій цифрових прав є нормативне забезпечення процедур доступу до цифрових публічних послуг. Перехід адміністративних процедур у цифровий формат зумовлює необхідність забезпечення рівності доступу громадян до електронних сервісів незалежно від місця проживання, соціального статусу та рівня цифрової грамотності.

Цифровізація публічного управління сприяє підвищенню ефективності адміністративних процесів, однак водночас потребує створення додаткових правових механізмів захисту прав користувачів електронних сервісів.

Особливого значення набуває принцип доступності цифрових сервісів. Він передбачає не лише технічну можливість користування електронними платформами, а й адаптацію цифрових ресурсів до потреб осіб з інвалідністю, людей похилого віку та соціально вразливих груп. Таким чином, забезпечення цифрових прав має розглядатися як складова реалізації принципу соціальної справедливості та рівності, що традиційно належить до фундаментальних конституційних цінностей.

Окрему увагу необхідно приділити гарантіям процесуальної справедливості в умовах автоматизованого управління. Використання алгоритмічних систем у сфері соціального забезпечення, адміністрування податків, надання державних послуг та правоохоронної діяльності створює нові ризики порушення прав людини. Адже автоматизовані рішення можуть бути непрозорими для громадян, що ускладнює можливість ефективного оскарження таких рішень і підриває принцип правової визначеності.

У цьому зв'язку важливим елементом гарантій цифрових прав є право особи на отримання інформації про логіку прийняття автоматизованих рішень та можливість людського перегляду результатів алгоритмічної обробки даних. Запровадження таких механізмів відповідає принципу верховенства права та забезпечує належний баланс між технологічною ефективністю та захистом прав людини.

Не менш значущим є питання відповідальності суб'єктів цифрових правовідносин. У цифровому середовищі порушення прав людини можуть здійснюватися як державними органами, так і приватними компаніями — операторами цифрових платформ, провайдерами послуг, власниками інформаційних ресурсів. Можна стверджувати, що конституційні відповіді на зміни, спричинені цифровими трансформаціями, не лише виникають у вимірах, які можна визначити як «класичні» в конституційній теорії, зокрема, на міжнародному, національному та регіональному рівнях,

і де державні інституції відіграють ще домінуючу роль, а й у нових контекстах, де, навпаки, домінують приватні компанії [9, с. 33].

Це зумовлює необхідність формування нових моделей регулювання, які поєднують публічно-правові та приватно-правові механізми захисту цифрових прав. Зокрема, йдеться про запровадження стандартів корпоративної відповідальності у сфері захисту персональних даних, алгоритмічної прозорості та модерації цифрового контенту.

У цьому контексті особливе значення має практика міжнародних судових органів, насамперед Європейського суду з прав людини, яка формує універсальні підходи до захисту свободи вираження поглядів, приватності та доступу до інформації в цифровому середовищі. Такі правові позиції сприяють поступовій гармонізації національних стандартів і зміцненню наднаціонального рівня захисту цифрових прав.

Окремим елементом системи гарантій цифрових прав є розвиток культури цифрової відповідальності в суспільстві. Формування правосвідомості у сфері цифрових прав передбачає не лише підвищення рівня цифрової грамотності, а й усвідомлення громадянами власних прав та обов'язків у цифровому просторі.

Система гарантій цифрових прав людини має комплексний характер і включає нормативні, інституційні, процедурні, судові та соціально-освітні елементи. Її ефективність визначається не лише рівнем правового регулювання, а й здатністю держави та суспільства адаптуватися до динамічних технологічних змін.

Розвиток конституційних гарантій цифрових прав має розглядатися як безперервний процес, спрямований на забезпечення реальної, а не формальної реалізації прав людини в цифрову епоху. Саме інтеграція правових, технологічних і соціальних механізмів створює умови для збереження фундаментальних конституційних цінностей у процесі цифрової трансформації держави і суспільства.

Суттєвим напрямом розвитку системи гарантій цифрових прав є формування правових механізмів захисту особи від надмірного цифрового контролю. Поширення технологій масового спостереження, біометричної ідентифікації, геолокаційного моніторингу та аналізу поведінкових даних створює ризики системного втручання у приватне життя людини. Сучасні цифрові технології здатні трансформувати державу у «цифрову наглядову систему», якщо відсутні належні правові обмеження та інституційні запобіжники.

Окремої уваги заслуговує проблема цифрової ідентифікації особи. Використання електронних документів, цифрових профілів, державних реєстрів і біометричних систем створює нові можливості для спрощення доступу до публічних послуг, однак одночасно підвищує ризики несанкціонованого доступу до персональних даних і зловживань інформацією. У цьому зв'язку ефективний захист цифрових прав передбачає не лише технічні засоби безпеки, а й чітке нормативне регулювання доступу до державних реєстрів та відповідальність за неправомірне використання даних.

Держава повинна виконувати регулятивну функцію, спрямовану на забезпечення конкуренції у цифровому середовищі, прозорості алгоритмічних механізмів та захисту користувачів від дискримінаційних практик. Такий підхід відповідає загальним принципам цифрового конституціоналізму, які передбачають адаптацію класичних механізмів стримувань і противаг до умов цифрової економіки.

Значущим гарантійним інструментом є також забезпечення права на цифрову автономію особи. Йдеться про можливість самостійно визначати обсяг використання персональних даних, обирати рівень цифрової присутності, контролювати власний інформаційний слід та користуватися механізмами права на забуття.

Рішення Суду Європейського Союзу у справі Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González стало поворотним моментом у формуванні

цього права, визнавши за особою можливість вимагати видалення застарілої або нерелевантної інформації з пошукових систем.

Заявник просив представників пошукової системи видалити посилання на публікацію 1998 року, де йшлося про розпродаж його майна за борги, аргументуючи тим, що проблема боргів давно врегульована і відповідна інформація застаріла. Представники пошукової системи Google зазначали, що керуються принципом нейтральності мережі Інтернет та відкритості інформації, що не передбачає контролю контенту. Однак Суд вказав, що діяльність пошукової системи з пошуку, зберігання та надання інформації через мережу Інтернету є обробкою даних в контексті Директиви 95/46/ЕС про захист персональних даних, а компанія, що використовує пошукову систему, відповідальна за таку обробку та зобов'язана контролювати процес обробки даних та забезпечувати суб'єктам персональних даних реалізацію всіх передбачених Директивою прав, зокрема і права на забуття. Суд дійшов висновку, що у цій справі захист персональних даних важливіший, ніж мережева нейтральність, та зобов'язав Google видалити відповідну інформацію [42].

Починаючи з 2013 року ООН прийняла дві резолюції з питань приватного життя під назвою «право на приватність у цифрову еру». Ці резолюції були ухвалені у відповідь на розвиток нових технологій та оприлюднення фактів масового спостереження в певних державах. У резолюціях засуджується масове спостереження і наголошується на його можливому впливі на такі засадничі права, як приватне життя та свобода вираження поглядів, а також на функціонування динамічного демократичного суспільства. Хоча резолюції не є юридично обов'язковими, вони дали поштовх важливій міжнародній дискусії високого рівня щодо приватності, нових технологій та спостереження. Вони також привели до запровадження посади Спеціального доповідача щодо права на приватне життя

з повноваженнями щодо популяризації та захисту цього права. Його конкретним завданням є збір інформації про підходи та досвід різних країн у питаннях приватності та про виклики, пов'язані з новими технологіями, обмін та популяризація найкращим досвідом, а також визначення потенційних перешкод [6, с. 24].

За словами Хелен Ніссенбаум, «недоторканність приватного життя — це не право на секретність чи контроль, а право на належний потік особистої інформації. Це означає, що залежно від ситуації та контексту, людина може оцінити та вирішити, чим поділитися з іншими у цифровому середовищі. Іншими словами, людина має право знати, як і для яких цілей використовуються її дані, хто і як довго їх зберігає, а також кому доступна така інформація. Особа повинна мати можливість звернутись про видалення особистих даних або їх виправлення» [43].

Не менш важливим є питання забезпечення цифрових прав у сфері праці. Поширення дистанційної роботи, платформенної зайнятості та автоматизованого управління персоналом зумовлює необхідність захисту трудових прав у цифровому середовищі. Алгоритмічне оцінювання продуктивності праці, цифровий моніторинг робочого часу та використання штучного інтелекту у кадрових процесах можуть призводити до порушення права на приватність, рівність і гідні умови праці. У цьому контексті цифрові права мають розглядатися як складова соціально-економічних гарантій.

Окремого аналізу потребує проблема цифрового суверенітету держави як чинника забезпечення прав людини. Залежність від іноземних цифрових платформ, хмарних сервісів і транснаціональних інформаційних інфраструктур створює ризики втрати контролю над даними громадян і критично важливою інформацією. Тому розвиток національних цифрових екосистем і власної інфраструктури кібербезпеки є важливим елементом захисту прав людини у цифровому просторі.

Водночас забезпечення цифрового суверенітету не повинно призводити до ізоляції інформаційного простору або необґрунтованих обмежень свободи слова. Тому державна політика у цій сфері має ґрунтуватися на принципах відкритості, пропорційності та дотримання міжнародних стандартів прав людини.

Гарантії цифрових прав не можуть обмежуватися лише формальним закріпленням правових норм. Вони повинні включати ефективні механізми реалізації, інституційну спроможність держави, високий рівень цифрової культури населення та розвинену правозастосовну практику.

Таким чином, конституційні гарантії цифрових прав людини формуються як динамічна система, здатна адаптуватися до технологічних змін і забезпечувати стабільність фундаментальних правових цінностей. Саме така модель дозволяє поєднати інноваційний розвиток цифрового суспільства із збереженням принципів верховенства права, правової визначеності та поваги до гідності людини.

Особливо важливою складовою гарантій цифрових прав виступає державна політика цифрової трансформації. В Україні перехід значної частини публічних послуг у цифровий формат призвів до формування моделі електронного урядування та цифрового державного управління, що істотно вплинуло на реалізацію права на інформацію, доступ до адміністративних процедур та участь громадян у публічному управлінні.

Запровадження цифрових платформ на кшталт «Дія» стало практичним інструментом забезпечення доступності державних сервісів.

Разом із тим цифровізація державних функцій супроводжується новими ризиками для прав людини. Автоматизація процесів, використання електронних реєстрів і масивів персональних даних підвищують загрозу порушення права на приватність на інформаційну безпеку.

Тому одним із ключових напрямів конституційних гарантій цифрових прав є захист персональних даних.

Важливу роль у цьому процесі відіграє гармонізація українського законодавства із європейськими стандартами захисту даних. Запровадження принципів GDPR у національну правову систему спрямоване на посилення гарантій приватності, встановлення чітких правил обробки персональної інформації та підвищення відповідальності суб'єктів, які здійснюють її обробку. Це дозволяє розглядати право на захист персональних даних як одну з ключових інституційних гарантій цифрових прав людини.

Окрему увагу необхідно приділити судовому захисту цифрових прав. Конституційний Суд України у своїй практиці підкреслює, що будь-яке обмеження права на доступ до інформації повинно відповідати принципу пропорційності та не порушувати сутнісного змісту права [20].

Такий підхід має фундаментальне значення для формування стандартів обмеження цифрових прав у демократичному суспільстві, оскільки дозволяє уникнути надмірного втручання держави у сферу цифрової свободи.

Разом із судовими механізмами важливу роль відіграють інституційні гарантії. Створення Міністерства цифрової трансформації України стало важливим кроком у формуванні централізованої державної політики у сфері цифрових прав, розвитку цифрових навичок населення та впровадження електронних сервісів [12].

Цей орган виконує функцію координації цифрових реформ та сприяє інституційному забезпеченню цифрової трансформації.

Окремим напрямом гарантій є забезпечення інформаційної безпеки. Стратегія кібербезпеки України визначає захист інформаційного простору як складову національної безпеки, безпосередньо пов'язану з охороною прав і свобод людини [14].

У цьому сенсі кібербезпека виступає не лише технічною, а й правозахисною категорією.

Таким чином, конституційні гарантії цифрових прав не можуть обмежуватися декларативним закріпленням окремих правомочностей. Вони мають охоплювати комплекс механізмів, спрямованих на забезпечення реальної доступності цифрових ресурсів, ефективного судового захисту та збереження фундаментальних конституційних цінностей у цифрову епоху.

5. Висновки

Цифрові права людини формуються як складна еволюційна категорія у системі прав людини, яка виникає внаслідок глибоких соціально-технологічних трансформацій сучасного суспільства. Вони не є ізольованим правовим явищем, а становлять органічне продовження інформаційних прав та класичних прав людини в умовах цифрового середовища.

Цифрові права характеризуються багатовимірною природою, що поєднує суб'єктивні правомочності, принципи реалізації прав у цифровому просторі, інституційні гарантії та механізми правового захисту. Їх розвиток відбувається у тісному взаємозв'язку з фундаментальними правами — свободою вираження поглядів, правом на інформацію, приватністю, правом участі в управлінні державними справами.

Процес конституціоналізації цифрових прав здійснюється у двох основних напрямах: через інтерпретаційне розширення змісту традиційних конституційних прав та шляхом прямого нормативного закріплення цифрових прав у конституційних актах окремих держав.

Міжнародні стандарти, судова практика Європейського суду з прав людини та досвід національних конституцій свідчать про поступове формування наднаціональної моделі цифрових прав людини.

Особливу роль у системі цифрових прав відіграє право на доступ до Інтернету, яке виступає базовою умовою реалізації інших прав у цифровому середовищі. Його правова природа має

міжпоколінний характер і поєднує ознаки інструментального та соціального права, реалізація якого залежить від створення відповідної інфраструктури та соціально-економічних умов в державі.

Важливим результатом дослідження є висновок про формування цифрового конституціоналізму як нової теоретичної парадигми, що адаптує класичні конституційні цінності до реалій цифрового суспільства. Цифровий конституціоналізм поєднує глобальні, національні та суспільні виміри правового регулювання і спрямований на забезпечення балансу між технологічним розвитком та захистом фундаментальних прав людини.

Ефективна реалізація цифрових прав неможлива без формування комплексної системи конституційних гарантій, яка включає нормативно-правове регулювання, судовий захист, інституційне забезпечення, розвиток цифрової грамотності населення та політику інформаційної безпеки.

Особливе значення у цьому контексті має діяльність спеціалізованих державних органів та гармонізація національного законодавства з європейськими стандартами захисту персональних даних.

Водночас сучасні виклики цифрової трансформації, а саме: алгоритмічне управління, діяльність приватних цифрових платформ, загрози інформаційній безпеці та цифрова нерівність потребують подальшого розвитку правових механізмів захисту цифрових прав людини. Це обумовлює необхідність удосконалення національного законодавства, розширення міжнародної співпраці та формування нових підходів до правового регулювання цифрового простору.

Отже, цифрові права людини у конституційно-правовому вимірі слід розглядати як стратегічний напрям розвитку сучасного конституційного права, що визначатиме подальшу еволюцію правового статусу особи в умовах цифрового суспільства та формуватиме основу для забезпечення гідності, свободи та рівності людини у цифрову епоху.

Список використаних джерел:

1. Бєлов Д. М., Переш І. Є., Покорба І. Цифрові права людини: доктринальні засади. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 110–115. DOI: https://doi.org/10.24144/2788-6018.2024.02.17.

2. Бінгем Т. Правовладдя / за ред. С. Головатого. пер. з англ. В. Кастеллі та Д. Шкрьоби. Київ : PENGUIN BOOKS, 2024. 212 с.

3. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал*. 2021. № 10. С. 58–61. DOI: https://doi.org/10.32782/2524-0374/2021-10/12.

4. Венгер В., Кошман А. Права людини в цифрову епоху: процедурні гарантії та судовий захист. *Наукові записки НаУКМА. Серія: Юридичні науки*. Т. 16. 2025. С. 18–28. URL: https://doi.org/10.18523/2617-2607.2025.16.18-28.

5. Верлос Н. В. Конституціоналізація цифрових прав людини: вітчизняна практика та зарубіжний досвід. *Часопис Київського університету права*. 2020. № 2. С. 129–133. DOI: https://doi.org/10.36695/2219-5521.2.2020.21.

6. Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України.* Т. 30. № 1. 2023 С. 15–30. DOI: 10.31359/1993-0909-2023-30-1-15.

7. Загальна теорія права : підручник / за ред. О. В. Петришина. Харків : Право, 2020. 568 с.

8. Конституційне право : навч. посібник / Д. Терлецький, М. Афанасьєва, Ю. Батан та ін. ; за заг. ред. Д. Терлецького ; НУ «Одес. юрид. академія». Одеса : Фенікс, 2023. 584 с.

9. Кушакова-Костицька Н. Вплив цифровізації на конституціоналізм: концептуальні підходи щодо перспектив державного регулювання інформаційного простору. *Філософські та методологічні проблеми права*. 2025. № 1 (29). С. 29–37. DOI: 10.33270/02252901.4.

10. Мединська О. Я., Синоруб Г. П. Права людини та цифрова трансформація. *Людина в українському суспільстві в системі цінностей прав людини: сучасний вимір медіадіяльності* : матер. Всеукр.

наук.-практ. конф., (Київ, 14 трав. 2021 р.). Київ : Інститут журналістики, 2021. С. 192–196.

11. Оніщенко Н. М. Проблеми реалізації прав і свобод людини та громадянина в України : моногр. / кол. авт. ; за ред. Н. М. Оніщенко, О. В. Зайчука. Київ, 2007. 424 с.

12. Про затвердження Положення про Міністерство цифрової трансформації України : Постанова Кабінету Міністрів України від 18.09.2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text

13. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України ; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

15. Рада ООН з прав людини ухвалила резолюцію про права онлайн. URL: https://cedem.org.ua/news/rada-oon-z-prav-lyudyny-uhvalyla-rezolyutsiyu-pro-prava-onlajn/

16. Размєтаєва Ю. С. Цифрові права людини та проблеми екстратериторіальності в їх захисті. *Право та державне управління*. 2020. № 4. С. 12–23. DOI: https://doi.org/10.32840/pdu.2020.4.2.

17. Рішення Конституційного Суду України від 1 червня 2016 року № 2-рп/2016 КСУ. URL: https://zakon.rada.gov.ua/laws/show/v002p710-16#Text

18. Рішення Конституційного Суду України від 12 липня 2019 року № 5-р(I)/2019. URL: https://zakon.rada.gov.ua/laws/show/va05p710-19#Text

19. Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

20. Рішення Конституційного Суду України від 22 січня 2020 року № 1-р(I)/2020. URL: https://zakon.rada.gov.ua/laws/show/va01p710-20/conv/parach_4:pu1:ch_2:zg_1/sp:dark#n14

21. Савицький О. В. Гармонізація законодавства України та Європейського Союзу у сфері захисту персональних даних. Київ, 2017. 188 с.

22. Сапарова А. О. Переосмислення прав людини в цифрову епоху: загрози і виклики. Захист прав людини в Україні в умовах воєнного стану та у післявоєнний період : збірник тез Міжнародної науково-практичної конференції Двадцять четверті осінні юридичні читання (м. Хмельницький, 23 жовтня 2025 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2025. С. 40–42.

23. Скіннер Кріс Людина цифрова / пер. з англ. Г. Якубовська. Харків : Вид-во «Ранок» ; Фабула, 2020. 272 с.

24. Тасіулас Джон Порятунок прав людини від права прав людини. *Філософія права і загальна теорія права*. № 1. 2020. С. 172–215. DOI: https://doi.org/10.21564/2227-7153.2020.1.219080.

25. Тиріна М. Покоління прав людини: проблеми сучасної класифікації. *Держава і право*. 2011. Вип. 52. С. 728–732.

26. Тихомиров О. О. Права людини: інформаційний вимір : монографія. Одеса : Видавництво «Юридика», 2023. 304 с. DOI: 10.32782/978-617-8263-30-0.

27. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Міжнародний документ від 27.06.2014. URL: http://zakon3.rada.gov.ua/laws/show/984_011

28. Удовика Л. Г. Права людини в умовах глобалізації. Велика українська юридична енциклопедія: у 20-ти т. Т. 2 : Філософія права / ред. кол.: С. І. Максимов (голова) та ін. Харків : Право, 2017. С. 603–606.

29. Чалчинський В. І. Сучасні тенденції забезпечення конституційних прав людини в умовах цифровізації. *Науковий часопис УДУ імені Михайла Драгоманова. Серія 18: Право.* 2024. Вип. 41. С. 110–120. DOI: https://doi.org/10.31392/NPU-nc.series18.2024.41.15.

30. Шваб Клаус. Четверта промислова революція, Формуючи четверту промислову революцію. Харків : Клуб сімейного дозвілля. 416 с.

31. 93 % українців володіють цифровими навичками: дослідження. URL: https://zib.com.ua/ua/159102.html

32. Bart Custers New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*. Vol. 44. April 2022. P. 1–13. DOI: https://doi.org/10.1016/j.clsr.2021.105636.

33. Celeste E. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*. 2019. 33(1). P. 76–99. DOI: 10.1080/13600869.2019.1562604.

34. Celeste E. The Irish Constitution and the Challenges of the Digital Age. Is it time for a Bunreacht na hÉireann 2.0? URL: https://ulsites.ul.ie/law/sites/default/files/Edoardo%20Celeste%20-%20Challenges%20of%20the%20Digital%20Age.pdf.

35. Charter of Fundamental Rights of the European Union (2000/C 364/01). URL: https://www.europarl.euro pa.eu/charter/pdf/text_en.pdf

36. Constitution of the Republic of Turkey. URL: https://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2024)029-e

37. Cristina Cocito, Paul De Hert The Transformative Nature of the EU Declaration on Digital Rights and Principles: Replacing the Old Paradigm (Normative Equivalency of Rights). *Computer Law & Security Review*. Vol. 50. 2023. DOI: https://doi.org/10.1016/j.clsr.2023.105846.

38. Digital democracy with a purpose. Lisbon declaration. URL: https://www.lisbondeclaration.eu/

39. European Court of Human Rights. Case of Ahmet Yildirim v. Turkey (Application no. 3111/10). URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-115705%22]}

40. European Declaration on Digital Rights and Principles for the Digital Decade. Brussels, 26.1.2022 COM(2022) 28 final. URL: https://digital-strategy.ec.europa.eu/en/library/decla¬ration-european-digital-rights-and-principles#Declaration

41. General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. URL: https://gdpr.eu/tag/gdpr/

42. Google Spain SL, Google Inc.v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Judgment of the Court (Grand Chamber) of 13 May 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

43. Nissenbaum H. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*. 1998. Vol. 17. P. 559–596. URL: https://nissenbaum.tech.cornell.edu/papers/privacy. pdf

44. Özbudun Ergun The constitutional system of Turkey: 1876 to the present. PALGRAVE MACMILLAN, 2011. DOI: 10.1057/9780230337855.

45. Portugal's Constitution of 1976 with Amendments through 2005. URL: https://www.constituteproject.org/constitution/Portugal_2005.pdf

46. Report of the special rapporteur on the promotion and protection of the right to free¬dom of opinion and expression, Frank La Rue, A/HRC/17/27, Human Rights Council, 16 May 2011. URL: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

47. Rights in the digital age challenges and ways forward OECD. Digital Economy Papers. December 2022. № 347. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf

48. The Charter of Digital Rights: A guide for policy-makers. The EDRi papers. URL: https://edri.org/wp-content/uploads/2014/06/EDRi_DigitalRightsCharter_web.pdf

49. The Constitution of Georgia. URL: https://matsne.gov.ge/en/document/view/ 30346?publication=36

50. The Constitution of Greece — Hellenic Parliament. URL: https://www.hellenicparliament.gr/en/Vouli-ton-Ellinon/To-Politevma/Syntagma/

51. The Decision of the Constitutional Court of Turkey on Omnibus Bill No. 6552 amending the Law on Regulation of Publications on the Internet and Suppression of Crimes Committed

by Means of such Publications, No. 5651 (Internet Law). URL: https://globalfreedomofexpression.columbia.edu/cases/the-turkish-twitter-case-of-2014/

52. The promotion, protection and enjoyment of human rights on the Internet. Resolution adopted by the Human Rights Council on 13 July 2021 47/16. URL: https://digitallibrary.un.org/record/3937534?v=pdf#files

53. The right to Internet access. Parliamentary Assembly Resolution 1987 (2014). Final version. URL: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid= 20870&lang=en

References:

1. Belov, D. M., Peresh, I. Ye., & Pokorba, I. (2024). *Tsyfrovi prava liudyny: Doktrynalni zasady. Analitychno-porivnialne pravoznavstvo*, (2), 110–115. https://doi.org/10.24144/2788-6018.2024.02.17.

2. Bingham, T. (2024). Pravovladdia (S. Holovatyi, Ed.; V. Kastelli & D. Shkroba, Trans.). Penguin Books.

3. Bratasiuk, O. B., & Mentukh, N. F. (2021). Poniattia ta klasyfikatsiia tsyfrovykh prav v Ukraini. *Yurydychnyi naukovyi elektronnyi zhurnal*, (10), 58–61. https://doi.org/10.32782/2524-0374/2021-10/12.

4. Venger, V., & Koshman, A. (2025). Prava liudyny v tsyfrovu epokhu: Protsedurni harantii ta sudovyi zakhyst. *Naukovi zapysky NaUKMA. Yurydychni nauky*, 16, 18–28. https://doi.org/10.18523/2617-2607.2025.16.18-28

5. Verlos, N. V. (2020). Konstytutsionalizatsiia tsyfrovykh prav liudyny: Vitchyzniana praktyka ta zarubizhnyi dosvid. *Chasopys Kyivskoho universytetu prava*, (2), 129–133. https://doi.org/10.36695/2219-5521.2.2020.21

6. Hyliaka, O. S. (2023). Pravo na pryvatnist ta zakhyst personalnykh danykh v umovakh tsyfrovizatsii. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*, 30(1), 15–30. https://doi.org/10.31359/1993-0909-2023-30-1-15.

7. Petryshyn, O. V. (Ed.). (2020). Zahalna teoriia prava. Pravo.

8. Terletskyi, D. (Ed.). (2023). Konstytutsiine pravo. Feniks.

9. Kushakova-Kostytska, N. (2025). Vplyv tsyfrovizatsii na konstytutsionalizm: Kontseptualni pidkhody shchodo perspektyv derzhavnoho rehuliuvannia. *Filosofski ta metodolohichni problemy prava*, 1(29), 29–37. https://doi.org/10.33270/02252901.4

10. Medynska, O. Ya., & Synorub, H. P. (2021). Prava liudyny ta tsyfrova transformatsiia. *In Liudyna v ukrainskomu suspilstvi v systemi tsinnostei prav liudyny* : Proceedings of the All-Ukrainian scientific conference (pp. 192–196).

11. Onishchenko, N. M. (Ed.). (2007). Problemy realizatsii prav i svobod liudyny ta hromadianyna v Ukraini.

12. Cabinet of Ministers of Ukraine. (2019). Pro zatverdzhennia Polozhennia pro Ministerstvo tsyfrovoi transformatsii Ukrainy (Resolution No. 856). Retrieved from https://zakon.rada.gov.ua/laws/show/856-2019-п

13. Law of Ukraine. (2010). Pro zakhyst personalnykh danykh (No. 2297-VI). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17

14. President of Ukraine. (2021). Pro Stratehiiu kiberbezpeky Ukrainy (Decree No. 447/2021). Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021

15. Human Rights Council. (n.d.). Resolution on rights online. Retrieved from https://cedem.org.ua/news/rada-oon-z-prav-lyudyny-uhvalyla-rezolyutsiyu-pro-prava-onlajn/

16. Razmetaieva, Yu. S. (2020). Tsyfrovi prava liudyny ta problemy ekstraterytorialnosti v yikh zakhysti. *Pravo ta derzhavne upravlinnia*, (4), 12–23. https://doi.org/10.32840/pdu.2020.4.2

17. Constitutional Court of Ukraine. (2016). Decision No. 2-rp/2016. https://zakon.rada.gov.ua/laws/show/v002p710-16#Text

18. Constitutional Court of Ukraine. (2019). Decision No. 5-r(I)/2019. https://zakon.rada.gov.ua/laws/show/va05p710-19#Text

19. Constitutional Court of Ukraine. (2012). Decision No. 2-rp/2012. https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

20. Constitutional Court of Ukraine. (2020). Decision No. 1-r(I)/2020. Retrieved from https://zakon.rada.gov.ua/laws/show/va01p710-20/conv/parach_4:pu1:ch_2:zg_1/sp:dark#n14

21. Savytskyi, O. V. (2017). Harmonizatsiia zakonodavstva Ukrainy ta YeS u sferi zakhystu personalnykh danykh.

22. Saparova, A. O. (2025). Pereosmyslennia prav liudyny v tsyfrovu epokhu: Zahrozy i vyklyky. In Proceedings of the international scientific conference (pp. 40–42).

23. Skinner, C. (2020). Liudyna tsyfrova (H. Yakubovska, Trans.). Ranok.

24. Tasioulas, J. (2020). Poriatunok prav liudyny vid prava prav liudyny. *Filosofiia prava i zahalna teoriia prava*, (1), 172–215. https://doi.org/10.21564/2227-7153.2020.1.219080.

25. Tyrina, M. (2011). Pokolinnia prav liudyny: Problemy suchasnoi klasyfikatsii. *Derzhava i pravo*, 52, 728–732.

26. Tykhomyrov, O. O. (2023). Prava liudyny: Informatsiinyi vymir. Yurydyka. https://doi.org/10.32782/978-617-8263-30-0.

27. Association Agreement between Ukraine and the European Union. (2014). Retrieved from http://zakon3.rada.gov.ua/laws/show/984_011

28. Udovyka, L. H. (2017). Prava liudyny v umovakh hlobalizatsii. In Velyka ukrainska yurydychna entsyklopediia (Vol. 2, pp. 603–606).

29. Chalchynskyi, V. I. (2024). Suchasni tendentsii zabezpechennia konstytutsiinykh prav liudyny v umovakh tsyfrovizatsii. *Naukovyi chasopys UDU*, 41, 110–120. https://doi.org/10.31392/NPU-nc.series18.2024.41.15.

30. Schwab, K. (2016). The fourth industrial revolution.

31. ZIB. (n.d.). 93 % ukraintsiv volodiiut tsyfrovymy navychkamy. Retrieved from https://zib.com.ua/ua/159102.html

32. Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*, 44, 1–13. https://doi.org/10.1016/j.clsr.2021.105636.

33. Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, 33(1), 76–99. https://doi.org/10.1080/13600869.2019.1562604.

34. Celeste, E. (n.d.). The Irish constitution and the challenges of the digital age. Retrieved from https://ulsites.ul.ie/law/sites/default/files/Edoardo%20Celeste%20-%20Challenges%20of%20the%20Digital%20Age.pdf

35. Charter of Fundamental Rights of the European Union. (2000). https://www.europarl.euro pa.eu/charter/pdf/text_en.pdf

36. Constitution of the Republic of Turkey. https://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2024)029-e

37. Cocito, C., & De Hert, P. (2023). The transformative nature of the EU declaration on digital rights and principles. *Computer Law & Security Review*, 50. https://doi.org/10.1016/j.clsr.2023.105846.

38. Digital democracy with a purpose. Lisbon declaration. Retrieved from https://www.lisbondeclaration.eu/

39. European Court of Human Rights. Case of Ahmet Yildirim v. Turkey (Application no. 3111/10). Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-115705%22]}

40. European Declaration on Digital Rights and Principles for the Digital Decade. Brussels, 26.1.2022 COM(2022) 28 final. Retrieved from https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration

41. General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Retrieved from https://gdpr.eu/tag/gdpr/

42. Google Spain SL, Google Inc.v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Judgment of the Court (Grand Chamber) of 13 May 2014. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

43. Nissenbaum, H. (1998). Protecting privacy in an information age. *Law and Philosophy*, 17, 559–596. https://nissenbaum.tech.cornell.edu/papers/privacy. pdf

44. Özbudun, E. (2011). The constitutional system of Turkey. Palgrave Macmillan.

45. Portugal's Constitution of 1976 with Amendments through 2005. https://www.constituteproject.org/constitution/Portugal_2005.pdf

46. Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, Human Rights Council, 16 May 2011. Retrieved from https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

47. Rights in the digital age challenges and ways forward OECD. Digital Economy Papers. December 2022. № 347. Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf

48. The Charter of Digital Rights: A guide for policy-makers. The EDRi papers. Retrieved from https://edri.org/wp-content/uploads/2014/06/EDRi_DigitalRightsCharter_web.pdf

49. The Constitution of Georgia. Retrieved from https://matsne.gov.ge/en/document/view/ 30346?publication=36

50. The Constitution of Greece — Hellenic Parliament. Retrieved from https://www.hellenicparliament.gr/en/Vouli-ton-Ellinon/To-Politevma/Syntagma/

51. The Decision of the Constitutional Court of Turkey on Omnibus Bill No. 6552 amending the Law on Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications, No. 5651 (Internet Law). Retrieved from https://globalfreedomofexpression.columbia.edu/cases/the-turkish-twitter-case-of-2014/

52. The promotion, protection and enjoyment of human rights on the Internet. Resolution adopted by the Human Rights Council on 13 July 2021 47/16. Retrieved from https://digitallibrary.un.org/record/3937534?v=pdf#files

53. The right to Internet access. Parliamentary Assembly Resolution 1987 (2014). Final version. Retrieved from https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid= 20870&lang=en

ПУБЛІЧНО-ПРИВАТНА СПІВПРАЦЯ У СФЕРІ КІБЕРБЕЗПЕКИ: БАЛАНС ІНТЕРЕСІВ ДЕРЖАВИ, БІЗНЕСУ ТА СУСПІЛЬСТВА

PUBLIC-PRIVATE COOPERATION IN CYBERSECURITY: BALANCE OF INTERESTS OF THE STATE, BUSINESS, AND SOCIETY

Slobodianiuk M. A.,
Candidate of Law,
Associate Professor of the Department
of Administrative and Financial Law,
National University "Odesa Law Academy",
Odesa, Ukraine

Abstract. This monograph is devoted to a comprehensive legal analysis of public-private cooperation (PPC) in the field of cybersecurity under the conditions of accelerated digital transformation, hybrid warfare, systemic cyber threats, and European integration processes as of 2026. The study proceeds from the premise that cybersecurity has evolved from a sectoral technical domain into a multidimensional legal category integrating elements of national security, administrative regulation, corporate governance, digital economy regulation, and the protection of fundamental human rights.

In contemporary conditions, cyber threats are no longer limited to isolated incidents of unauthorized access or data breaches.

They constitute complex, often state-sponsored or transnationally coordinated activities aimed at disrupting critical infrastructure, financial stability, public administration systems, and democratic processes. For Ukraine, which continues to resist large-scale military aggression while simultaneously pursuing integration into the European legal space, cybersecurity has become a core component of national resilience and sovereign capacity.

The rapid development of artificial intelligence, cloud computing, and large-scale data processing technologies further increases the complexity of cyber risk management and reinforces the need for coordinated governance mechanisms involving both public authorities and private technological actors.

Particular attention is paid to the transformation of the European Union's regulatory framework towards a resilience-oriented governance model. This shift is reflected primarily in Directive (EU) 2022/2557 [1], which establishes a legal framework for the resilience of critical entities, and in Directive (EU) 2022/2555 [2], which significantly strengthens cybersecurity obligations for essential and important entities across the Union. These instruments demonstrate the transition from a reactive security paradigm to a proactive, risk-based, and governance-centered model, emphasizing accountability of management bodies, mandatory risk management systems, and structured incident reporting mechanisms.

The research substantiates that cybersecurity should be understood as a systemic legal institution that operates at the intersection of public and private law. On the one hand, the state retains its constitutional obligation to ensure national security and protect public interests. On the other hand, the majority of digital and critical infrastructure assets are owned, operated, or technically maintained by private entities. This structural interdependence necessitates a legally formalized and institutionally coordinated model of public-private cooperation.

The subject of the study is the system of legal norms, institutional mechanisms, and practical models regulating public-private cooperation in the field of cybersecurity, as well as the balance of interests between the state, private sector entities, and society in ensuring cyber resilience. The research encompasses both supranational EU regulations and Ukrainian national legislation, including the Constitution of Ukraine [3], sectoral cybersecurity legislation, and strategic policy documents adopted in the context of wartime governance and post-war reconstruction planning.

The purpose of the study is to develop a comprehensive doctrinal and practical concept of public-private cooperation in cybersecurity, to determine its legal nature as an institution of public law with hybrid characteristics, and to substantiate mechanisms for achieving a balanced interaction between public security objectives, economic freedoms of business entities, and the protection of fundamental human rights. The monograph also aims to identify structural gaps in Ukrainian legislation and propose directions for harmonization with EU standards as of 2026.

The scientific novelty of the research lies in the development of an integrated legal model of public-private cooperation in cybersecurity adapted to the conditions of hybrid warfare, digital transformation, and EU legal approximation as of 2026. The study also proposes a conceptual framework for balancing security interests, economic freedoms, and fundamental human rights in the governance of cyber resilience.

The research methodology is based on a combination of general scientific and special legal methods. The dialectical method enabled the analysis of cybersecurity as a dynamic and evolving legal phenomenon influenced by technological, geopolitical, and economic factors. The comparative legal method was applied to examine the EU regulatory framework and its interaction with Ukrainian legislation, as

well as national regulatory approaches in selected EU member states (Germany, France, and the Netherlands).

The systemic-structural method facilitated the identification of institutional elements of public-private cooperation and their functional interrelations. The formal-legal method was used for the interpretation of normative acts, including the Constitution of Ukraine [3] and EU secondary legislation. In addition, elements of risk-based analysis were applied to assess the practical implementation of cyber resilience policies, especially in sectors of critical infrastructure such as energy, finance, and digital public services.

The study demonstrates that public-private cooperation in cybersecurity is not merely a contractual or voluntary arrangement but a structurally embedded governance mechanism. In the EU model, private operators of essential services are entrusted with legally binding obligations that reflect public interests. Management bodies bear direct responsibility for compliance failures, while supervisory authorities exercise risk-based oversight. Financial instruments, including recovery and resilience funding mechanisms, complement regulatory measures by supporting investments in digital security and infrastructural modernization. These mechanisms include targeted funding programs, innovation support schemes, and cross-sectoral investments in digital infrastructure security, which demonstrate the importance of combining regulatory obligations with economic incentives.

In the Ukrainian context, public-private cooperation has developed under conditions of ongoing military aggression, which has intensified cyber threats and accelerated institutional reforms. The monograph emphasizes that Ukraine's harmonization with EU standards is not limited to formal legislative transposition but requires deeper institutional restructuring, capacity building, and the establishment of sustainable financial mechanisms for cyber resilience. Particular challenges include ensuring proportionality of regulatory measures,

preventing excessive administrative burdens on businesses, and safeguarding human rights during emergency or wartime measures.

The study concludes that public-private cooperation in cybersecurity has become a system-forming element of modern national security policy. The European Union model demonstrates a high level of regulatory coherence, institutional coordination, and financial support mechanisms for cyber resilience. Ukraine, in turn, is undergoing an active phase of harmonization with EU standards while simultaneously addressing the challenges posed by ongoing military aggression and the need for post-war reconstruction of digital and physical infrastructure.

An effective balance of interests requires:

— clear legal delineation of powers and responsibilities between public authorities and private operators;

— proportionality and legal certainty of regulatory measures;

— transparent and enforceable mechanisms of accountability, including management-level responsibility;

— Sustainablefinancial instruments for supporting cyber resilience, including co-financing models and incentives;

— procedural safeguards to ensure the protection of fundamental human rights, especially privacy, data protection, and freedom of expression.

The monograph argues that cybersecurity in 2026 should be regarded as a shared public good, the protection of which depends on structured cooperation, mutual trust, institutional transparency, and a legally defined distribution of risks and responsibilities among the state, business, and society. Only through such an integrated and balanced approach can states ensure digital sovereignty, economic stability, and the protection of democratic values in an increasingly contested and technologically complex global environment. The findings of this research may contribute to the development of

national cybersecurity strategies, legislative reforms, and institutional cooperation mechanisms both in Ukraine and in other states facing hybrid security challenges.

Keywords: Public-Private Partnership, Cybersecurity, Public Interests, Balance of Interests, State Regulation, Digital Security.

1. Вступ

У XXI столітті кіберпростір остаточно перетворився на повноцінний стратегічний домен функціонування держави, економіки та суспільства. Якщо ще два десятиліття тому цифрова інфраструктура сприймалася як допоміжний технологічний ресурс, то станом на 2026 рік вона стала критично важливою складовою національної безпеки, економічної стабільності та гарантування прав людини. Для України ця трансформація має особливо драматичний вимір, адже відбувається в умовах триваючої збройної агресії, системних кібератак на об'єкти критичної інфраструктури та цілеспрямованого використання цифрового середовища як інструменту гібридного впливу. Зокрема, кібератаки на енергетичну систему України у 2015–2016 рр., масштабні атаки із використанням шкідливого програмного забезпечення NotPetya у 2017 році та численні інциденти під час повномасштабної агресії Російської Федерації після 2022 року продемонстрували вразливість критичної цифрової інфраструктури та необхідність системної модернізації механізмів кіберзахисту.

У 2026 році кібербезпека дедалі більше пов'язується з категорією цифрового суверенітету, що означає здатність держави самостійно визначати правила функціонування цифрового середовища, контролювати критичні дані та забезпечувати технологічну автономію в умовах зовнішнього впливу. Ця концепція активно розвивається у праві Європейського Союзу та міжнародному праві і передбачає не лише технічний контроль над цифровою інфраструктурою,

але й нормативну спроможність держави визначати правила обігу даних, кіберзахисту та функціонування цифрових платформ.

По-перше, кібербезпека сьогодні є невід'ємною складовою національної безпеки у її класичному розумінні як стану захищеності життєво важливих інтересів особи, суспільства і держави. Відповідно до Закону України «Про національну безпеку України» [4], кібербезпека визначається одним із пріоритетних напрямів державної політики у сфері безпеки і оборони. Одночасно Закон України «Про критичну інфраструктуру» [5] закріплює правові та організаційні засади функціонування системи захисту критичної інфраструктури, що охоплює енергетику, транспорт, фінансовий сектор, охорону здоров'я, телекомунікації та цифрові реєстри. Масовані атаки на енергетичну систему, банківські установи, державні електронні сервіси та системи зв'язку переконливо засвідчили, що цифровий компонент є невід'ємною частиною критичних функцій держави.

По-друге, розвиток цифрової економіки призвів до того, що значна частина інфраструктури, від якої залежить життєдіяльність суспільства, перебуває у власності або під управлінням приватних суб'єктів. Оператори телекомунікацій, банківські установи, енергетичні компанії, хмарні провайдери, великі ІТ-компанії фактично забезпечують функціонування сервісів, що мають публічне значення. За таких умов держава об'єктивно не може гарантувати кіберстійкість виключно адміністративними засобами. Виникає необхідність формування сталої моделі публічно-приватної співпраці, яка забезпечує координацію, розподіл відповідальності та узгодження інтересів.

У європейському праві ця трансформація отримала чітке нормативне оформлення. Зокрема, Directive (EU) 2022/2557 [1] закріплює концепцію стійкості критичних суб'єктів, що передбачає їхню здатність запобігати інцидентам, протидіяти їм та відновлювати функціонування після кризових подій. Паралельно Directive

(EU) 2022/2555 [2] формує сучасну модель кіберстійкості, яка базується на ризикоорієнтованому управлінні, посиленій відповідальності керівництва компаній та обов'язковому повідомленні про інциденти. Йдеться про так звану директиву NIS2, яка істотно розширює коло суб'єктів регулювання, посилює вимоги до управління кіберризиками та передбачає більш жорстку систему відповідальності за порушення вимог кібербезпеки. Ці акти не лише розширюють сферу регулювання, але й концептуально змінюють співвідношення між державою і бізнесом у сфері безпеки, фактично перетворюючи приватних операторів на співвідповідальних суб'єктів публічної політики.

Для України питання імплементації європейських стандартів має стратегічне значення у контексті виконання зобов'язань за Association Agreement between the European Union and Ukraine [6]. Гармонізація законодавства у сфері кібербезпеки передбачає не лише формальне приведення нормативних актів у відповідність до acquis ЄС, але й зміну концептуального підходу до розуміння кіберстійкості як спільної відповідальності держави та приватного сектору.

В умовах післявоєнної реконструкції цифрової та енергетичної інфраструктури питання кіберстійкості набуває інвестиційного виміру. Від рівня правової визначеності та прозорості механізмів публічно-приватної співпраці залежить залучення міжнародних фінансових ресурсів та участь приватного сектору у відновленні держави.

Разом з тим питання безпеки не може розглядатися ізольовано від проблематики прав людини. Конституційні гарантії, закріплені в конституції України від 28 червня 1996 року № 254к/96-ВР [3], зобов'язують державу забезпечувати права і свободи навіть в умовах воєнного стану. Тому будь-які заходи кіберзахисту повинні відповідати принципам законності, пропорційності та правової визначеності. З одного боку, держава має право й обов'язок запобігати загрозам; з іншого — надмірне втручання у діяльність бізнесу

або у сферу приватності громадян може підірвати довіру до самої системи безпеки. Ці принципи випливають як із Конституції України, так і з практики Європейського суду з прав людини щодо допустимості втручання держави у сферу приватності та обробки персональних даних.

Окремого значення набуває міжнародно-правовий вимір кібербезпеки, зокрема питання відповідальності держав за кібератаки, що мають транскордонний характер, та формування глобальних стандартів поведінки у кіберпросторі. У міжнародному праві поступово формується система принципів відповідальної поведінки держав у кіберпросторі, що розробляється в рамках Організації Об'єднаних Націй та інших міжнародних майданчиків.

Саме в цьому контексті публічно-приватна співпраця набуває значення юридичного механізму реалізації публічного інтересу. У теорії права публічний інтерес розглядається як узагальнення соціально значущих потреб, що визнаються державою і забезпечуються нею через правові інструменти. У цифрову епоху таким інтересом є стабільність функціонування електронних сервісів, захист персональних даних, безперервність енергопостачання та збереження довіри до цифрової держави.

Актуальність теми зумовлена тим, що 2026 рік характеризується одночасним впливом трьох процесів: воєнного протистояння, цифрової трансформації та європейської інтеграції. По-перше, зростає складність і масштаб кібератак, що потребує переходу від реактивної моделі захисту до системної моделі кіберстійкості. По-друге, цифровізація публічних послуг підвищує залежність держави від приватних технологічних рішень. По-третє, імплементація європейських директив вимагає переосмислення механізмів відповідальності, фінансування та державного нагляду.

Наукова новизна дослідження полягає у комплексному теоретико-правовому осмисленні публічно-приватної співпраці

як самостійного інституту публічного права, що функціонує на перетині національної безпеки, адміністративного регулювання та господарської діяльності. У роботі обґрунтовується підхід до розгляду публічно-приватної співпраці у сфері кібербезпеки не лише як інструменту договірного партнерства, але як принципу організації сучасної безпекової політики.

Метою дослідження є комплексний аналіз правових засад публічно-приватної співпраці у сфері кібербезпеки та формування моделі забезпечення балансу інтересів держави, бізнесу і суспільства в умовах 2026 року. **Об'єктом дослідження** є суспільні відносини, що виникають у процесі забезпечення кібербезпеки та функціонування критичної інфраструктури, тоді як **предметом** — норми національного законодавства України та права Європейського Союзу, що регулюють питання стійкості критичних суб'єктів, державного контролю, відповідальності та взаємодії з приватним сектором.

Для досягнення поставленої мети визначено такі **завдання:**

— розкрити теоретико-правову природу публічно-приватної співпраці у сфері кібербезпеки;

— проаналізувати європейські стандарти регулювання кібербезпеки та їх вплив на національну правову систему;

— дослідити стан нормативно-правового забезпечення кібербезпеки в Україні станом на 2026 рік;

— визначити механізми забезпечення балансу інтересів держави, бізнесу та суспільства;

— окреслити проблеми правозастосування та державного нагляду у сфері кібербезпеки;

— сформулювати пропозиції щодо вдосконалення законодавства України з урахуванням європейських стандартів.

Методологічну основу дослідження поєднує діалектичний підхід, що дозволяє розглядати кібербезпеку як динамічне явище, системний аналіз, який забезпечує цілісне бачення інституційної

архітектури безпеки, формально-юридичний метод тлумачення нормативних актів, а також порівняльно-правовий метод для зіставлення української моделі регулювання з правом Європейського Союзу. Додатково використано функціональний та прогностичний підходи для оцінки ефективності існуючих механізмів і формування рекомендацій щодо їх удосконалення.

Практичне значення монографії полягає в тому, що її висновки можуть бути використані у нормотворчій діяльності Верховної Ради України, у роботі органів виконавчої влади при розробленні стратегічних документів, у процесі імплементації стандартів ЄС, а також у діяльності суб'єктів господарювання під час формування корпоративних політик управління кіберризиками. Окрім цього, результати дослідження мають значення для освітнього процесу та подальших наукових розвідок у сфері публічного права та національної безпеки.

Запропонована концепція спрямована на формування сучасної правової моделі публічно-приватної співпраці, здатної забезпечити стійкість держави, конкурентоспроможність економіки та належний рівень захисту прав людини в умовах цифрових і воєнних викликів 2026 року. Структурно дослідження складається з двох розділів, у яких послідовно розглядаються теоретико-правові засади публічно-приватної співпраці та механізми її практичної реалізації у сфері кібербезпеки.

2. Теоретико-правові засади публічно-приватної співпраці у сфері кібербезпеки

Кібербезпека як складник національної безпеки та публічного інтересу

У XXI столітті кіберпростір перестав бути допоміжним середовищем функціонування суспільства і трансформувався у самостійний вимір реалізації державної влади, економічних процесів і соціальних відносин. Станом на 2026 рік кібербезпека в Україні

не може розглядатися ані як суто технічна проблема, ані як вузький сегмент інформаційної політики. Вона набула ознак комплексного правового інституту, який органічно поєднує елементи національної безпеки, публічного управління, захисту прав людини та регулювання господарської діяльності.

Нормативне регулювання кібербезпеки має міжгалузевий характер. Воно охоплює норми адміністративного, інформаційного, господарського, фінансового та конституційного права. Саме ця міжгалузевість зумовлює складність інституціоналізації публічно-приватної співпраці: суб'єкти господарювання залишаються автономними учасниками ринку, але одночасно набувають публічно-правових обов'язків.

Таким чином, кібербезпека функціонує як інтегративна категорія, що долає традиційні галузеві межі та формує нову модель безпекового управління.

Повномасштабна збройна агресія проти України остаточно продемонструвала, що кіберпростір є одним із ключових театрів гібридного протистояння. Кібератаки на енергетичну інфраструктуру, фінансову систему, телекомунікаційні мережі та державні електронні реєстри мали не лише технічні, а й безпосередні соціально-правові наслідки. Порушення доступу до електронних сервісів, банківських операцій або систем охорони здоров'я прямо впливало на реалізацію базових прав людини та здатність держави виконувати свої конституційні функції. За цих умов кібербезпека об'єктивно інтегрувалася у систему національної безпеки та оборони.

Європейський Союз ще до повномасштабних безпекових криз почав формувати нормативну модель, у якій цифрова безпека розглядається крізь призму стійкості. Відповідно до Directive (EU) 2022/2557 [1], ключовим завданням держав-членів є не лише запобігання загрозам, а й забезпечення здатності критичних суб'єктів протистояти кризам та відновлювати функціонування після них.

Такий підхід принципово відрізняється від традиційної логіки «захисту від загроз» і фактично переносить акцент на управління ризиками та довгострокову стійкість систем.

В українському праві подібний підхід отримав нормативне закріплення у Законі України «Про критичну інфраструктуру» [5], який визначив основи ідентифікації, захисту та координації функціонування критичної інфраструктури. Разом із ним Закон України «Про національну безпеку України» [4] формує правову рамку, у межах якої кібербезпека розглядається як складник загальної системи безпеки держави. У теоретико-правовому вимірі кібербезпека є складником ширшої категорії національної безпеки. Національна безпека, у доктринальному розумінні, охоплює стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз. У цьому контексті цифрові системи, інформаційні ресурси та мережі зв'язку стають об'єктами правової охорони нарівні з територією, економічним потенціалом і обороноздатністю.

У сучасній правовій доктрині кібербезпека дедалі частіше розглядається крізь призму теорії публічних благ. Її результат — стабільність цифрового середовища, безперервність функціонування критичних сервісів та захищеність інформаційних ресурсів — має властивості не виключності та суспільної значущості. Порушення кіберстійкості одного суб'єкта здатне спричинити каскадні ефекти для інших учасників ринку та державних інституцій.

Така системна взаємозалежність означає, що забезпечення кібербезпеки не може бути повністю делеговане приватній ініціативі або виключно адміністративному контролю. Воно потребує моделі спільного управління, у межах якої приватні суб'єкти виступають співучасниками реалізації публічного інтересу.

З огляду на це кібербезпека набуває ознак комплексного публічно-правового режиму, що поєднує імперативні приписи, механізми координації та елементи саморегулювання.

Разом із тим кібербезпека має безпосередній зв'язок із категорією публічного інтересу. Як зазначається у теорії права, публічний інтерес є узагальненим виразом соціально значущих потреб, що визнаються державою та забезпечуються нею через правові механізми [7]. Водночас будь-яке обмеження прав заради публічного інтересу має базуватися на принципах правової визначеності та пропорційності [8]. У сфері кібербезпеки таким інтересом є безперервність функціонування життєво необхідних сервісів, захист персональних даних, стабільність фінансової системи та довіра до цифрових інституцій.

Особливістю реалізації публічного інтересу у сфері кібербезпеки є те, що значна частина цифрової та критичної інфраструктури перебуває у власності або під управлінням приватних суб'єктів. Саме вони забезпечують функціонування телекомунікаційних мереж, платіжних систем, хмарних сервісів, програмного забезпечення для органів державної влади. За таких умов держава не спроможна забезпечити кіберстійкість виключно адміністративними засобами. Виникає об'єктивна потреба у правовій моделі співпраці, що поєднує публічні та приватні ресурси.

Станом на 2026 рік у праві формується нове розуміння кібербезпеки як кіберстійкості. Йдеться не лише про запобігання інцидентам, а про здатність систем функціонувати в умовах постійних загроз, швидко адаптуватися до змін та відновлюватися після атак. Саме ця логіка лежить в основі сучасних європейських стандартів [1; 9]. Для України, яка функціонує в умовах воєнного стану, такий підхід має не декларативне, а практичне значення.

Кібербезпека як складник публічного інтересу також перебуває у тісному зв'язку з правами людини. З одного боку, держава зобов'язана забезпечити захист цифрових систем, від яких залежить реалізація соціальних, економічних і особистих прав. З іншого — заходи кіберзахисту не можуть виправдовувати необмежене втручання у приватне життя, свободу вираження поглядів чи право

на захист персональних даних. Отже, правове регулювання у цій сфері має ґрунтуватися на принципах верховенства права, пропорційності та правової визначеності.

Таким чином, у 2026 році кібербезпека постає як багатовимірна правова категорія, що інтегрує елементи національної безпеки, публічного управління, корпоративної відповідальності та прав людини. Її забезпечення неможливе без інституціоналізованої взаємодії держави та приватного сектору.

Еволюція національного підходу до кібербезпеки не може розглядатися ізольовано від європейських інтеграційних процесів. Саме право Європейського Союзу упродовж останнього десятиліття сформувало методологічні орієнтири переходу від моделі захисту до моделі стійкості, які поступово імплементуються в українську правову систему.

Еволюція концепції кіберстійкості у праві Європейського Союзу: системний порівняльний аналіз

Формування сучасної концепції кіберстійкості в праві Європейського Союзу є результатом тривалої еволюції підходів до регулювання цифрової безпеки. Початково увага зосереджувалася на технічному захисті інформаційних систем, однак із розвитком цифрової економіки та зростанням гібридних загроз стало очевидним, що фрагментарні заходи не здатні забезпечити належний рівень безпеки.

Першим системним кроком у цьому напрямі стало ухвалення Директиви (ЄС) 2016/1148 (NIS) [9], яка заклала основи спільної політики кібербезпеки. Вона встановила мінімальні вимоги до безпеки мережевих та інформаційних систем і започаткувала механізм повідомлення про інциденти. Проте практика її застосування виявила обмеженість такого підходу, особливо в умовах масштабних криз. Обмеженість першої директивної моделі проявилася у фрагментарності імплементації, різному рівні національного регулювання та недостатній координації у випадку транскордонних

інцидентів. Саме ці фактори зумовили необхідність перегляду підходів і посилення наднаціональний складник регулювання.

Практична реалізація публічно-приватного співробітництва у сфері кібербезпеки та захисту критичної інфраструктури передбачає формування комплексної системи процедур, інструментів контролю та стандартів управління ризиками. Її ефективність визначається здатністю забезпечити оперативне реагування на інциденти, належний рівень державного нагляду та впровадження уніфікованих технічних підходів. В умовах воєнного стану такі механізми набувають особливого значення, оскільки кіберінциденти можуть бути складникширших гібридних загроз.

Ключовим елементом цієї системи є процедура повідомлення про інциденти, яка в праві Європейського Союзу побудована за принципом поетапності. Відповідно до Directive (EU) 2022/2555 (NIS2 Directive) [2], суб'єкти повинні здійснювати раннє повідомлення протягом 24 годин з моменту виявлення суттєвого інциденту, надати первинний звіт упродовж 72 годин та подати фінальний звіт після завершення розслідування. Така триступенева модель дозволяє поєднати вимогу оперативності з необхідністю формування повної та перевіреної інформації про характер і наслідки події. Для України імплементація подібного механізму потребує деталізації на рівні підзаконних нормативно-правових актів із врахуванням специфіки воєнних ризиків та режиму обмеженого доступу до окремих категорій інформації.

Процедура поетапного повідомлення виконує не лише інформативну, а й правову функцію. Вона фіксує момент виникнення юридичного факту — кіберінциденту, з яким пов'язуються обов'язки суб'єкта, можливість застосування наглядових заходів та оцінка належності виконання вимог управління ризиками.

У національному контексті імплементація подібної моделі потребує деталізації процесуальних гарантій, зокрема захисту

конфіденційної інформації та недопущення її використання у конкурентній боротьбі.

Не менш важливим механізмом виступає ризикоорієнтований нагляд, що поєднує превентивний та реактивний компоненти контролю. Превентивний (ex ante) підхід спрямований на аудит систем управління безпекою до виникнення інциденту, тоді як реактивний (ex post) передбачає перевірку після настання події та можливість застосування санкцій або коригувальних заходів. Європейська модель нагляду передбачає інтеграцію обох підходів у межах єдиної системи, що забезпечує баланс між профілактикою та відповідальністю. Така конструкція сприяє формуванню передбачуваного регуляторного середовища та підвищенню дисципліни суб'єктів господарювання.

Практичну перевірку ефективності нормативних вимог забезпечують спільні кризові та кібернавчання, які дозволяють моделювати складні сценарії атак і оцінювати реальну готовність державних органів і приватних операторів до взаємодії. Координацію міжнародних навчань у Європейському Союзі здійснює European Union Agency for Cybersecurity, зокрема в межах ініціативи Cyber Europe [10]. Такі навчання сприяють виробленню спільних алгоритмів реагування та формуванню довіри між учасниками системи публічно-приватного співробітництва.

Важливу роль у реалізації положень Директиви Європейського Союзу про заходи для забезпечення високого спільного рівня кібербезпеки (NIS2) відіграє European Union Agency for Cybersecurity [10], яка виступає ключовим координаційним центром у формуванні європейської політики кіберстійкості. У межах свого мандату агентство розробляє методичні рекомендації для держав-членів, забезпечує аналітичну підтримку імплементації нормативних актів та сприяє узгодженню національних підходів до управління кіберризиками. Зокрема, ENISA готує технічні керівництва

щодо впровадження вимог NIS2, включаючи стандарти управління інцидентами, процедури обміну інформацією про кіберзагрози та моделі взаємодії між державними органами й приватними операторами критичної інфраструктури.

Крім того, діяльність ENISA спрямована на формування єдиної системи оцінювання кіберстійкості в Європейському Союзі. Агентство проводить регулярні аналітичні дослідження, оцінює рівень готовності секторів критичної інфраструктури до кіберінцидентів та розробляє рекомендації щодо підвищення рівня захищеності цифрових систем. У межах цих процесів значна увага приділяється розробленню стандартів кібербезпеки, узгоджених із міжнародними підходами до управління інформаційною безпекою, а також підтримці механізмів сертифікації та оцінки ризиків. Така діяльність сприяє формуванню комплексної системи кіберстійкості, у якій поєднуються нормативні вимоги, технічні стандарти та практичні інструменти реагування на кіберзагрози [11].

Додатковим економічним стимулом для впровадження високих стандартів безпеки є розвиток ринку кіберстрахування. Страхові компанії, оцінюючи рівень захищеності потенційних клієнтів, фактично здійснюють незалежну перевірку їхніх систем управління ризиками, що створює додатковий механізм ринкової дисципліни. У результаті кіберстрахування стає елементом багаторівневої системи забезпечення стійкості поряд із державним контролем і внутрішнім корпоративним управлінням.

Технічну основу реалізації ППС формують міжнародні стандарти управління інформаційною безпекою. Зокрема, стандарт ISO/IEC 27001:2022 визначає вимоги до системи управління інформаційною безпекою [11], а NIST Cybersecurity Framework пропонує структуровану модель управління ризиками, що охоплює процеси ідентифікації, захисту, виявлення, реагування та відновлення [12]. Інкорпорація зазначених стандартів у національні

нормативні акти підвищує рівень правової визначеності та сприяє гармонізації українського регулювання з європейськими підходами.

Проте навіть наявність процедур і стандартів не усувала стратегічної проблеми — відсутності персоналізованої управлінської відповідальності та єдиного підходу до міжсекторний ризиків. Саме ця обставина стала одним із ключових аргументів для оновлення нормативної моделі Європейського Союзу.

Таким чином, практичні механізми реалізації публічно-приватного співробітництва у сфері кібербезпеки формують багаторівневу систему, в якій нормативні приписи, контрольні процедури, навчальні інструменти, ринкові стимули та міжнародні стандарти взаємодіють між собою, забезпечуючи підвищення стійкості критичної інфраструктури.

Відповіддю на системні виклики цифрової трансформації та зростання гібридних загроз стало ухвалення Directive (EU) 2022/2555 [2], яка закріпила перехід до ризикоорієнтованої моделі регулювання. На відміну від попередньої директиви, новий акт встановлює комплексні вимоги до управління ризиками, корпоративного контролю та державного нагляду.

Кібербезпека перестала сприйматися як вузькоспеціалізована функція ІТ-підрозділу і була інтегрована у систему корпоративного управління. Директива прямо покладає на керівництво компаній обов'язок забезпечувати впровадження ефективних систем управління ризиками, контролювати їх функціонування та проходити відповідне навчання. Така персоналізація відповідальності означає, що питання кіберстійкості набуває статусу елементу стратегічного планування і корпоративної політики, а не лише технічної операційної діяльності.

Одночасно держава отримує розширені інструменти нагляду, включно з правом проведення перевірок, вимогою усунення порушень та застосуванням значних санкцій у разі недотримання встановлених вимог. Таким чином, формується модель, у якій корпоративна

автономія поєднується з жорсткішим регуляторним контролем, що відповідає логіці ризикоорієнтованого управління.

Паралельно із цим Directive (EU) 2022/2557 [1] закріпила розширене бачення стійкості, яке виходить за межі суто кіберризиків. Вона інтегрує фізичні, організаційні та цифрові аспекти безпеки, орієнтуючись на здатність критичних суб'єктів не лише запобігати інцидентам, але й забезпечувати безперервність функціонування та оперативне відновлення після кризових подій.

У сукупності NIS2 [2] та CER [1] формують цілісну нормативну конструкцію, яку можна схарактеризувати як модель "resilience governance" — багаторівневу систему управління стійкістю, у межах якої відповідальність розподіляється між державою, регуляторними органами та операторами критичної інфраструктури. У цій системі кіберстійкість виступає складником ширшої категорії критичної стійкості, а співпраця публічного і приватного секторів стає не факультативним інструментом, а структурною умовою ефективного функціонування безпекової архітектури.

Такий підхід відображає еволюцію європейського права від секторального регулювання до інтегрованої моделі управління ризиками, що враховує міжсекторний залежності та транскордонний характер сучасних загроз.

Таблиця 1 — Порівняльний аналіз NIS2 [2] та CER [1] дозволяє виділити такі відмінності та спільні риси

Критерій	NIS2	CER
Предмет регулювання	Кіберризики та мережеві системи	Фізичні та багатовимірні ризики
Основний підхід	Управління кіберризиками	Загальна стійкість критичних суб'єктів
Механізм нагляду	Ризикоорієнтований контроль	Державна координація та національні стратегії
Відповідальність	Персональна відповідальність керівництва	Інституційна відповідальність суб'єктів

У системному вимірі взаємодія цих актів створює багаторівневу архітектуру управління стійкістю, в межах якої кіберризики розглядаються як складник ширшого комплексу загроз критичним суб'єктам.

Європейська концепція кіберстійкості також характеризується розвитком механізмів транскордонної співпраці. NIS2 [2] передбачає створення мережі співробітництва компетентних органів, посилення ролі ENISA та гармонізацію процедур реагування на інциденти.

Для України європейська модель має не лише порівняльне, а й безпосереднє нормативне значення. Імплементація положень NIS2 і CER у національне законодавство випливає із зобов'язань за Association Agreement between the European Union and Ukraine [6] та водночас виступає інструментом модернізації власної системи безпеки. У 2023–2026 роках українська модель демонструє поступову гармонізацію з європейськими стандартами, зокрема через розвиток ризикоорієнтованого нагляду та уточнення вимог до операторів критичної інфраструктури, однак питання персональної відповідальності керівництва та транскордонної координації потребують подальшого нормативного розвитку.

Європейська модель кіберстійкості має не лише нормативне, а й доктринальне значення. Вона закріплює розуміння стійкості як здатності системи функціонувати в умовах постійних загроз, що відповідає сучасним викликам воєнного часу.

Отже, еволюція концепції кіберстійкості у праві Європейського Союзу відображає перехід від фрагментарного секторального регулювання до інтегрованої моделі управління ризиками, відповідальності та міжсекторний координації. Для України у 2026 році цей процес має характер не лише правової конвергенції, а й стратегічної адаптації безпекової архітектури до умов воєнного часу та цифрової трансформації.

Публічно-приватна співпраця як інститут публічного права у сфері кібербезпеки

Публічно-приватна співпраця (далі — ППС) у сфері кібербезпеки у 2026 році дедалі чіткіше проявляє риси самостійного інституту публічного права, який формується на перетині адміністративного, безпекового, інформаційного та господарського права. Її становлення є не випадковим етапом еволюції правового регулювання, а закономірною реакцією держави на трансформацію природи загроз у цифрову епоху. Якщо у традиційній моделі національної безпеки основними об'єктами правової охорони виступали територія, кордони та оборонний потенціал, то у XXI столітті до цього переліку остаточно приєдналися цифрові мережі, інформаційні ресурси, дата-центри, хмарна інфраструктура та програмні платформи, без яких неможливе функціонування державного управління та економіки.

У цьому контексті ППС набуває ознак інституціоналізованої форми делегованої участі приватного сектору у реалізації публічної функції безпеки. Йдеться не про передачу державних повноважень, а про нормативно врегульовану співучасть у досягненні публічного результату — забезпеченні кіберстійкості. Такий підхід відповідає сучасній концепції «розподіленої безпеки», у межах якої держава не монополізує безпекову діяльність, а координує її.

Об'єктивність розвитку ППС у сфері кібербезпеки зумовлена тим, що критична цифрова інфраструктура переважно перебуває у власності або під управлінням приватних суб'єктів. Оператори телекомунікацій, банки, енергетичні компанії, великі ІТ-провайдери забезпечують безперервність процесів, які мають публічне значення. Водночас відповідно до Закону України «Про національну безпеку України» [4] забезпечення національної безпеки є конституційним обов'язком держави. Таким чином, виникає нормативний і функціональний дуалізм: ресурси безпеки значною мірою

приватні, а відповідальність — публічна. Саме на перетині цих двох площин і формується сучасний інститут публічно-приватної співпраці.

Такий дуалізм зумовлює необхідність чіткого розмежування сфер автономії та підконтрольності: приватні суб'єкти зберігають господарську самостійність, проте в частині забезпечення кіберстійкості діють у межах спеціального публічно-правового режиму. Саме ця подвійність визначає складність правового конструювання відповідальності та нагляду.

У класичному розумінні публічно-приватне партнерство розглядається як договірна взаємодія держави та бізнесу з метою реалізації інфраструктурних або соціально значущих проєктів. Однак у сфері кібербезпеки ця конструкція зазнає суттєвої трансформації. Йдеться не про концесії чи інвестиційні угоди, а про постійний процес спільного управління ризиками, обміну інформацією щодо загроз, узгодження стандартів безпеки та координації реагування на інциденти. У цьому контексті співпраця перестає бути факультативною і набуває імперативного характеру.

З позицій адміністративно-правової доктрини ППС у сфері кібербезпеки може бути визначена як під підінститут публічного права безпекового спрямування, що характеризується:

— наявністю вираженого публічного інтересу;
— обов'язковістю взаємодії;
— державною координацією та наглядом;
— встановленням спеціального режиму відповідальності;
— процесуальними гарантіями прав суб'єктів.

Така конструкція відрізняється від класичних договірних форм партнерства та має ознаки нормативно зумовленої співучасті у реалізації функцій держави.

З теоретико-правової точки зору інститут ППС у сфері кібербезпеки характеризується передусім наявністю чітко вираженого

публічного інтересу. Захист безперервності енергопостачання, стабільності фінансової системи чи функціонування державних реєстрів є не корпоративним, а суспільним завданням. По-друге, приватні суб'єкти наділяються публічно-правовими обов'язками, що виходять за межі звичайної господарської діяльності. Вони зобов'язані впроваджувати системи управління ризиками, здійснювати аудит безпеки, повідомляти державні органи про інциденти та співпрацювати під час розслідування атак. По-третє, співпраця передбачає інституційну координацію та державний нагляд, що відрізняє її від звичайних ринкових відносин.

Системне нормативне закріплення такого підходу відбулося у праві Європейського Союзу, де кіберстійкість розглядається як спільна відповідальність держави та операторів критичних суб'єктів. Зокрема, Directive (EU) 2022/2555 [2] розширює коло суб'єктів регулювання, встановлює комплексні вимоги до управління ризиками та передбачає персональну відповідальність керівництва компаній. Таким чином, питання кібербезпеки інтегрується у систему корпоративного управління, а відповідальність за її забезпечення набуває стратегічного та управлінського характеру.

Паралельно Directive (EU) 2022/2557 [1] формує ширшу модель стійкості критичних суб'єктів. Вона передбачає системне оцінювання ризиків, розроблення національних стратегій стійкості та координацію між державами-членами ЄС. Поєднання NIS2 і CER створює багаторівневу конструкцію, в якій приватні оператори не лише виконують обов'язки, але й стають невід'ємною частиною публічної безпекової архітектури.

Особливістю цієї моделі є формування постійних каналів обміну інформацією, процедур раннього попередження та механізмів кризової координації, які функціонують незалежно від наявності надзвичайної ситуації. Таким чином, ППС у сфері кібербезпеки перестає бути реактивною та набуває превентивного характеру.

Для України ці процеси мають безпосереднє значення у контексті імплементації зобов'язань за Association Agreement between the European Union and Ukraine [6]. Гармонізація законодавства у сфері кібербезпеки означає не лише формальне приведення норм у відповідність до європейських стандартів, а й переосмислення ролі бізнесу у забезпеченні публічного інтересу.

Національну правову основу ППС у цій сфері становить, зокрема, Закон України «Про критичну інфраструктуру», який визначає принципи ідентифікації об'єктів критичної інфраструктури, їх категоризації та взаємодії з державними органами [5]. У поєднанні із Законом України «Про національну безпеку України» [4] цей акт формує рамку, в межах якої можлива координація державних і приватних зусиль. Однак практика воєнного часу продемонструвала, що формальної наявності норм недостатньо — необхідна реальна інституційна довіра та чітко визначені процедури обміну інформацією.

Функціонування ППС у 2026 році відбувається в умовах воєнного стану, що істотно впливає на баланс інтересів. З одного боку, держава посилює координаційну роль і запроваджує додаткові вимоги безпеки. З іншого — саме приватні оператори забезпечують відновлення цифрових сервісів після атак, підтримку хмарної інфраструктури та безперервність фінансових операцій. Така взаємозалежність підкреслює, що кіберстійкість є результатом спільних зусиль, а не односторонніх дій держави.

Воєнний стан модифікує класичну модель розподілу ризиків. Частина кібератак має ознаки актів збройної агресії, що виходять за межі господарського ризику. У таких випадках доцільним є нормативне закріплення принципу належної кіберобачності, за яким суб'єкт звільняється від відповідальності за умови доведення впровадження встановлених стандартів безпеки.

Це дозволяє уникнути дисбалансу між публічним інтересом і економічною стійкістю операторів критичної інфраструктури.

Водночас інституціоналізація ППС у сфері кібербезпеки породжує складні правові питання. Насамперед постає проблема меж державного втручання у господарську діяльність. Вимоги щодо розкриття інформації про інциденти або внутрішні системи безпеки можуть конфліктувати з комерційною таємницею. Крім того, у разі масштабних кібератак виникає питання розподілу відповідальності між державою та оператором: чи є інцидент наслідком неналежного виконання обов'язків суб'єктом господарювання, чи результатом обставин непереборної сили в умовах воєнної агресії.

Не менш важливим є аспект захисту прав людини. Посилення кіберконтролю та моніторингу мереж може створювати ризики для права на приватність та свободу вираження поглядів. Тому ППС повинна розвиватися у межах принципів верховенства права, пропорційності та правової визначеності. Баланс інтересів держави, бізнесу і суспільства можливий лише за умови чіткої нормативної регламентації та передбачуваності правових наслідків.

Відсутність такої визначеності може призвести до «надмірної безпекізації» цифрового простору, коли превентивні механізми контролю перетворюються на інструменти необґрунтованого втручання у приватне життя. Саме тому ППС має розвиватися паралельно з механізмами судового та парламентського контролю.

Перспективи розвитку ППС у 2026 році пов'язані з подальшою імплементацією стандартів NIS2 [2], удосконаленням механізмів державного нагляду та створенням єдиного координаційного середовища взаємодії держави та операторів критичної інфраструктури. Важливим напрямом є також формування прозорої моделі фінансування заходів кіберстійкості, оскільки надмірне перекладання фінансового навантаження на бізнес може підірвати економічну стабільність, тоді як повне фінансування за рахунок бюджету є нереалістичним.

Фінансове забезпечення заходів кіберстійкості є самостійним структурним елементом публічно-приватної співпраці. Його

правова природа полягає у поєднанні бюджетних, міжнародних та корпоративних ресурсів у межах змішаної моделі фінансування.

З огляду на воєнний стан та післявоєнну реконструкцію, державний бюджет не може повністю покривати витрати на модернізацію критичної цифрової інфраструктури. Водночас надмірне перекладання фінансового навантаження на суб'єктів господарювання може створити дисбаланс між безпековими вимогами та економічною свободою підприємництва, що суперечитиме принципу пропорційності регулювання.

У цьому контексті особливого значення набуває інтеграція України у європейські фінансові механізми підтримки цифрової трансформації та стійкості відповідно до Association Agreement between the European Union and Ukraine [6]. Такий підхід дозволяє: 1) диверсифікувати джерела фінансування; 2) забезпечити доступ до грантових та інвестиційних інструментів ЄС; 3) гармонізувати стандарти кіберзахисту; 4) мінімізувати фіскальні ризики для держави. Крім того, участь у європейських програмах підтримки дозволяє запровадити стандартизовані підходи до оцінки ефективності інвестицій у кіберстійкість, що підвищує прозорість використання коштів і сприяє довгостроковій стратегічній стабільності системи.

Отже, у 2026 році публічно-приватна співпраця у сфері кібербезпеки набуває статусу системоутворюючого інституту національної безпеки. Вона ґрунтується на розподіленій відповідальності, ризикоорієнтованому управлінні, фінансовій збалансованості та дотриманні прав людини. Її подальший розвиток залежить не лише від нормативної деталізації, а й від рівня інституційної довіри, стабільності процедур координації та глибини інтеграції України до правового простору Європейського Союзу. Саме ці чинники визначатимуть реальну ефективність кіберстійкості у воєнний та післявоєнний період.

3. Механізми реалізації публічно-приватної співпраці у сфері кібербезпеки в Україні та ЄС

Станом на 2026 рік публічно-приватна співпраця у сфері кібербезпеки остаточно вийшла за межі декларативних програмних положень і перетворилася на структурований механізм реалізації державної безпекової політики. Якщо на початковому етапі її розвиток обмежувався формальним проголошенням необхідності взаємодії держави та бізнесу, то сьогодні йдеться про чітко регламентовані процедури, встановлені строки реагування, інструменти контролю та моделі відповідальності. Така трансформація стала наслідком не лише технологічного розвитку, а й системного ускладнення загроз, що поєднують кіберкомпонент із фізичними та економічними ризиками. У доктринальному вимірі йдеться про інституціоналізацію ППС як процесуального механізму реалізації публічного інтересу у сфері безпеки. На відміну від класичних моделей взаємодії, сучасна архітектура співпраці базується на нормативно визначених обов'язках, процедурній стандартизації та ризикоорієнтованому управлінні.

У Європейському Союзі практична архітектура ППС у сфері кібербезпеки побудована на нормативному балансі між імперативними вимогами до операторів та координуючою роллю держави. Відповідно до Directive (EU) 2022/2555 [2] держави-члени зобов'язані створити компетентні органи, визначити національні CSIRT та забезпечити механізми координації реагування на інциденти. Проте ключовим є те, що відповідальність за практичне забезпечення кіберстійкості покладається не лише на державу, а й на суб'єктів господарювання, віднесених до категорій «суттєвих» та «важливих».

Механізм повідомлення про інциденти, передбачений NIS2, має чітку процесуальну структуру: раннє попередження упродовж 24 годин, подання детального звіту протягом 72 годин та

фінального звіту після завершення розслідування. Така регламентація дисциплінує операторів і водночас забезпечує державі своєчасний доступ до інформації, необхідної для координації реагування. У поєднанні з ризикоорієнтованим державним наглядом і можливістю застосування суттєвих фінансових санкцій ця модель формує стимулююче середовище, у якому недотримання стандартів кібербезпеки стає економічно невигідним.

Водночас NIS2 не функціонує ізольовано. Її логічним продовженням є Directive (EU) 2022/2557 [1], яка розширює фокус із суто кіберризиків до комплексної стійкості критичних суб'єктів. Цей акт зобов'язує держави-члени розробляти національні стратегії стійкості, здійснювати системну оцінку ризиків і визначати критичні суб'єкти, діяльність яких має вирішальне значення для суспільства. Взаємодія держави та бізнесу в межах CER набуває стратегічного виміру: йдеться не лише про реагування на інциденти, а про довгострокове планування, аудит, кризові навчання та формування культури безпеки.

Таким чином, у праві ЄС формується багаторівнева модель "compliance + governance + resilience", у межах якої юридичні обов'язки поєднуються зі стратегічним управлінням та довгостроковим плануванням. Саме ця інтеграція відрізняє сучасну модель від попередніх секторальних підходів.

Окремої уваги заслуговує регулювання в енергетичному секторі. Regulation (EU) 2019/941 встановлює вимоги до підготовки до ризиків у секторі електроенергетики [13]. Інтеграція цифрових ризиків у секторі електроенергетики демонструє міжгалузеву природу сучасної стійкості: кібератака може трансформуватися у фізичну кризу, а отже потребує спільної регуляторної відповіді. Хоча цей регламент не обмежується кіберзагрозами, він демонструє інтеграцію цифрових ризиків у загальну систему безпеки енергосистеми. Таким чином, у праві ЄС формується багаторівнева

модель, де нагляд, відповідальність, координація та фінансова підтримка утворюють єдину систему забезпечення стійкості.

Українська модель ППС у сфері кібербезпеки має власну специфіку, зумовлену воєнним станом та високою інтенсивністю гібридних загроз. Нормативною основою виступають, зокрема, Закон України «Про критичну інфраструктуру» [5], Закон України «Про національну безпеку України» [4] та Закон України «Про основні засади забезпечення кібербезпеки України» [14]. Закон 2017 року заклав основу функціонування національної системи кібербезпеки та визначив принцип взаємодії державних органів із підприємствами незалежно від форми власності. Однак саме події 2022–2026 років наповнили ці положення реальним змістом.

У практичному вимірі співпраця реалізується через діяльність галузевих центрів реагування, координацію на рівні Національного координаційного центру кібербезпеки, спільні кібернавчання та оперативне залучення приватних ІТ-компаній до відновлення цифрових сервісів після атак. Особливої ваги набула співпраця у сфері захисту енергетичної інфраструктури, банківської системи та державних реєстрів, де приватні оператори фактично виконують функцію гарантування безперервності публічних послуг.

Водночас українська модель характеризується більшою централізацією порівняно з європейською. Це пояснюється необхідністю оперативного реагування в умовах воєнної агресії. Держава відіграє домінуючу координуючу роль, однак без технічного та організаційного ресурсу приватного сектору забезпечити кіберстійкість було б неможливо. Така взаємозалежність формує нову конфігурацію відповідальності.

На відміну від більш децентралізованої моделі ЄС, український підхід у 2022–2026 роках характеризується концентрацією координаційних повноважень на рівні держави, що зумовлено воєнними обставинами. Водночас довгострокова перспектива передбачає

поступове збалансування централізації з інституційною автономією операторів.

Питання юридичної відповідальності є одним із ключових елементів ППС. Європейський підхід, закріплений у NIS2 [2], передбачає персональну відповідальність керівництва компаній за невиконання вимог кібербезпеки. Це означає, що управління кіберризиками стає складником корпоративного governance, а недбалість або ігнорування вимог можуть мати персональні наслідки для топменеджменту. Така модель підсилює превентивний характер регулювання.

У ширшому контексті транскордонних інцидентів питання відповідальності держав корелює з положеннями Документа Комісії міжнародного права ООН — Articles on Responsibility of States for Internationally Wrongful Acts [15], який формує доктринальну основу міжнародно-правової відповідальності. Хоча зазначений документ не містить спеціальних положень щодо кібероперацій, його принципи атрибуції, протиправності та репарації залишаються методологічною основою для оцінки транскордонних кіберінцидентів.

В Україні відповідальність за порушення вимог кібербезпеки наразі переважно має адміністративний та господарський характер. Відсутність деталізованої моделі персональної відповідальності керівників операторів критичної інфраструктури створює прогалини у стимулюванні дотримання стандартів стійкості. Гармонізація із підходами ЄС у цій сфері могла б підвищити ефективність превентивних механізмів та сприяти формуванню культури управління ризиками.

Фінансування залишається практичним ядром ППС. У Європейському Союзі розвиток кіберстійкості підтримується через інструменти стратегічного фінансування. Regulation (EU) 2021/241 [16] створює механізм Recovery and Resilience Facility, який спрямований на підтримку реформ і інвестицій, зокрема у сфері цифрової

інфраструктури та кіберзахисту. Додатково Regulation (EU) 2021/836 [17] забезпечує координацію допомоги державам у кризових ситуаціях, включаючи інциденти, що стосуються критичної інфраструктури.

Ефективність ППС у сфері кібербезпеки залежить не лише від нормативних вимог і процедур контролю, а й від економічної обґрунтованості покладених на суб'єктів обов'язків. Саме тому питання пропорційності витрат, стимулювання інвестицій та розподілу фінансового навантаження набувають принципового значення.

У цьому контексті ключовим є принцип економічної пропорційності, відповідно до якого витрати на забезпечення кіберстійкості повинні бути співмірними з масштабом діяльності, фінансовими можливостями та рівнем ризику конкретного суб'єкта. Надмірне регуляторне навантаження, особливо для малих і середніх підприємств, може негативно вплинути на конкурентне середовище, створюючи бар'єри для входу на ринок або знижуючи інноваційну активність. Водночас недостатній рівень інвестицій у захист критичної інфраструктури створює системні ризики для держави. Таким чином, фінансова модель ППС повинна забезпечувати розумний баланс між вимогами безпеки та економічною доцільністю.

Важливим інструментом досягнення такого балансу є механізми співфінансування та державного стимулювання. На рівні Європейського Союзу відповідні підходи реалізуються, зокрема, через Regulation (EU) 2021/241 [16], яким запроваджено механізм підтримки цифрової трансформації та підвищення стійкості економік держав-членів. Фінансування заходів з цифровізації, модернізації інфраструктури та впровадження інноваційних технологій створює передумови для інтеграції кібербезпеки у ширші програми розвитку.

Для України перспективною видається модель, що поєднує інструменти податкового стимулювання витрат на кіберзахист, створення спеціалізованого фонду кіберстійкості та запровадження

механізму часткової компенсації інвестицій у захисні технології. Податкові пільги можуть зменшити фінансовий тиск на бізнес і водночас стимулювати добровільне впровадження високих стандартів безпеки. Формування окремого фонду дозволило б акумулювати ресурси для підтримки об'єктів критичної інфраструктури, особливо в умовах воєнних ризиків. Механізм часткової компенсації інвестицій, своєю чергою, сприяв би модернізації технічних систем без надмірного перекладання витрат на приватний сектор.

У цьому ж контексті в окремих державах Європейського Союзу обговорюються моделі секторальних фондів підтримки критичної інфраструктури, що передбачають солідарний розподіл фінансового навантаження між державою та операторами ринку. Такий підхід дозволяє поєднати публічний інтерес у забезпеченні національної безпеки з економічною мотивацією приватних суб'єктів, формуючи більш стійку та передбачувану систему фінансування заходів із кіберзахисту.

Отже, фінансова модель ППС у сфері кібербезпеки має ґрунтуватися на принципах пропорційності, солідарності та стимулювання інвестицій. Лише за умови поєднання регуляторних вимог з економічно обґрунтованими механізмами підтримки можливо забезпечити довгострокову стійкість критичної інфраструктури та зберегти конкурентоспроможність національної економіки.

В Україні фінансування заходів у сфері кібербезпеки переважно здійснюється за рахунок державного бюджету, а також власних ресурсів суб'єктів господарювання, що експлуатують об'єкти критичної інформаційної інфраструктури. Водночас аналіз чинної нормативної бази свідчить, що національна система фінансової підтримки кіберстійкості перебуває на етапі формування та потребує подальшого інституційного розвитку. На відміну від моделі Європейського Союзу, де функціонують комплексні фінансові інструменти стимулювання інвестицій у кіберзахист, в Україні механізми

економічного заохочення приватного сектору ще не набули системного характеру. У зв'язку з цим одним із ключових напрямів удосконалення державної політики має стати формування збалансованої моделі фінансування кіберстійкості, що поєднуватиме державні ресурси, інвестиції бізнесу та міжнародну технічну допомогу.

Отже, станом на 2026 рік ППС у сфері кібербезпеки в Україні та ЄС функціонує як багатовимірна система взаємодії, що поєднує нормативні вимоги, координаційні механізми, відповідальність і фінансові інструменти. Її ефективність визначається не лише наявністю законодавчих актів, а й здатністю держави та бізнесу діяти як партнери у спільному забезпеченні стійкості критичної інфраструктури.

Кібербезпека нині перестала розглядатися виключно як технічна або секторальна категорія. Вона набула статусу публічного інтересу, що безпосередньо пов'язаний із реалізацією конституційних прав громадян, безперервністю публічних послуг та стабільністю демократичних інститутів.

У національному праві обов'язок держави забезпечувати безпеку прямо випливає із Закону України «Про національну безпеку України» [4]. Водночас у світлі практики Європейського суду з прав людини кібербезпека може розглядатися як складник позитивних зобов'язань держави за Конвенцією про захист прав людини і основоположних свобод.

Позитивні зобов'язання означають, що держава повинна не лише утримуватися від втручання у права людини, але й вживати активних заходів для їх захисту від посягань третіх осіб. У цифрову епоху це включає обов'язок створювати нормативну та інституційну систему захисту інформаційної безпеки.

У рішеннях ЄСПЛ послідовно підкреслюється, що втручання у цифрову сферу повинно відповідати принципам законності, необхідності та пропорційності. У справі Big Brother Watch and Others

v. the United Kingdom Суд сформулював підхід до оцінки систем масового перехоплення даних, наголосивши на необхідності ефективного нагляду та процесуальних гарантій [18].

У справі Centrum för rättvisa v. Sweden Суд підтвердив, що держави можуть здійснювати стратегічну розвідку в інтересах національної безпеки, однак лише за умови чітких запобіжників від зловживань [19].

Ці рішення мають значення для формування механізмів ППС, оскільки передбачають, що держава, делегуючи певні функції приватним суб'єктам або залучаючи їх до обробки інформації, зберігає обов'язок забезпечити належний контроль. Отже, залучення приватних суб'єктів до обробки інформації або моніторингу мереж не звільняє державу від обов'язку забезпечувати ефективні гарантії від зловживань. ППС у сфері кібербезпеки повинна супроводжуватися процедурними запобіжниками, включно із судовим контролем та механізмами незалежного нагляду.

Кібербезпека часто перетинається зі свободою вираження поглядів. Обмеження доступу до цифрових ресурсів, блокування сервісів або обмеження контенту повинні відповідати критеріям демократичного суспільства.

Європейська практика після імплементації NIS2 демонструє обережний підхід: заходи реагування на інциденти не повинні перетворюватися на інструмент надмірного втручання у цифрові свободи. У низці держав-членів (Німеччина, Нідерланди, Франція) імплементаційні акти передбачають обов'язковий судовий контроль за застосуванням окремих обмежувальних заходів [20].

Зазначені підходи найбільш виразно простежуються у практиці окремих держав-членів Європейського Союзу, які сформували власні моделі публічно-приватної співпраці у сфері кібербезпеки. Серед них особливу увагу привертають Німеччина, Нідерланди та Франція, де поєднуються різні інституційні механізми державного

регулювання, обміну інформацією та залучення приватного сектору до забезпечення кіберстійкості.

У Німеччині ключову роль у координації кібербезпеки відіграє Федеральне відомство з безпеки інформаційної техніки (Bundesamt für Sicherheit in der Informationstechnik, BSI) [21]. Його повноваження були істотно розширені після ухвалення Закону про IT-безпеку 2.0 (IT-Sicherheitsgesetz 2.0), який посилив вимоги до операторів критичної інфраструктури та запровадив нові механізми взаємодії між державою і приватним сектором. Законодавство зобов'язує операторів критичної інфраструктури впроваджувати сучасні технічні та організаційні заходи захисту, а також оперативно повідомляти BSI про кіберінциденти, що можуть вплинути на стабільність функціонування життєво важливих систем.

Важливою особливістю німецької моделі є інституціоналізований обмін інформацією між державними органами та приватними компаніями. У межах спеціалізованих платформ співпраці оператори критичної інфраструктури отримують від BSI аналітичну інформацію щодо актуальних кіберзагроз, вразливостей та методів їх нейтралізації. Така взаємодія має двосторонній характер: приватний сектор не лише отримує рекомендації від держави, але й передає інформацію про виявлені інциденти або підозрілі активності. У результаті формується система раннього попередження та колективного реагування на кіберзагрози, що значно підвищує загальний рівень кіберстійкості [22].

Іншим прикладом ефективної організації публічно-приватної співпраці є Нідерланди, де центральну роль у національній системі кібербезпеки відіграє National Cyber Security Centre (NCSC) [23]. Нідерландська модель традиційно характеризується високим рівнем довіри між державними структурами та приватним сектором, що відображається у практиці регулярного обміну інформацією про кіберінциденти, технічні вразливості та нові види атак. Значну

увагу приділено створенню механізмів швидкого інформування компаній, які можуть бути потенційними цілями кіберзлочинців.

Особливістю нідерландського підходу є так звана модель «добровільно-обов'язкового» обміну інформацією. З одного боку, приватні компанії заохочуються до добровільної участі у програмах кібербезпеки та партнерства з державою. З іншого боку, у випадках, коли мова йде про захист критичної інфраструктури або національної безпеки, законодавство передбачає обов'язковість повідомлення про серйозні кіберінциденти. Такий баланс між гнучкістю та регуляторними вимогами дозволяє забезпечити ефективну взаємодію без надмірного адміністративного тиску на бізнес [24].

Франція, на відміну від Німеччини та Нідерландів, застосовує більш централізовану модель управління кібербезпекою. Центральним органом у цій сфері є Національне агентство з безпеки інформаційних систем (Agence nationale de la sécurité des systèmes d'information, ANSSI) [25], яке здійснює стратегічну координацію, регуляторний нагляд та технічну підтримку державних органів і ключових операторів критичної інфраструктури. Французька модель передбачає значно активнішу роль держави у встановленні стандартів кіберзахисту та контролі за їх дотриманням.

Однією з характерних рис французького підходу є система обов'язкової сертифікації засобів кібербезпеки та підвищені вимоги до операторів життєво важливих об'єктів (operators of vital importance). Вони зобов'язані впроваджувати визначені державою технічні стандарти захисту, регулярно проходити аудити кібербезпеки та повідомляти ANSSI про всі суттєві інциденти. Така система дозволяє забезпечити високий рівень централізованого контролю та швидке реагування на кіберзагрози на національному рівні [26].

Досвід зазначених держав свідчить про існування різних моделей публічно-приватної співпраці у сфері кібербезпеки — від більш децентралізованих і партнерських до централізованих

і регуляторно орієнтованих. Водночас для всіх них характерним є поєднання механізмів обміну інформацією, правових обов'язків операторів критичної інфраструктури та процедур державного контролю.

Саме в цьому контексті особливого значення набуває принцип пропорційності, який виступає базовим критерієм оцінки допустимості державного втручання у сферу цифрових прав та свобод.

Принцип пропорційності є ключовим для оцінки будь-яких заходів у сфері кібербезпеки. Він включає: легітимну мету; необхідність; адекватність; співмірність втручання.

Після імплементації NIS2 держави ЄС активно застосовують ризикоорієнтований підхід, що дозволяє диференціювати обсяг обов'язків залежно від категорії суб'єкта [9]. Така модель зменшує надмірний регуляторний тиск на малі підприємства та забезпечує економічну пропорційність.

Для України принцип пропорційності має особливе значення в умовах воєнного стану, коли допустимі більш суворі заходи безпеки, однак вони не повинні нівелювати сутність прав людини.

Перша редакція NIS Directive 2016/1148 [9] була орієнтована переважно на мінімальні вимоги до безпеки та повідомлення про інциденти. NIS2 [2] суттєво розширила сферу дії, запровадивши governance model та персоналізовану відповідальність керівництва.

Directive (EU) 2022/2557 [1] (CER) інтегрувала кіберризики у ширший контекст фізичної та організаційної стійкості. Таким чином, відбувся перехід від моделі «захисту систем» до моделі «забезпечення безперервності функціонування».

Governance model передбачає: участь керівництва у затвердженні заходів безпеки; регулярну оцінку ризиків; внутрішній аудит; відповідальність за невиконання зобов'язань. Таким чином, governance model трансформує юридичний обов'язок дотримання стандартів безпеки в елемент стратегічного управління компанією,

інтегруючи кіберризики до системи корпоративного контролю та внутрішнього аудиту.

Ця модель перетворює кібербезпеку на складник корпоративного управління.

За даними звітів Європейської Комісії щодо впровадження NIS [27], основними проблемами першої директиви були фрагментарність національних режимів та нерівномірність санкцій.

Після ухвалення NIS2 [2] держави-члени отримали більш чіткі критерії визначення суб'єктів та механізми нагляду. Очікується, що до кінця 2026 року більшість країн завершить гармонізацію національного законодавства.

European Union Agency for Cybersecurity [28] відіграє координаційну та методичну роль у реалізації європейської політики кіберстійкості. Її діяльність сприяє гармонізації підходів до ППС, формуванню спільних стандартів реагування та розвитку транскордонної довіри.

У системному вимірі ППС у сфері кібербезпеки постає як багаторівнева правова конструкція, що поєднує адміністративне регулювання, корпоративне управління, фінансові стимули та міжнародно-правові механізми відповідальності. Її ефективність визначається не лише нормативною деталізацією, а й здатністю інтегрувати принципи пропорційності, економічної доцільності та захисту прав людини у практичні процедури реагування.

4. Баланс інтересів держави, бізнесу та суспільства у сфері кібербезпеки: правові конфлікти та шляхи їх вирішення

У 2026 році проблема балансу інтересів у сфері кібербезпеки набуває для України системного характеру, оскільки поєднує три взаємопов'язані виміри: воєнну агресію проти держави, інтенсивну цифрову трансформацію публічного управління та поступову інтеграцію до правового простору Європейського Союзу. У таких

умовах публічно-приватна співпраця перестає бути лише інструментом організаційної координації й перетворюється на простір постійного узгодження конкуруючих інтересів — безпекових, економічних і правозахисних. Саме тут виникають найбільш чутливі питання співмірності втручання держави, економічної доцільності обов'язків бізнесу та гарантій дотримання прав людини.

Для держави кібербезпека у 2026 році є не просто напрямом секторальної політики, а елементом національного суверенітету. Відповідно до Закону України «Про національну безпеку України» [4], забезпечення інформаційної та кібербезпеки належить до ключових функцій держави у сфері захисту національних інтересів. В умовах воєнного стану ця функція набуває пріоритетного значення, оскільки кібератаки безпосередньо впливають на обороноздатність, функціонування енергетики, фінансової системи, транспорту та зв'язку. З точки зору публічного права держава зобов'язана вживати активних заходів для попередження та нейтралізації загроз, що випливає з її позитивного обов'язку гарантувати безпеку громадян.

Паралельно Україна імплементує стандарти Європейського Союзу, зокрема положення Directive (EU) 2022/2555 [2] та Directive (EU) 2022/2557 [1], які передбачають посилення державного нагляду, розширення обов'язків операторів критичної інфраструктури та запровадження ефективних санкційних механізмів. Європейська модель виходить із презумпції, що кіберстійкість є спільною відповідальністю, однак координаційна та регуляторна функція держави має бути чітко визначеною й ефективною. Водночас посилення наглядових повноважень неминуче породжує ризик надмірної концентрації владних інструментів у виконавчих органах.

Практика держав — членів Європейського Союзу свідчить, що баланс інтересів у сфері кібербезпеки досягається через інституціоналізацію публічно-приватних платформ взаємодії. У багатьох

країнах функціонують галузеві центри обміну інформацією про кіберзагрози (Information Sharing and Analysis Centers — ISAC), які забезпечують безпечний обмін даними між державними органами та приватними операторами. Такі механізми дозволяють зменшити інформаційну асиметрію та підвищити рівень довіри між учасниками системи кіберзахисту [28].

У 2026 році для України принципово важливо забезпечити, щоб розширення контрольних функцій не трансформувалося у непропорційне втручання у господарську діяльність та не порушувало принцип верховенства права. Йдеться не лише про формальну законність повноважень, а й про їхню змістовну обґрунтованість, процесуальні гарантії та можливість ефективного судового контролю. В умовах воєнного стану спокуса спростити процедури або розширити дискрецію органів влади є об'єктивною, проте довгострокова стійкість правової системи залежить від збереження балансу між безпекою і свободою.

З боку бізнесу інтерес полягає у збереженні економічної стабільності та передбачуваності регуляторного середовища. Приватні оператори критичної інфраструктури несуть значне фінансове навантаження, пов'язане з виконанням вимог кіберстійкості. Впровадження систем управління ризиками, проведення регулярних аудитів, сертифікація інформаційних систем, створення резервних дата-центрів, інвестиції у системи резервного живлення та кіберстрахування — усе це потребує довгострокових інвестицій. Для великого бізнесу такі витрати можуть розглядатися як елемент корпоративної відповідальності, тоді як для малого і середнього бізнесу вони здатні стати фактором зниження конкурентоспроможності.

У Європейському Союзі відповідно до NIS2 [2] передбачено значні штрафи за недотримання вимог кібербезпеки, що можуть сягати суттєвого відсотка річного обороту компанії. Такий підхід

формує дисципліну та стимулює керівництво компаній інтегрувати кіберризики у систему корпоративного управління. Проте поряд із санкціями застосовуються й інструменти підтримки, зокрема механізми, передбачені Regulation (EU) 2021/241 [16], які дозволяють державам-членам спрямовувати кошти на цифрову трансформацію та зміцнення кіберзахисту. Таким чином, у праві ЄС простежується поєднання примусу та стимулювання.

Важливою новелою європейського регулювання є персональна відповідальність керівництва компаній за дотримання вимог кібербезпеки. Директива передбачає обов'язок менеджменту забезпечувати належну систему управління кіберризиками, а також проходити відповідну підготовку. Такий підхід формує нову управлінську культуру, у межах якої кібербезпека розглядається не лише як технічне питання, а як елемент корпоративного управління та стратегічного планування.

В Україні проблема полягає в тому, що нормативні обов'язки бізнесу нерідко не супроводжуються достатніми компенсаційними механізмами. Витрати на кібербезпеку сприймаються як додатковий регуляторний тягар, особливо в умовах воєнної економіки. У 2026 році питання податкових стимулів, державного співфінансування стратегічних проєктів та розвитку ринку кіберстрахування має стати одним із ключових напрямів реформи. Без економічно збалансованої моделі співпраці ризик формального виконання вимог або їх ігнорування зростатиме.

Одним із можливих інструментів формування економічно збалансованої моделі публічно-приватної співпраці у сфері кібербезпеки є розвиток механізмів кіберстрахування. У державах Європейського Союзу ринок кіберстрахування поступово стає важливим елементом управління кіберризиками, оскільки дозволяє частково компенсувати фінансові втрати від інцидентів інформаційної безпеки та стимулює бізнес інвестувати у підвищення рівня захисту

цифрових систем. Страхові компанії, оцінюючи рівень кіберзахисту підприємств, фактично формують додатковий ринковий механізм контролю за дотриманням стандартів безпеки. У цьому контексті розвиток кіберстрахування в Україні може стати важливим фактором формування культури управління кіберризиками, а також інструментом часткового розподілу відповідальності між державою, бізнесом та страховим сектором.

Поряд із цим у практиці Європейського Союзу застосовуються фінансові інструменти стимулювання кіберстійкості, зокрема програми державного співфінансування цифрової модернізації та фонди підтримки інфраструктурної безпеки. Значну роль у цьому відіграють механізми фінансування в межах політики відновлення та стійкості ЄС, які передбачають інвестиції у цифрову трансформацію та захист критичних інформаційних систем [16]. Крім того, у ряді держав-членів застосовуються податкові стимули для підприємств, що інвестують у модернізацію систем кібербезпеки, включаючи можливість податкових відрахувань або спеціальних програм підтримки інновацій у сфері інформаційної безпеки. Запровадження подібних інструментів в Україні могло б сприяти формуванню більш стійкої системи взаємодії держави та приватного сектору у сфері захисту цифрової інфраструктури.

Суспільний інтерес у сфері кібербезпеки проявляється передусім через забезпечення безперервності публічних послуг та захист основоположних прав. Порушення роботи електронних реєстрів, медичних інформаційних систем чи банківських сервісів безпосередньо впливає на реалізацію прав, гарантованих Конституцією України. Право на соціальний захист, медичну допомогу, свободу підприємницької діяльності чи доступ до інформації сьогодні значною мірою залежить від стабільності цифрової інфраструктури.

Водночас заходи кібербезпеки можуть обмежувати право на приватність, таємницю комунікацій або свободу вираження

поглядів. Розширення моніторингових повноважень, впровадження систем збору та аналізу даних, обов'язкове зберігання інформації про трафік — усе це створює ризик надмірного втручання у приватне життя. У цьому контексті доктринальні підходи до прав людини, розроблені у працях Ю. С. Шемшученка [29], набувають особливої актуальності: будь-яке обмеження прав повинно бути не лише формально законним, а й необхідним у демократичному суспільстві та пропорційним поставленій меті.

У практиці Європейського суду з прав людини підкреслюється, що втручання держави у сферу електронних комунікацій повинно супроводжуватися ефективними гарантіями проти зловживань, включаючи незалежний контроль, чіткі процедури доступу до даних та можливість подальшого судового перегляду. Такі стандарти мають бути враховані під час формування національної системи кібербезпеки.

Отже, баланс інтересів у сфері кібербезпеки базується на трьох фундаментальних принципах — законності, пропорційності та правової визначеності. Законність передбачає чітке нормативне закріплення повноважень держави й процедур їх реалізації. Пропорційність означає, що втручання у діяльність бізнесу або права людини має бути співмірним реальній загрозі. Правова визначеність вимагає передбачуваності регуляторних вимог і стабільності правового середовища.

На практиці баланс інтересів проявляється у кількох конфліктних зонах. Однією з них є обмін інформацією про інциденти. Бізнес обґрунтовано побоюється розголошення комерційної таємниці або репутаційних втрат, тоді як держава наполягає на повній та оперативній прозорості. Вирішення цього конфлікту можливе через створення захищених каналів обміну інформацією, чітке законодавче визначення режиму конфіденційності та запровадження відповідальності за неправомірне використання отриманих даних.

Іншою проблемною сферою є доступ держави до інформаційних ресурсів у період воєнного стану. Потреба в оперативності не повинна нівелювати процесуальні гарантії, зокрема судовий контроль або можливість оскарження рішень. Лише за таких умов розширені повноваження зберігатимуть легітимність у демократичному суспільстві.

Не менш складним є питання фінансування заходів кіберстійкості. Витрати бізнесу можуть перевищувати безпосередні економічні вигоди, що створює напруженість у відносинах із державою. Запровадження моделей співфінансування, розвиток ринку кіберстрахування та участь міжнародних донорів здатні зменшити цю напругу та підвищити рівень довіри.

Ще однією проблемною зоною є кадрове забезпечення кібербезпеки. Державні органи та приватні компанії фактично конкурують за обмежену кількість висококваліфікованих фахівців у сфері кіберзахисту. Нерідко приватний сектор пропонує значно вищі фінансові умови, що ускладнює формування спроможних державних кіберструктур. У таких умовах актуальним стає розвиток програм спільної підготовки кадрів, академічно-індустріальних партнерств та механізмів тимчасового обміну експертами між державними органами та бізнесом.

Окрему увагу слід приділити транскордонним інцидентам. З огляду на інтеграцію України до європейського правового простору відповідно до Association Agreement between the European Union and Ukraine [6], виникає необхідність узгодження процедур реагування та відповідальності у випадку кібератак міжнародного характеру. Координація з європейськими структурами, взаємне визнання результатів розслідувань і обмін доказами стають невід'ємними елементами ефективної системи.

У стратегічній перспективі кібербезпека має розглядатися як сфера спільної відповідальності, де держава забезпечує нормативну

рамку й координацію, бізнес — технологічну спроможність та інновації, а суспільство — демократичний контроль і легітимність безпекових заходів. Лише за умови взаємної довіри, прозорості процедур і справедливого розподілу тягаря обов'язків можливо досягти стійкого балансу інтересів. У 2026 році саме формування такої моделі стає не лише правовим завданням, а й передумовою національної стійкості України в умовах триваючих викликів. У довгостроковій перспективі формування збалансованої моделі кібербезпеки потребує переходу від реактивної до превентивної політики, що передбачає системне управління ризиками, стратегічне планування інвестицій у цифрову інфраструктуру та розвиток культури кіберстійкості у всіх секторах суспільства.

5. Юридична відповідальність та правозастосування у сфері публічно-приватної співпраці з кібербезпеки

Станом на 2026 рік юридична відповідальність у сфері кібербезпеки перестала бути допоміжним елементом правового регулювання та набула системоутворюючого значення для всієї моделі публічно-приватної співпраці. Якщо на ранніх етапах формування національної системи кібербезпеки основна увага приділялася інституційному розмежуванню повноважень і створенню координаційних механізмів, то сучасний етап характеризується переходом до моделі відповідального управління ризиками, в якій кожен суб'єкт не лише наділений повноваженнями, але й несе чітко визначені правові наслідки за їх неналежну реалізацію.

У доктринальному вимірі юридична відповідальність у сфері кібербезпеки розглядається як сукупність правових наслідків, що настають у разі порушення встановлених стандартів управління кіберризиками та обов'язків щодо забезпечення безпеки інформаційних систем. Її функціями є не лише покарання правопорушника, але й превенція інцидентів, відновлення порушених

прав та стимулювання належної поведінки суб'єктів цифрового середовища.

Юридична відповідальність у сфері публічно-приватної співпраці (далі — ППС) має комплексний характер і охоплює адміністративні, господарські, цивільноправовий, дисциплінарні, кримінальні та міжнародно-правові механізми. Її специфіка полягає в тому, що вона виникає у сфері, де межа між публічним і приватним інтересом є рухомою. Забезпечення кіберстійкості критичної інфраструктури є публічним обов'язком держави відповідно до Закону України «Про національну безпеку України» [4], однак практична реалізація цього обов'язку значною мірою покладається на приватних операторів, діяльність яких регламентується, зокрема, Законом України «Про основні засади забезпечення кібербезпеки України» [14] та Законом України «Про критичну інфраструктуру» [5].

У науковій літературі пропонується розглядати юридичну відповідальність у сфері кібербезпеки за кількома рівнями [30]:

1) організаційний, що стосується відповідальності суб'єкта господарювання як інституції;

2) персональний, який покладається на керівництво та посадових осіб;

3) державний, пов'язаний із відповідальністю органів влади за неналежну координацію або контроль;

4) міжнародний, що виникає у випадку участі держав у кібератаках або невиконання міжнародних зобов'язань.

Європейський підхід, закріплений у Directive (EU) 2022/2555 [2], виходить із принципу, що кібербезпека є складником корпоративного управління, а отже, відповідальність має бути не лише інституційною, але й персоналізованою. У поєднанні з Directive (EU) 2022/2557 [1] цей підхід формує модель, у якій невиконання обов'язків щодо управління ризиками розглядається як порушення публічного інтересу.

В українському праві питання відповідальності поки що розвивається менш системно. Норми про адміністративні санкції, господарські штрафи або кримінальну відповідальність існують фрагментарно, проте відсутня цілісна концепція відповідальності керівництва операторів критичної інфраструктури за неналежне управління кіберризиками. Саме тому у 2026 році актуальним є формування інтегрованої моделі, що поєднує європейські стандарти з національною специфікою воєнного періоду.

Адміністративна відповідальність у сфері кібербезпеки пов'язана передусім із невиконанням встановлених законом обов'язків щодо впровадження систем управління ризиками, повідомлення про інциденти, проходження аудитів та надання інформації компетентним органам. У Європейському Союзі NIS2 встановлює значні фінансові санкції, що можуть сягати до 10 млн євро або 2 % від загального світового річного обороту підприємства, залежно від того, яка сума є більшою [2]. Такий розмір штрафів має превентивний характер і стимулює інтеграцію кібербезпеки у стратегічні рішення компаній.

В Україні адміністративні санкції за порушення вимог у сфері кібербезпеки не мають настільки вираженого стримувального ефекту. Наявні механізми відповідальності зазвичай застосовуються в межах господарського законодавства або законодавства про захист інформації. Водночас Закон України «Про критичну інфраструктуру» [5] не містить детально прописаної системи санкцій за невиконання заходів зі забезпечення стійкості, що створює прогалину у правозастосуванні.

Додатковою проблемою є інституційна фрагментація органів контролю. Повноваження у сфері кібербезпеки розподілені між кількома органами державної влади, включаючи Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, Національний банк України та інші регулятори. Така

багаторівнева система потребує чіткого розмежування компетенції та узгоджених процедур правозастосування.

Господарська відповідальність може проявлятися у формі відшкодування збитків, завданих неналежним забезпеченням кіберзахисту. Наприклад, якщо внаслідок порушення стандартів безпеки відбувається витік даних або зупинка критичного сервісу, оператор може нести відповідальність перед контрагентами чи споживачами послуг. Проте для ефективного застосування цього механізму необхідно чітко визначити стандарт належної обачності, що у сфері кібербезпеки є динамічним і залежить від розвитку технологій.

У 2026 році доцільним є законодавче закріплення обов'язковості впровадження мінімальних стандартів управління ризиками, узгоджених із міжнародними практиками, що дозволило б судовим органам оцінювати дії оператора через призму конкретних критеріїв, а не абстрактної категорії «належного рівня захисту».

Однією з найбільш суттєвих новел європейського регулювання є персоналізація відповідальності. Відповідно до NIS2 [2], керівні органи суттєвих та важливих суб'єктів зобов'язані затверджувати заходи з управління кіберризиками, контролювати їх реалізацію та проходити спеціалізоване навчання. Невиконання цих обов'язків може стати підставою для застосування санкцій або навіть тимчасової заборони обіймати керівні посади.

Такий підхід принципово змінює філософію регулювання: кібербезпека перестає бути виключною сферою технічних підрозділів і стає елементом стратегічного управління. У правовому сенсі це означає розширення змісту фідуціарних обов'язків менеджменту — поряд із фінансовою стабільністю та дотриманням корпоративного законодавства керівництво несе відповідальність за кіберстійкість організації.

В Україні аналогічний механізм поки що не розвинений. Законодавство не містить прямої норми, яка б покладала персональну

відповідальність на членів правління або наглядових рад операторів критичної інфраструктури за неналежне управління кіберризиками. У контексті європейської інтеграції та виконання зобов'язань за Угодою про асоціацію [6] доцільним є поступове впровадження такої моделі з урахуванням принципів пропорційності та правової визначеності.

Персоналізація відповідальності не повинна перетворюватися на інструмент тиску, проте вона здатна сформувати культуру відповідального управління, в якій кібербезпека сприймається як стратегічний ресурс, а не як технічний додаток до основної діяльності.

У сфері ППС особливе значення має цивільно-правовий механізм відшкодування шкоди. Кібератаки можуть спричиняти як прямі матеріальні збитки (втрата даних, зупинка виробництва, фінансові втрати), так і нематеріальні (порушення репутації, зниження довіри споживачів). У разі доведення причинно-наслідкового зв'язку між бездіяльністю оператора та настанням шкоди можливе застосування загальних норм деліктного права.

Проблема полягає у складності доказування. Додатковою складністю є визначення стандарту доказування у справах, пов'язаних із кіберінцидентами. Судові органи повинні оцінювати технічні аспекти функціонування інформаційних систем, що потребує залучення експертних знань. У зв'язку з цим важливим напрямом розвитку правозастосування є формування спеціалізованої судової практики та використання технічної експертизи у сфері кібербезпеки. Кіберінциденти часто мають транскордонний характер, що ускладнює атрибуцію дій та визначення винної сторони. У воєнних умовах додатковим фактором є можливість визнання кібератаки обставиною непереборної сили.

Перспективним напрямом є розвиток ринку кіберстрахування, який дозволяє перерозподіляти ризики між учасниками правовідносин. Страхування не замінює юридичну відповідальність, але створює

фінансовий буфер для покриття збитків, що особливо важливо у сфері критичної інфраструктури. За даними OECD, ринок кіберстрахування демонструє стабільне зростання у 2023–2025 роках [31], що свідчить про інституціоналізацію цього інструменту.

Кримінально-правовий аспект стосується як відповідальності фізичних осіб за здійснення кібератак, так і відповідальності службових осіб за службову недбалість у сфері кіберзахисту. У 2026 році для України ключовим залишається питання притягнення до відповідальності за кібероперації, пов'язані з агресією проти держави.

Особливого значення набуває кримінально-правова кваліфікація дій службових осіб, які через недбалість або неналежне виконання службових обов'язків допускають істотні порушення вимог кіберзахисту. У випадках, коли такі порушення спричиняють тяжкі наслідки для функціонування критичної інфраструктури, можливе застосування норм кримінального законодавства щодо службової недбалості або зловживання службовим становищем.

Міжнародно-правовий вимір визначається положеннями Articles on Responsibility of States for Internationally Wrongful Acts, які встановлюють принципи відповідальності держав за міжнародно-протиправні діяння [15]. У контексті кіберпростору центральною проблемою є атрибуція — встановлення зв'язку між кібератакою та конкретною державою. Якщо такий зв'язок доведено, можливе застосування механізмів міжнародно-правової відповідальності, включаючи контрзаходи.

У сучасній доктрині міжнародного права активно обговорюються підходи до застосування принципів державної відповідальності у кіберпросторі. Одним із таких підходів є використання стандарту «належної обачності» (due diligence), відповідно до якого держава повинна вживати розумних заходів для запобігання використанню своєї території або інфраструктури для здійснення кібератак проти інших держав.

Для України це питання має не теоретичне, а практичне значення, з огляду на системні кібератаки, що супроводжують воєнну агресію. Формування доказової бази та документування інцидентів є необхідною умовою подальших міжнародно-правових процедур.

Посилення наглядових повноважень держави у сфері кібербезпеки повинно супроводжуватися ефективними механізмами судового контролю. Відповідно до принципу верховенства права, розкритого у працях М. І. Козюбри [8], будь-яке втручання у сферу господарської діяльності має бути передбаченим законом, необхідним і пропорційним поставленій меті.

Оператори критичної інфраструктури повинні мати можливість оскаржувати приписи органів контролю, рішення про накладення санкцій або вимоги щодо розкриття інформації. Процесуальні гарантії (доступ до матеріалів перевірки, право бути заслуханим, можливість судового перегляду) є обов'язковими елементами легітимності державного втручання.

В умовах воєнного стану допустимі певні обмеження, однак вони не повинні нівелювати сутність права на ефективний засіб правового захисту. Саме баланс між безпекою та свободою визначає якість правової системи у кризових умовах.

Європейський підхід поєднує санкції з фінансовою підтримкою. Зокрема, Regulation (EU) 2021/241 передбачає фінансування реформ і проєктів, спрямованих на зміцнення цифрової інфраструктури [16]. Це дозволяє зменшити фінансове навантаження на операторів та стимулювати інвестиції у кіберзахист. ENISA у своїх методичних рекомендаціях щодо імплементації NIS2 наголошує на необхідності поєднання регуляторного контролю з консультаційною та методичною підтримкою суб'єктів [28].

Для України актуальним є створення змішаної моделі фінансування, що включає бюджетні кошти, міжнародну допомогу та інвестиції бізнесу. Відповідальність за неналежне забезпечення

кіберстійкості не повинна зводитися лише до покарання; вона має поєднуватися зі стимулюючими механізмами, що формують економічну зацікавленість у дотриманні стандартів.

Юридична відповідальність у сфері публічно-приватної співпраці з кібербезпеки у 2026 році є багаторівневою та комплексною. Вона охоплює адміністративні, господарські, цивільні, кримінальні та міжнародно-правові механізми, а також інтегрується у систему корпоративного управління. Європейська модель демонструє тенденцію до персоналізації відповідальності та поєднання санкцій із фінансовими стимулами. Українська система перебуває у стадії розвитку та потребує подальшої гармонізації з європейськими стандартами.

Формування цілісної моделі відповідальності є необхідною умовою ефективності ППС, оскільки лише чітке визначення правових наслідків за неналежне управління кіберризиками забезпечує реальну, а не декларативну стійкість критичної інфраструктури. У стратегічній перспективі розвиток системи юридичної відповідальності у сфері кібербезпеки має бути спрямований на формування превентивної моделі правового регулювання, у якій основний акцент робиться не лише на покаранні за порушення, але й на створенні стимулів для добровільного дотримання стандартів кіберстійкості.

6. Висновки

Монографічне дослідження «Публічно-приватна співпраця у сфері кібербезпеки: баланс інтересів держави, бізнесу та суспільства» присвячене комплексному аналізу правової природи, інституційних механізмів та перспектив розвитку взаємодії публічного і приватного секторів у сфері кібербезпеки в умовах цифрової трансформації та воєнних викликів. У роботі послідовно доведено, що у 2026 році кібербезпека остаточно сформувалася як багатовимірна правова категорія, яка інтегрує елементи національної безпеки, адміністративного регулювання, господарської діяльності та

захисту прав людини, а отже, потребує міжгалузевого підходу до правового осмислення.

Проведене дослідження засвідчило, що кібербезпека перестала бути суто технічною або технологічною проблемою. Вона трансформувалася у самостійний напрям державної політики, який визначає рівень стійкості інституцій, економіки та суспільства загалом. У цифровізованому середовищі стабільність державного управління, функціонування фінансової системи, енергетики, транспорту, охорони здоров'я безпосередньо залежать від стану кіберзахисту. Саме тому кібербезпека у 2026 році розглядається не як допоміжна складник інформаційної політики, а як базовий чинник національної стійкості.

У межах монографії обґрунтовано, що публічно-приватна співпраця у сфері кібербезпеки не є факультативним або додатковим інструментом державного управління. Вона виступає системоутворюючим елементом сучасної моделі забезпечення національної безпеки. Об'єктивна залежність держави від приватних операторів критичної цифрової інфраструктури — телекомунікаційних компаній, банківських установ, енергетичних підприємств, IT-провайдерів — зумовлює необхідність нормативного оформлення спільної відповідальності, інституційної координації та справедливого розподілу ризиків. Держава не може ефективно гарантувати кіберстійкість без залучення технологічних ресурсів бізнесу, а бізнес, своєю чергою, не може забезпечити повноцінний захист без нормативної підтримки та координації з боку публічної влади.

Аналіз правового регулювання Європейського Союзу продемонстрував, що сучасна концепція кіберстійкості закріплена, зокрема, у Directive (EU) 2022/2555 [2] та Directive (EU) 2022/2557 [1], які формують інтегровану модель управління кібер- та фізичними ризиками. Ці акти встановлюють ризикоорієнтований нагляд, запроваджують персональну відповідальність керівництва суб'єктів,

передбачають високий рівень інституційної координації та визначають стандарти кризового реагування. Європейський підхід поєднує регуляторний примус із фінансовими стимулами, зокрема через механізми, передбачені Regulation (EU) 2021/241 [16], що спрямовані на підтримку цифрової трансформації та інвестицій у кіберзахист. Таким чином, у праві ЄС сформовано цілісну модель, де вимоги до бізнесу супроводжуються інструментами підтримки й координації.

Практичне втілення зазначених підходів простежується у національних моделях окремих держав-членів Європейського Союзу. Зокрема, у Німеччині ключову роль у координації кібербезпеки відіграє Федеральне відомство з безпеки інформаційної техніки (BSI), діяльність якого спрямована на організацію обміну інформацією між державними органами та операторами критичної інфраструктури. У Нідерландах сформовано модель партнерської взаємодії держави та бізнесу, засновану на активній ролі National Cyber Security Centre (NCSC) та механізмах добровільно-обов'язкового обміну інформацією про кіберінциденти. Франція, своєю чергою, використовує більш централізований підхід, у межах якого Національне агентство з безпеки інформаційних систем (ANSSI) здійснює регуляторний нагляд, сертифікацію засобів кіберзахисту та контроль за діяльністю операторів життєво важливих об'єктів. Досвід цих держав свідчить про можливість існування різних інституційних моделей публічно-приватної співпраці, об'єднаних спільною метою забезпечення високого рівня кіберстійкості.

Українська модель, сформована на підставі законодавства у сфері національної безпеки та кібербезпеки, перебуває у стадії активної адаптації до стандартів Європейського Союзу. Воєнні умови 2022–2026 років суттєво прискорили розвиток механізмів координації, зумовили інтенсивну взаємодію між державними органами та приватним сектором і сприяли формуванню практики спільного

реагування на кібератаки. Водночас дослідження виявило низку структурних проблем: недостатню деталізацію персональної відповідальності керівників операторів критичної інфраструктури, фрагментарність фінансових інструментів підтримки бізнесу та потребу у більш чітких процесуальних гарантіях захисту прав людини під час реалізації заходів кібербезпеки.

Практика правозастосування у 2022–2026 роках демонструє поступове формування інституційної взаємодії між державними органами, центрами реагування на кіберінциденти та операторами критичної інфраструктури. Водночас подальший розвиток цієї системи потребує чіткішого нормативного визначення процедур обміну інформацією, стандартизації реагування на кіберінциденти та посилення ролі спеціалізованих органів кіберкоординації.

Особливу увагу в роботі приділено проблемі балансу інтересів держави, бізнесу та суспільства. Доведено, що інтерес держави полягає у забезпеченні суверенітету, обороноздатності та безперервності функціонування критичної інфраструктури. Інтерес бізнесу зосереджений на збереженні економічної автономії, регуляторної передбачуваності, мінімізації надмірного адміністративного тиску та пропорційності встановлених вимог. Інтерес суспільства пов'язаний із гарантіями прав людини, цифрової довіри та безперервності публічних сервісів, що випливають із положень Конституції України [3]. У цифрову епоху реалізація конституційних прав дедалі більше залежить від стабільності інформаційних систем, а отже, кібербезпека набуває безпосереднього правозахисного виміру.

У монографії обґрунтовано, що ефективна публічно-приватна співпраця можлива лише за умови дотримання принципів верховенства права, пропорційності, правової визначеності та інституційної довіри. Надмірна концентрація контрольних повноважень держави здатна призвести до зловживань і втрати довіри з боку бізнесу та суспільства. Водночас перекладання фінансового навантаження

виключно на приватний сектор може знизити економічну стійкість операторів і, як наслідок, ослабити всю систему кіберзахисту. Баланс інтересів досягається не через домінування однієї зі сторін, а через узгодження позицій і прозорі механізми розподілу відповідальності.

У стратегічному вимірі 2026 року кібербезпека постає як спільне публічне благо. Вона не може бути забезпечена виключно силами держави, оскільки технологічна інфраструктура значною мірою перебуває у приватній власності. Водночас вона не може бути гарантована лише ринковими механізмами, адже питання національної безпеки виходять за межі комерційної доцільності. Саме тому ефективна модель кіберстійкості є результатом поєднання нормативної визначеності, інституційної координації та взаємної довіри між усіма суб'єктами правовідносин.

Додатковим фактором, що визначає актуальність публічно-приватної співпраці у сфері кібербезпеки, є стрімкий розвиток технологій штучного інтелекту, хмарних сервісів та великих даних. Ці технології відкривають нові можливості для цифрової трансформації, водночас формуючи складні ризики кіберзагроз, що мають транскордонний характер. У таких умовах координація між державою та приватним сектором набуває не лише національного, але й міжнародного виміру.

Дослідження також дозволило сформулювати перспективні напрями розвитку публічно-приватної співпраці в Україні. Серед них — подальша гармонізація із правом ЄС, удосконалення моделі персональної відповідальності керівництва суб'єктів критичної інфраструктури, розвиток механізмів співфінансування заходів кіберстійкості, а також посилення процесуальних гарантій захисту прав людини під час реалізації безпекових заходів. Важливим завданням є формування культури управління кіберризиками, за якої кібербезпека розглядатиметься не як формальний обов'язок, а як стратегічний компонент корпоративної та державної політики.

Таким чином, публічно-приватна співпраця у сфері кібербезпеки повинна розглядатися як довгострокова модель партнерства, що забезпечує стійкість держави, конкурентоспроможність економіки та ефективний захист прав людини в цифрову епоху. Концептуальний внесок монографії полягає у комплексному поєднанні теоретико-правового аналізу з практико-орієнтованим дослідженням механізмів взаємодії, що дозволяє сформувати цілісне бачення розвитку інституту публічно-приватної співпраці в умовах сучасних безпекових викликів. Отримані результати можуть бути використані при вдосконаленні законодавства України у сфері кібербезпеки, формуванні державної політики цифрової стійкості, а також у практичній діяльності органів державної влади, суб'єктів господарювання та міжнародних партнерів. Розроблені у монографії підходи можуть слугувати теоретичною основою для подальших наукових досліджень у сфері кіберправа, публічного управління та міжнародної безпеки.

Список використаних джерел:

1. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. 2022. L 333. Pp. 164–198. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022. L 333. Pp. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

3. Конституція України : Закон України від 28 червня 1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

4. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19

5. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради України*. 2022. № 5. Ст. 37. URL: https://zakon.rada.gov.ua/laws/show/1882-20

6. Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part (consolidated version). *Official Journal of the European Union*. 2014. L 161. Pp. 3–2137. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22014A0529%2801%29

7. Рабінович П. М. Основи загальної теорії права та держави. Львів : Світ, 2012. 320 с.

8. Козюбра М. І. Верховенство права: українська модель та європейський досвід. *Наукові записки НаУКМА. Серія: Юридичні науки*. 2007. Т. 64. С. 3–9.

9. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*. 2016. L 194. Pp. 1–30. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

10. European Union Agency for Cybersecurity (ENISA). Cyber Europe Programme. URL: https://www.enisa.europa.eu

11. ISO/IEC 27001:2022. Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. 3rd ed. Geneva: International Organization for Standardization, 2022. 20 p.

12. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0. 2024. URL: https://nvlpubs.nist.gov

13. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. *Official Journal of the European Union*. 2019. L 158. Pp. 1–21. URL: https://eur-lex.europa.eu/eli/reg/2019/941/oj

14. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

15. International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts. *Yearbook of the International Law Commission*. 2001. Vol. II. Part Two. Pp. 26–143. URL: https://legal.un.org

16. Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. *Official Journal of the European Union*. 2021. L 57. Pp. 17–75. URL: https://eur-lex.europa.eu/eli/reg/2021/241/oj

17. Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism. *Official Journal of the European Union*. 2021. L 185. Pp. 1–16. URL: https://eur-lex.europa.eu/eli/reg/2021/836/oj

18. Big Brother Watch and Others v. the United Kingdom. Judgment of the European Court of Human Rights, 25 May 2021.

19. Centrum för rättvisa v. Sweden. Judgment of the European Court of Human Rights, 25 May 2021.

20. European Commission. Implementation of the NIS2 Directive in EU Member States. Brussels, 2024.

21. IT-Sicherheitsgesetz 2.0. Bundesgesetzblatt I. 2021.

22. Federal Office for Information Security (BSI). Cyber Security Strategy for Germany. Bonn, 2023.

23. National Cyber Security Centre Netherlands. Annual Report 2023. The Hague, 2024.

24. Cybersecurity Act (Netherlands). Government of the Netherlands, 2022.

25. ANSSI. French National Cybersecurity Strategy. Paris, 2022.

26. ANSSI. Regulatory Framework for Operators of Vital Importance. Paris, 2023.

27. European Commission. Report on the implementation of Directive (EU) 2016/1148. Brussels, 2023.

28. European Union Agency for Cybersecurity (ENISA). NIS2 Directive: Technical Implementation Guidance. 2023.

29. Шемшученко Ю. С. та ін. Правознавство: академічний курс : підручник. Київ : Юридична думка, 2004. 520 с.

30. Shackelford S. J. Governing New Frontiers in the Information Age: Toward Cyberpeace. Cambridge : Cambridge University Press, 2020. 358 p.

31. OECD. Cyber Insurance Market Trends 2024. Paris : OECD Publishing, 2024.

References:

1. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. 2022. L 333. Pp. 164–198. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (in English).

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022. L 333. Pp. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (in English).

3. Constitution of Ukraine: Law of Ukraine No. 254k/96-VR dated 28 June 1996. *Bulletin of the Verkhovna Rada of Ukraine*. 1996. No. 30. Art. 141. URL: https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text (in Ukrainian).

4. On National Security of Ukraine: Law of Ukraine of 21 June 2018 No. 2469-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2018. No. 31. Art. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (in Ukrainian).

5. On Critical Infrastructure: Law of Ukraine of 16 November 2021 No. 1882-IX. Bulletin of the Verkhovna Rada of Ukraine. 2022. No. 5. Art. 37. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (in Ukrainian).

6. Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part (consolidated version). *Official Journal of the European Union*. 2014. L 161. Pp. 3–2137. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22014A0529%2801%29 (in English).

7. Rabinovych, P. M. Fundamentals of the General Theory of Law and State. Lviv: Svit, 2012. 320 p. (in Ukrainian).

8. Kozyubra, M. I. The rule of law: Ukrainian model and European experience. *Scientific Notes of the National Academy of Sciences of Ukraine. Legal Sciences*. 2007. Vol. 64. Pp. 3–9 (in Ukrainian).

9. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*. 2016. L 194. Pp. 1–30. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (in English).

10. European Union Agency for Cybersecurity (ENISA). Cyber Europe Programme. URL: https://www.enisa.europa.eu (in English).

11. ISO/IEC 27001:2022. Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. 3rd ed. Geneva: International Organization for Standardization, 2022. 20 p. (in English).

12. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0. 2024. URL: https://nvlpubs.nist.gov (in English).

13. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. *Official Journal of the European Union*. 2019. L 158. Pp. 1–21. URL: https://eur-lex.europa.eu/eli/reg/2019/941/oj (in English).

14. On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine of 5 October 2017 No. 2163-VIII.

Bulletin of the Verkhovna Rada of Ukraine. 2017. No. 45. Art. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian).

15. International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts. *Yearbook of the International Law Commission*. 2001. Vol. II, Part Two. Pp. 26–143. URL: https://legal.un.org (in English).

16. Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. *Official Journal of the European Union*. 2021. L 57. Pp. 17–75. URL: https://eur-lex.europa.eu/eli/reg/2021/241/oj (in English).

17. Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No. 1313/2013/EU on a Union Civil Protection Mechanism. *Official Journal of the European Union*. 2021. L 185. Pp. 1–16. URL: https://eur-lex.europa.eu/eli/reg/2021/836/oj (in English).

18. Big Brother Watch and Others v. the United Kingdom. Judgment of the European Court of Human Rights, 25 May 2021 (in English).

19. Centrum för rättvisa v. Sweden. Judgment of the European Court of Human Rights, 25 May 2021 (in English).

20. European Commission. Implementation of the NIS2 Directive in EU Member States. Brussels, 2024 (in English).

21. IT Security Act 2.0. Bundesgesetzblatt I. 2021 (in German).

22. Federal Office for Information Security (BSI). Cyber Security Strategy for Germany. Bonn, 2023 (in English).

23. National Cyber Security Centre Netherlands. Annual Report 2023. The Hague, 2024 (in English).

24. Cybersecurity Act (Netherlands). Government of the Netherlands, 2022 (in English).

25. ANSSI. French National Cybersecurity Strategy. Paris, 2022 (in French).

26. ANSSI. Regulatory Framework for Operators of Vital Importance. Paris, 2023 (in French).

27. European Commission. Report on the implementation of Directive (EU) 2016/1148. Brussels, 2023 (in English).

28. European Union Agency for Cybersecurity (ENISA). NIS2 Directive: Technical Implementation Guidance. 2023 (in English).

29. Shemshuchenko, Y. S. et al. Jurisprudence: academic course: textbook. Kyiv: Yurydychna Dumka, 2004. 520 p. (in Ukrainian).

30. Shackelford, S. J. Governing New Frontiers in the Information Age: Toward Cyberpeace. Cambridge: Cambridge University Press, 2020. 358 p. (in English).

31. OECD. Cyber Insurance Market Trends 2024. Paris: OECD Publishing, 2024 (in English).

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЄС ТА УКРАЇНИ В РЕАЛІЗАЦІЇ ПУБЛІЧНИХ ІНТЕРЕСІВ В ЕКОЛОГІЧНІЙ СФЕРІ

STRATEGIC COMMUNICATIONS OF THE EU AND UKRAINE IN IMPLEMENTING PUBLIC INTERESTS IN THE ENVIRONMENTAL SPHERE

Khorishko L. S.,
Doctor of Political Sciences, Professor,
Professor at the Department of Political Science,
Zaporizhzhia National University,
Zaporizhzhia, Ukraine

Abstract. Environmental protection is a fundamental public interest, as it defines society's need for a safe living environment and the expansion of opportunities to preserve natural resources for future generations. A key mechanism for synchronizing the efforts of policymakers, the public, and other stakeholders is the search for compromise solutions aimed at balancing private demands and public needs with the processes of sustainable, ecologically balanced development. This underscores the need to employ strategic communications to enhance political dialogue and international cooperation in the environmental sphere. By setting ambitious goals to achieve climate neutrality by 2050, the EU seeks to ensure higher levels of public well-being through the implementation of cutting-edge green technologies. The essence of the EU's public interests in the environmental sector is systematized within the European Green Deal, which aims to secure climate neutrality by 2050. Key

objectives include achieving net-zero greenhouse gas emissions by 2050, fostering economic growth through efficient resource management and the transition to a circular economy, and ensuring fairness and inclusivity in the green transition by supporting regions and resource-intensive industries. The environmental consequences of the war negatively affect all spheres of life and health of Ukrainian citizens, exacerbate the demographic crisis, making the problem of preserving human capital urgent. In this context, environmental markers are a component of post-war green reconstruction and sustainable economic development.

The purpose of the scientific investigation is to analyze the strategic communications of the EU and Ukraine in the implementation of public interests in the environmental sphere. Among the key tasks are to determine the content of public interests in the environmental sphere, to specify the features of using the resource potential of strategic communications (public diplomacy and special PR events) in the implementation of environmental public interests. The study used a systematic approach that contributed to specifying the content of public interests of the EU and Ukraine. The analysis method allowed to determine the features of using strategic communications in the implementation of public environmental interests. The formation of intermediate and final conclusions of the study was facilitated by the generalization method.

Strategic communications between the EU and Ukraine involve intensifying political dialogue on implementing the core principles of the European Green Deal. This includes mobilizing the initiatives of Ukrainian government institutions and the public to execute environmental projects aimed at expanding green transition opportunities within the context of European integration and post-war recovery. Participation in thematic conferences and partnership programs promotes the global positioning of Ukraine's environmental

interests and attracts the resource and technological potential of European partners to large-scale post-war reconstruction processes.

Keywords: Strategic Communications, European Union, Public Interests, Environmental Security, Environmental Policy, Ukraine–EU Cooperation.

1. Вступ

В умовах глобальних викликів сьогодення захист навколишнього середовища стає базовим публічним інтересом, який визначає потребу суспільства у безпечному просторі життєдіяльності та самореалізації. Синхронізації зусиль суб'єктів політики, громадськості та інших стейкхолдерів сприяє пошук компромісних рішень з метою збалансування приватних запитів і суспільних потреб з процесами сталого розвитку. Масштабні наслідки російського вторгнення в Україну актуалізують питання пошуку механізмів і ресурсів для повоєнного відновлення. Йдеться про зелену відбудову інфраструктури за принципом "Build Back Better" із залученням широко спектру інноваційних екологічних рішень. Публічний інтерес полягає у створенні енергоефективного, екологічно безпечного простору життєдіяльності та повоєнного відновлення. ЄС, ставлячи амбітні цілі у досягненні кліматичної нейтральності до 2050 року, прагне забезпечити громадянам високий рівень добробуту через упровадження новітніх зелених технологій. Міжнародні зобов'язання щодо імплементації принципів Паризької кліматичної угоди, упровадження ініціативи Європейський зелений курс (далі — ЄЗК) — все це вимагає колективної відповідальності у досягненні балансу між економічними вигодами та публічним запитом на чисте довкілля.

Ефективне реагування на глобальні екологічні виклики потребує залучення ініціативи стейкхолдерів до формування кліматичного порядку денного, гармонізації законодавства, розвитку стратегічного партнерства та впровадження зелених технологічних

інновацій. Це актуалізує потребу у використанні стратегічних комунікацій як інструменту активізації політичного діалогу та глобального партнерства. Для України стратегічні комунікації з ЄС в екологічній сфері є запорукою залучення ресурсного та технологічного потенціалу європейських партнерів до масштабних процесів повоєнного відновлення.

Метою наукового дослідження є аналіз особливостей використання ресурсного потенціалу стратегічних комунікацій ЄС та України в реалізації публічних інтересів в екологічній сфері. Серед ключових завдань — визначення змісту публічних інтересів в екологічній сфері, вивчення особливостей використання ресурсного потенціалу стратегічних комунікацій (публічної дипломатії та спеціальних PR-подій) у реалізації екологічних публічних інтересів. Системний підхід сприяв конкретизації змісту публічних інтересів ЄС та України в умовах сучасної політичної дійсності. За допомогою методу аналізу визначено особливості використання стратегічних комунікацій в реалізації публічних екологічних інтересів. Формуванню проміжних і підсумкових висновків дослідження сприяв метод узагальнення.

2. Поняття публічних інтересів в екологічній сфері

Публічні інтереси є комплексним відображенням сукупності суспільних потреб і прагнень, задоволення яких забезпечує сталість розвитку та відповідний рівень добробуту громадян. До основних характеристик публічних інтересів відносять: 1) загальність, тобто спрямованість на досягнення суспільного блага; 2) об'єктивність існування як потреба суспільного розвитку; 3) визнання державою необхідності їх захисту. На думку Дж. Дьюї, публічний інтерес формується у ході життєдіяльності суспільства на основі комунікативної взаємодії щодо синхронізації зусиль у розв'язанні актуальних проблем. Стейкхолдери

у процесі комунікації можуть приймати рішення щодо спрямування спільних зусиль на подолання ймовірних загроз приватним інтересам. Задоволення ж інтересів більшості вимагає залучення ресурсного потенціалу політичних інститутів [1, с. 12–65]. Відтак комунікація щодо механізмів впливу відбувається між політичними інститутами та суспільними групами стосовно інтересів, які набувають публічного характеру. Критеріями публічності у даному випадку є суспільна значущість, повторюваність дії, довготривалість впливу наслідків.

Науково-технічний прогрес, на думку Е. Гідденса, стає фактором виникнення непередбачуваних природних ризиків, які впливають на стабільність суспільно-політичного розвитку [2]. Це актуалізує питання захисту публічних інтересів в екологічній сфері, оскільки безпечний екологічний простір життєдіяльності є запорукою виживання людства через забезпечення трансгенераційної справедливості та економічної стабільності. Одним із інструментів взаємодії стейкхолдерів у сфері охорони навколишнього середовища є пошук компромісних рішень задля встановлення відповідного балансу між приватними та публічними інтересами [3]. Провідна роль у цьому процесі належить державі, яка має сприяти розширенню можливостей прийняття компромісного рішення в умовах наростання впливу природних ризиків. Саме компроміси забезпечують реалізацію публічних інтересів в екологічній сфері, оскільки передбачають більш зважений підхід до аналізу ймовірних втрат і переваг, формуючи відповідний рівень трансгенераційної відповідальності. Не менш важливим є залучення широкого кола стейкхолдерів до розв'язання глобальних екологічних проблем. Йдеться про актуалізацію екологічного порядку денного, оновлення національної законодавчої бази, поглиблення стратегічного партнерства та комунікацій зі стейкхолдерами, упровадження інноваційних рішень в екологічній сфері.

ЄС відіграє значну роль у позиціюванні значущості формування безпечного екологічного простору як публічного інтересу європейської спільноти. Стаття 191 Договору про функціонування ЄС акцентує увагу на таких цілях упровадження політики в екологічній сфері: 1) збереження, захист і покращення якості навколишнього середовища; 2) захист здоров'я людини; 3) раціональне природокористування; 4) підтримка політичного діалогу та стратегічного партнерства у реагуванні на екологічні виклики сьогодення [3]. Загалом на реалізацію екологічної політики впливають такі фактори як регіональні особливості стану навколишнього середовища, потенційні вигоди та витрати від дії/бездіяльності, соціально-економічний розвиток ЄС в цілому. Акцентовано увагу на потребі упровадження широкого спектру превентивних заходів, які знижують рівень забрудненості навколишнього середовища.

В Україні зміст публічних інтересів в екологічній сфері представлено в низці документів. Декларацією про державний суверенітет України визначено зобов'язання держави щодо встановлення порядку організації охорони довкілля та природокористування у контексті гарантування безпеки громадян та молодого покоління [5]. У статті 16 Конституції України обов'язком держави визначено гарантування екологічної безпеки громадянам на всій території. Стаття 50 надає громадянам право на безпечне для життєдіяльності та здоров'я довкілля, порушення якого вимагає відшкодування збитків. Не менш важливим є право громадян на отримання інформації про стан довкілля та її поширення [6]. У статті 441 Кримінального кодексу України масове знищення флори і фауни визнано злочином проти людства, тобто найвищим рівнем порушення публічного інтересу [7]. Це свідчить про визнання державою чистого довкілля базовим інтересом усього суспільства та його пріоритетності над приватними економічними вигодам.

Закон України «Про основні засади державної кліматичної політики» окреслює основні напрямки кліматичної політики держави, спрямованої на забезпечення низьковуглецевого сталого розвитку та досягнення кліматичної нейтральності до 2050 року [8]. У ньому конкретизовано зміст кліматичного врядування України, фінансові інструменти досягнення кліматичних цілей, а також синхронізовано цілі кліматичної політики держави з програмами післявоєнного відновлення. Українськими законодавцями низьковуглецевий розвиток розглядається як модель стратегування державотворчих процесів крізь призму економічного зростання на основі екологічної модернізації. Її ключовими індикаторами є зменшення викидів парникових газів і розширення можливостей їх природнього поглинання для досягнення кліматичної нейтральності. Основна мета реалізації вказаної моделі — забезпечення високої якості життя населення та сприяння раціональному природокористуванню.

Зміст публічних інтересів ЄС в екологічній сфері систематизовано в ЄЗК, мета якого — забезпечення кліматичної нейтральності до 2050 року [9]. Серед ключових цілей — досягнення нульового рівня викидів парникових газів до 2050 року, економічне зростання через ефективне природокористування та перехід до циркулярної економіки, забезпечення справедливості й інклюзивності у здійсненні зеленого переходу через підтримку регіонів і ресурсоємних галузей виробництва. У заяві для преси з нагоди імплементації ЄЗК У. фон дер Ляєн наголосила, що кінцева мета ініціативи — досягнення суспільного блага для європейської спільноти [10]. Йдеться про упровадження зелених технологічних інновацій з метою сприяння сталому економічному розвитку, формування екологічно безпечного простору життєдіяльності, а також колективну відповідальність за збереження та розширення можливостей молодого покоління в самореалізації.

До основних напрямків реалізації ЄЗК відносять: 1) декарбонізацію енергетичного сектору та поступовий перехід до використання

енергії з відновлювальних джерел; 2) розширення можливостей використання електромобілів, модернізацію інфраструктури залізничного та водного транспорту; 3) реформування сільського господарства, а саме — скорочення використання пестицидів і добрив, підтримка органічного фермерства; 4) стимулювання розвитку циркулярної економіки; 5) підвищення рівня енергоефективності житлового фонду; 6) сприяння розвитку біорізноманіття та екосистеми в цілому. ЄЗК визначає довгострокові пріоритети у захисті, збереженні та примноженні природного потенціалу ЄС, що безпосередньо впливає на підвищення рівня захисту здоров'я та благополуччя громадян від ймовірних екологічних ризиків. У цьому контексті європейські інституції покликані надавати всебічну консультативну підтримку національним владним і самоврядним інституціям, громадським активістам, бізнесу з метою синхронізації зусиль і ресурсного потенціалу в досягненні екологічних цілей.

Загалом зелений перехід передбачає не лише упровадження інноваційних технологій, але й трансформацію підходів до життєдіяльності, споживання природних ресурсів і ведення бізнесу. Європейські інституції сприяють систематичному інформуванню та залученню громадської ініціативи до прийняття рішень, пов'язаних з реалізацією публічних інтересів в екологічній сфері. Це зумовлено впливом низки факторів: 1) знанням специфіки розвитку конкретної громади та її ключових потреб; 2) необхідністю забезпечення справедливого зеленого переходу муніципалітетів через адаптацію ринку праці, надання фінансової підтримки вразливим категоріям населення, ефективний розподіл ресурсів; 3) потребою легітимізації екологічних ініціатив через громадську залученість до взаємодії. Директивою 2003/4/ЄС гарантовано право громадськості на всебічний доступ до отримання екологічної інформації та її поширення [11]. Йдеться про інформацію щодо змісту міжнародних договорів та законодавства з екологічних питань; планів і програм екологічного

розвитку; звітності про стан навколишнього середовища, моніторинг екологічної діяльності та оцінювання екологічних ризиків.

У Директиві 2003/35/ЄС вказано, що залученість громадськості та неурядових організацій до впровадження екологічної політики дозволяє владним інституціям враховувати громадську думку з приводу актуальних проблем, що підвищує рівень колективної відповідальності та публічності процесу прийняття рішень, сприяючи формуванню колективної відповідальності й екологічної свідомості [12]. По-перше, держави-члени ЄС мають сприяти розширенню можливостей громадськості приймати участь у розробці, внесенні змін до планів чи програм в екологічній сфері, крім питань, пов'язаних зі сферою безпеки. Йдеться про надання публічної інформації про зміст екологічної ініціативи та потенційні можливості участі громадян в її реалізації чи оптимізації. По-друге, процедура, канали інформування (публічні оголошення, електронні ЗМІ), види консультацій (письмове звернення, громадське розслідування) із зацікавленою громадськістю визначаються державами-членами. Коментарі та думки громадян, надіслані згідно встановленої національним законодавством процедури, обов'язкові до розгляду та раціонального врахування відповідними владними інституціями. По-третє, реалізація екологічних проєктів може потенційно впливати на стан довкілля інших держав-членів. Відтак держава-ініціатор проєкту зобов'язана проінформувати про це як іншу державу, так і її громадськість, аби забезпечити за потреби ефективну участь у процедурах прийняття рішень щодо навколишнього середовища.

Вказані Директиви спрямовані на забезпечення імплементації в європейську практику положень Орхуської конвенції, яка є основою упровадження екологічної демократії. Її мета — забезпечення права особистості на сприятливе для життя та здоров'я навколишнє середовище. Реалізації цієї мети сприяють три основні механізми: 1) доступ до інформації, тобто можливість отримувати від владних

і самоврядних інституцій інформацію щодо стану екологічної ситуації та запланованих заходів, які потенційно можуть вплинути на безпеку громадян; 2) участь у врядуванні, тобто розширення можливостей залучення громадської ініціативи до процесу прийняття рішень з екологічно значущих питань; 3) доступ до незалежного судового розгляду з метою здійснення контролю за дотриманням екологічних норм і захисту своїх екологічних прав [13]. Директива 2003/35/ЄС про громадську участь і Директива 2003/4/ЄС про доступ до екологічної інформації містять окремі положення про гарантування права на правосуддя з метою захисту екологічних прав та інтересів громадян.

Україна також ратифікувала Орхуську конвенцію, взявши на себе зобов'язання, щодо забезпечення прозорості та підзвітності перед громадянами в екологічній сфері. По-перше, розширено можливості доступу до отримання інформації про екологічну ситуацію. Йдеться про індивідуальні запити до профільних владних інституцій про стан забруднення повітря чи радіаційний фон, отримання інформації з відкритих реєстрів (ЕкоСистема, SaveEcoBot). Наприклад, національна онлайн-платформа ЕкоСистема забезпечує доступ громадян до екологічної інформації та адміністративних послуг у сфері охорони довкілля. Платформа містить такі види відкритих даних: 1) моніторинг стану довкілля в реальному часі; 2) екологічні реєстри; 3) візуалізацію даних про забруднення та стан природних ресурсів на карті України.

По-друге, гарантовано залучення громадської ініціативи до прийняття рішень, пов'язаних із оцінкою впливу на довкілля. У Законі України «Про оцінку впливу на довкілля» зазначено, що громадське обговорення забезпечує систематизацію пропозицій громадськості з подальшим їх врахуванням у плановій діяльності суб'єктів господарювання. Зауваження та пропозиції можуть надаватися як у письмовій, так і в усній формі [14]. Залучення громадян

відбувається на етапі ознайомлення з повідомленням про планову діяльність та при громадському обговоренні звіту.

Регламентом ЄС 2021/1119 зміни клімату визнано екзистенційною загрозою, що вимагає від держав-членів активізації дій у боротьбі з глобальними екологічними викликами [15]. У документі конкретизовано взаємозв'язок політик ЄС з виконанням кліматичних зобов'язань у контексті задоволення потреб та інтересів європейських громадян. По-перше, дії щодо досягнення кліматичної нейтральності синхронізовані з процесами модернізації різних секторів промисловості, серед ключових — енергетика, транспорт, енергоефективне будівництво, управління відходами, сільське господарство. Єврокомісія бере зобов'язання сприяти міжсекторальному діалогу стейкхолдерів у розробці дорожніх карт змін та залученню інвестицій для переходу до кліматично нейтральної економіки. Вказаний перехід передбачає упровадження інновацій, створення нових робочих місць і забезпечення довгострокового сталого економічного розвитку.

По-друге, інституції ЄС акцентують увагу на розширенні нормативно-правових і фінансових можливостей протидії зростаючим ризикам для здоров'я європейських громадян, пов'язаних з кліматом. Йдеться про посилення спеки, лісові пожежі та повені, поширення інфекційних захворювань, зниження якості харчових продуктів і води. По-третє, ЄС активізує політичний діалог та міжнародне співробітництво задля залучення ініціативи стейкхолдерів до пошуку ефективних інструментів розв'язання глобальних екологічних проблем. Це сприяє позиціювання глобального лідерства ЄС у кліматичній сфері. По-четверте, досягнення кліматичної нейтральності вимагає синхронізації зусиль національних урядів та європейських інституцій у виробленні спільних рішень щодо підвищення якості громадського здоров'я, розширення можливостей самореалізації громадян в умовах переходу до циркулярної економіки, створення нових робочих місць, упровадження технологічних інновацій

у скороченні викидів, а також забезпечення справедливості та солідарності держав-членів ЄС у здійсненні зеленого переходу.

Загалом у Регламенті ЄС 2021/1119, кліматична політика ЄС та держав-членів розуміється як сукупність комплексного захисту суспільства й навколишнього середовища від загроз, пов'язаних із зміною клімату. Головною метою є забезпечення добробуту та економічного процвітання в межах глобальних екологічних можливостей, що відповідає Цілям сталого розвитку ООН та Паризькій кліматичній угоді. У досягненні цієї мети ЄС керується такими принципами: 1) вживання превентивних заходів, тобто недопущення виникнення екологічних ризиків; 2) фінансова відповідальність суб'єктів за шкоду довкіллю; 3) енергоефективність у всіх секторах промисловості; 4) будь-яка економічна діяльність або реформа не повинна шкодити іншим екологічним цілям.

Досягнення кліматичної нейтральності передбачає поступовість виконання кліматичних зобов'язань з метою забезпечення справедливого та соціально-обґрунтованого переходу, враховуючи також публічні інтереси на національному рівні. У пакеті законодавчих ініціатив "Fit for 55" окреслено ряд проміжних зобов'язань: 1) скорочення викидів на 55 % до 2030 року; 2) упровадження інновацій для підвищення рівня конкурентоспроможності розвитку промисловості; 3) позиціювання ЄС як глобального лідера у боротьбі з кліматичними змінами [16]. Серед ключових інструментів "Fit for 55" — реформування системи торгівлі викидами (ETS), заборона продажу нових автомобілів з двигунами внутрішнього згорання з 2035 року, упровадження вуглецевого коригування на кордоні (CBAM), тобто податку на імпорт товарів із високим вуглецевим вмістом.

Виконання зобов'язань у межах ЄЗК є стратегічною основою для євроінтеграції та післявоєнного відновлення України. За даними Держекоінспекції сума екологічних збитків, яких зазнала Україна внаслідок війни становить близько 6,01 трлн грн [17].

Йдеться про руйнування Каховської ГЕС і греблі Оскільського водосховища, знищення флори та фауни природоохоронних територій, частина яких знаходиться в окупації, забруднення ґрунтів, збільшення токсичних викидів в атмосферу через масовані обстріли цивільної та промислової інфраструктури, мінування сільськогосподарських угідь. В умовах війни публічний інтерес в екологічній сфері пов'язується з екологічною стійкістю, складовими якої є запобігання радіаційним або хімічним аваріям на об'єктах інфраструктури, а також доведення факту завдання шкоди довкіллю для виплати репарацій на відновлення екосистем.

Екологічні наслідки війни негативно впливають на всі сфери життєдіяльності та здоров'я українських громадян, посилюють демографічну кризу, актуалізуючи проблему збереження людського капіталу в Україні. У цьому контексті екологічні маркери є складовою післявоєнної зеленої відбудови. Йдеться про забезпечення синергії між технологічними рішеннями (енергоефективне будівництво, розширення можливостей використання енергії з відновлювальних джерел), екологічними стандартами (зменшення викидів вуглецю, управління відходами), економічними стимулами (циркулярна економіка, нові робочі місця) та соціальними змінами (переосмислення значущості екологічних інтересів і цінностей).

Набувши статусу кандидата на членство в ЄС, Україна взяла на себе виконання низки зобов'язань, серед яких — адаптація до екологічних стандартів ЄС у межах 4 переговорного кластеру «Зелений прядок денний та стале з'єднання». Йдеться про синхронізацію законодавства та політики у сфері управління відходами, забезпечення якості повітря, охорони біорізноманіття, а також упровадження вуглецевого коригування імпорту та збільшення частки використання енергії з відновлювальних джерел. Прогрес у виконанні взятих зобов'язань розширює можливості України в отриманні доступу до інноваційних зелених технологій та фінансування екологічних проєктів.

Проміжним інструментом реалізації вказаних напрямків у 2024–2027 роках є ініційована ЄС програма фінансової підтримки Ukraine Facility з бюджетом у 50 млрд євро, з яких — 20 % мають спрямовуватися на здійснення зеленого переходу [18]. Поетапне досягнення цілей кліматичної нейтральності розглядається українськими урядовцями як складова післявоєнного відновлення національної економіки на основі залучення масштабних інвестицій в енергетику, низьковуглецеве виробництво сталі та стимулювання розвитку технологічного агровиробництва. Серед стратегічних пріоритетів екологічної модернізації України: 1) досягнення кліматичної нейтральності у межах взятих міжнародних зобов'язань; 2) упровадження сучасних технологій моніторингу та очищення для мінімізації забруднення довкілля промисловими підприємствами; 3) запуск національного ринку торгівлі шкідливими викидами; 4) посилення протидії незаконній вирубці лісів та сприяння розширенню лісових площ; 5) активізація переходу до циркулярної економіки. Реалізація вказаних пріоритетів потенційно сприятиме підвищенню рівня конкурентоспроможності української економіки та добробуту громадян.

У звіті ЄС про прогрес у боротьбі зі змінами клімату за 2025 рік окреслено низку тенденцій, що формують ризики для життєдіяльності європейської спільноти: 1) екстремальна спека та спровоковані нею лісові пожежі у Греції, Болгарії, Румунії; 2) масштабні повені у Франції, Іспанії, Німеччині, Бельгії та Нідерландах; 3) швидке танення льодовиків. Близько 440 тис. людей постраждали унаслідок вказаних природних катаклізм, що актуалізує подальшу синхронізацію зусиль держав-членів ЄС у боротьбі зі змінами клімату для захисту людського капіталу, зменшення ризиків у розвитку національних економік та забезпечення стійкості ЄС до кліматичних загроз [19]. Водночас у звіті систематизовано проміжні досягнення у зниженні викидів парникових газів у різних секторах економіки (див. Таблицю 1). Загалом ЄС досягнув загального скорочення

викидів на 1,8 % за період 2023–2024 роки, передусім, за рахунок збільшення частки споживання енергії з відновлювальних джерел. Найбільш проблемним залишається транспортний сектор, що потребує додаткових зусиль у реалізації кліматичних зобов'язань.

Таблиця 1 — Проміжні результати у зниженні викидів парникових газів у ЄС

Сектор	Ключові тенденції
Енергетика	зменшення викидів від виробництва електроенергії на 10,7 %; зростання частки відновлюваної енергетики на 8 %, за рахунок, сонячної та гідрогенерації; збільшення частки виробництва атомної енергії на 5 %; скорочення частки використання вугілля на 12 % та газу на 8%.
Промисловість	зменшення частки викидів від промислових процесів на 0,5 %, при збільшенні частки викидів при спалюванні палива для виробництва електроенергії на 0.4 %; зростання викидів у хімічному секторі на 8,2 %; зниження викидів у мінеральному секторі на 2,5 %.
Транспорт	зростання викидів від внутрішніх перевезень на 0,7 %; зростання викидів від міжнародних авіаційних і морських перевезень на 3 %.
Сільське господарство	скорочення загальної частки викидів на 1,2 %; збільшення кількості поглиначів вуглецю у секторі землекористування на 7 %.

Джерело: розроблено автором на основі [19]

На думку єврокомісара з питань клімату, нульових викидів і чистого зростання Г. Вопке, досягнуто значного прогресу у зниженні викидів парникових газів в атмосферу на 2,5 % порівняно з 2023 роком. Це свідчить про згуртованість європейської спільноти у розумінні ймовірних наслідків глобального потепління та потреби подальшої включеності у досягнення кліматичної нейтральності як запоруки підвищення якості життя громадян та конкурентоспроможності ЄС. Генеральний директор Генерального

директорату Єврокомісії з питань клімату (DG CLIMA) К. Ванденберге зазначив, що подальше інвестування у реалізацію кліматичної політики є обґрунтованим економічним вибором, спрямованим на підвищення рівня безпеки громадян в умовах глобальних викликів сьогодення. Стійкість до змін клімату є складовою стратегічної автономії ЄС та запорукою реалізації лідерського потенціалу на глобальному рівні [20]. У коментарях щодо звіту європейські очільники вкотре наголосили на важливості подальших зусиль у досягненні кліматичної нейтральності, покращенні якості життя та забезпеченні сталого розвитку ЄС.

У минулорічному зверненні до ЄС очільниця Єврокомісії У. фон дер Ляєн акцентувала увагу на значущості екологічних пріоритетів ЄЗК у досягненні стратегічної автономії та підвищенні рівня добробуту європейських громадян [21]. По-перше, ЄС займає лідерські позиції у впровадженні інновацій та зелених технологій, досягши 70 % виробництва електроенергії з відновлювальних джерел. По-друге, активізація державно-приватного партнерства та залучення додаткових інвестицій забезпечує формування нових ринків екологічного виробництва та позитивно впливає на функціонування ринку праці. По-третє, циркулярна економіка сприяє утворенню нових високотехнологічних галузей виробництва, які є цікавими для країн Глобального Півдня, Африки та Індії. Це формує передумови розвитку стратегічних партнерств та глобального масштабування екологічних маркерів ЄЗК.

Отже, зміст публічних інтересів ЄС в екологічній сфері розкривається через прагнення реалізувати лідерський потенціал у досягненні кліматичної нейтральності, створивши передумови справедливого зеленого переходу. Його ключові принципи визначені в ЄЗК, що спрямований на упровадження зелених інноваційних технологій у різні сфери життєдіяльності у контексті сприяння довгостроковому сталому розвитку економіки, підвищення рівня

добробуту європейської спільноти на основі трансгенераційної справедливості. Масштабні наслідки російського вторгнення в Україну впливають на визначення змісту публічних екологічних інтересів крізь призму повоєнного відновлення з використанням інноваційних зелених технологій. Це актуалізує потребу стратегічних комунікацій з ЄС у здійсненні зеленого переходу.

3. Стратегічні комунікації України та ЄС в екологічній сфері

В умовах глобальних викликів сьогодення стратегічні комунікації є важливим інструментом зовнішньополітичної діяльності для сучасних держав і міжнародних організацій. Доцільність їх використання замовлена: 1) потребою формування репутаційного капіталу через позиціювання суб'єкта як надійного партнера у залученні зовнішніх ресурсів та підтримки; 2) необхідністю адаптації до умов діджиталізації, що потребує впровадження інноваційних комунікативних технологій; 3) актуалізацією запиту на стратегічні партнерства, що передбачають усвідомлення цінностей та запитів стейкхолдерів; 4) створенням середовища взаємної довіри та солідарної відповідальності за спільні політичні рішення [22]. Згідно з доповіддю Chatham House, стратегічні комунікації — це комплексна та багаторівнева система дій (від планування до безпосередньої реалізації), спрямована на розуміння потреб та інтересів цільової аудиторії [23]. Основна мета — формування бажаних переконань, цінностей і моделей поведінки у суб'єктів політики із залученням різних каналів комунікації.

Стратегічні комунікації розглядаються ЄС як ключовий інструмент реалізації лідерського потенціалу та забезпечення конкурентоспроможності на глобальному рівні [24]. По-перше, ресурсний потенціал стратегічних комунікацій є основою формування європейського інформаційного порядку денного, спрямованого на актуалізацію пріоритетних тем для міжнародного політичного

дискурсу. Це передбачає залучення широкого спектру комунікаційних каналів з метою трансляції тематичних інформаційних повідомлень, розрахованих як на внутрішню, так і на зовнішню аудиторію. По-друге, використання стратегічних комунікацій вимагає чіткого алгоритму синхронізації зусиль владних інституцій та стейкхолдерів з метою пошуку найбільш оптимальних форм міжнародного партнерства для досягнення взаємовигідних інтересів. Йдеться про політико-практичний та оперативний рівні реалізації стратегічних комунікацій, що потребують різних інструментів комунікативної взаємодії (див. Таблицю 2).

Таблиця 2 — Рівні реалізації стратегічних комунікацій

Рівень	Інструменти комунікативної взаємодії	Зміст політико-комунікативної діяльності
Політико-практичний	Публічна дипломатія, інформаційні та PR-кампанії, використання медіаресурсів, управління інформаційними повідомленнями.	Стратегічне позиціонування ЄС як глобального лідера. Формування позитивного відношення громадськості до змісту політики та цінностей ЄС.
Оперативний	Моніторинг інформаційного простору, реагування на деструктивні інформаційні повідомлення третіх сторін.	Інформування громадськості про зміст порядку денного ЄС. Протидія деструктивним інформаційним впливам.

Джерело: розроблено автором на основі [24]

Для ЄС використання ресурсного потенціалу стратегічних комунікацій є вагомим інструментом реалізації лідерського потенціалу та дієвим механізмом протидії деструктивним впливам третіх сторін. До ключових інструментів стратегічних комунікацій відносять PR та публічну дипломатію, які спрямовані на здійснення цілеспрямованого впливу на формування громадської думки, розширення можливостей синхронізації ресурсів і зусиль владних інституцій зі стейкхолдерами у розв'язанні актуальних проблем.

Публічна дипломатія є багатовимірним процесом, що реалізується в ключових сферах суспільного буття [25]. Її ресурсний потенціал сприяє не тільки поясненню змісту інформаційних повідомлень, але й моделюванню порядку денного, забезпечуючи активізацію політичного діалогу та залучення ініціативи стейкхолдерів до його реалізації. Це підвищує рівень суб'єктності у позиціюванні значущості власних цінностей та захисті інтересів в умовах глобальних викликів сьогодення. Функціональне призначення PR полягає у змістовному обґрунтуванні певних ідей, цінностей та стратегій діяльності для внутрішньої та зовнішньої громадськості [26]. Основний акцент зміщується на демонстрацію гуманітарних, екологічних та соціокультурних переваг певних ідей чи цінностей. Через апеляцію до емоційної сфери PR формує у масовій свідомості переконання в етичності та доцільності обраного курсу, забезпечуючи його відповідність індивідуальним ціннісним орієнтаціям. Інструменти PR-впливу сприяють формування відповідного рівня екологічної свідомості та колективної відповідальності за майбутнє на основі пошуку компромісних рішень.

Загалом ресурсний потенціал стратегічних комунікацій розширює можливості інформування суспільства про проблеми довкілля, сприяючи зміні моделей поведінки, формуванню екологічної відповідальності та засвоєнню нових екологічно орієнтованих цінностей. Цьому також сприяє консолідація зусиль держави, бізнесу і громадян у розв'язанні глобальних екологічних проблем. По-перше, стратегічні комунікації актуалізують екологічні публічні інтересів на порядку денному, роблячи їх складовими стратегування державного розвитку. З одного боку йдеться про всебічне інформування громадськості про зміст екологічних ініціатив та інструменти їх подальшої легітимізації у відповідних рішеннях та політиках, а з іншого — про розуміння екологічних інтересів як ключового фактора безпеки, здоров'я та економічного добробуту.

По-друге, стратегічні комунікації сприяють позиціюванню екологічного лідерства конкретних держав, які через активне упровадження зелених технологій підвищують рівень репутаційного капіталу, залучають ініціативу стейкхолдерів до розв'язання актуальних екологічних проблем з метою підтримки сталого розвитку економіки. У цьому контексті відбувається поступова трансформація іміджевих характеристик держави як відповідального суб'єкта трансгенераційної екологічної діяльності. По-третє, публічний характер екологічних інтересів вимагає залученості різних стейкхолдерів до їх реалізації, ключовими з яких є владні інституції, громадські активісти, бізнес-структури, міжнародні партнери. Стратегічні комунікації перетворюють екологічні інтереси на складову суспільного договору, кожен учасник якого розуміє свою вигоду та відповідальність за майбутнє наступних поколінь.

ЄС докладає значних зусиль у використанні ресурсного потенціалу стратегічних комунікацій для актуалізації екологічного порядку денного та залучення ініціативи стейкхолдерів до міжнародного партнерства. Йдеться про активізацію публічної дипломатії задля посилення глобального політичного діалогу з питань клімату та ініціювання різних форматів міжнародного зеленого партнерства. У 2025 році Єврокомісія представила міжнародну стратегію позиціювання європейського екологічного порядку денного з метою захисту інтересів та адаптації до нових глобальних викликів сьогодення [27]. Визначено наступні напрямки реалізації лідерського потенціалу ЄС в екологічній сфері: 1) використання інноваційних зелених технологій у різних сферах промислового виробництва; 2) декарбонізація європейської економіки через розширення можливостей цифровізації, упровадження механізмів торгівлі викидами (ETS) та коригування викидів на кордоні (CBAM); 3) активізація різних форм стратегічного партнерства у кліматичній сфері через посилення дипломатичних зусиль у технологічній та регуляторній співпраці.

ЄС активно сприяє розширенню можливостей України у здійсненні зеленого переходу. Екологічна модернізація ключових сфер життєдіяльності є складовою зобов'язань у контексті євроінтеграції та післявоєнного відновлення української економіки. Україна залучена до стратегічної ініціативи EU4ClimateResilience, що фінансується ЄС та Федеральним міністерством охорони навколишнього середовища, боротьби зі зміною клімату, охорони природи та ядерної безпеки Німеччини. Її мета — підтримка зеленого переходу, посилення декарбонізації та забезпечення кліматичної стійкості в країнах Східного партнерства [28]. Серед ключових напрямків співпраці: 1) упровадження зелених технологій в агротехнологічне та промислове виробництво; 2) сприяння адаптації національних екологічних стратегій та нормативних актів до стандартів ЄС; 3) розширення можливостей бізнесу та фермерів в отриманні додаткового фінансування на реалізацію екологічних проєктів; 4) залучення ініціативи органів місцевого самоврядування до реалізації екологічних проєктів на рівні громад.

За сприяння ЄС протягом 2020-2025 років Україна приймала участь у реалізації проєкту APENA, спрямованого на забезпечення ефективності упровадження європейських екологічних стандартів регіональними і місцевими органами влади [29]. Проєкт акцентував увагу на декількох напрямках стратегічної співпраці. По-перше, сприяння синхронізації українського законодавства в екологічній сфері з європейським стандартам. По-друге, забезпечення інституційної стійкості національних органів влади через упровадження європейських управлінських і технічних процедур в реалізації ключових напрямків екологічної політики. По-третє, розширення можливостей залучення ініціативи громад і бізнесу до розробки планів адаптації до змін клімату та управління відходами.

Українські міста та окремі громади є підписантами Угоди мерів-Схід (CoM East), що покликана активізувати співпрацю владних

інституцій, місцевого самоврядування та громад країн Східного партнерства у сфері клімату та енергетики [30]. Міста-підписанти взяли на себе зобов'язання щодо скорочення викидів вуглецю та підвищення рівня стійкості територіальних громад до кліматичних змін. Співпраця у межах угоди розширює можливості громад у: 1) доступі до спеціалізованих служб підтримки та методичних рекомендацій щодо фінансування екопроєктів; 2) залученні до різних освітньо-просвітницьких ініціатив та обміні досвідом зі стейкхолдерами; 3) отриманні інструментів планування діяльності та шаблонів звітності; 4) використанні даних Дослідницького центру Єврокомісії для здійснення моніторингу досягнень. В основу співпраці покладені принципи прозорості, адаптивності, відповідальності та публічності.

Слід зазначити, що на рівні ЄС міста розглядаються ключовим суб'єктами реалізації європейських амбіцій щодо досягнення кліматичної нейтральності [31]. По-перше, міські простори відкриті до упровадження інновацій та зелених технологій, оскільки виступають ключовими осередками економічної активності в умовах глобального розвитку. По-друге, саме у містах проживає близько 75 % європейського населення, наслідком чого є доволі високі показники вуглецевих викидів. Відтак ЄС прагне активізувати залучення міської ініціативи до реалізації ключових принципів ЄЗК з метою підвищення рівня добробуту європейських громадян. У межах програми Horizon Europe започаткована Місія «100 кліматично нейтральних і розумних міст до 2030 року», що передбачає екологічну трансформацію європейських міст у центри передового досвіду та інновацій.

Наразі учасниками місії є 377 міст як країн-членів ЄС, так і міста з так званих асоційованих країн. Основою співпраці є залучення участі громадськості та інших стейкхолдерів до формування контрактів кліматичних міст. Вони визначають дорожню карту досягнення кліматичної нейтральності, плани підвищення рівня енергоефективності та управління відходами, а також інструменти

фінансування. Успішне виконання плану передбачає отримання знаку Місії ЄС, що розширює можливості доступ до державного та приватного фінансування.

У цьому році вказану нагороду отримали — Дортмунд (Німеччина) за ініціативу громади у використанні балконних сонячних систем генерування та зберігання енергії; функціональна міська зона Сараєво (Боснія та Герцеговина) за зміцнення міської демократії через розширення можливостей залучення громадської ініціативи до виконання кліматичного контракту; Ельбасан (Албанія) за міжсекторальний підхід до розвитку агросонячних систем та використання геотермальної енергії у сільському господарстві та будівництві [32]. Активізації стратегічних комунікацій європейських міст сприяє онлайн платформа NetZeroCities, яка акумулює дані, ресурси та різні інструменти упровадження екологічної політики на міському рівні.

Визнаючи прогрес України в імплементації ключових принципів кліматичної нейтральності на шляху до євроінтеграції, ЄС започаткував ініціативу SUN4Ukraine. У межах якої Чернігів, Чернівці, Дніпро, Калуш, Харків, Конотоп, Київ, Миколаїв, Нововолинськ, Первомайськ, Вінниця та Звягель долучені до Місії ЄС «100 кліматично нейтральних і розумних міст до 2030 року». Серед ключових завдань ініціативи SUN4Ukraine: 1) технічна та консультаційна підтримка українських міст на шляху до кліматичної нейтральності; 2) активізація обміну передовим європейським досвідом в реалізації кліматичної політики через міські партнерства; 3) залучення ініціативи громадян та стейкхолдерів до міського планування та упровадження зелених технологій [33]. Українські міста отримали унікальну можливість через навчання та різні формати комунікативної взаємодії (начальні візити, конференції міст Місії ЄС), не тільки вивчати передовий досвід європейських міст-наставників, але й масштабувати в межах країни інноваційні рішення сталого міського розвитку.

Прагнучи активізації взаємодії зі стейкхолдерами у розв'язанні глобальних кліматичних проблем, ЄС продовжує з 1992 року фінансування програми LIFE [34]. Її бюджет на період 2021–2027 року становить 5,4 млрд євро. Фінансування розподіляється за чотирма стратегічними напрямками: 1) природа та біорізноманіття: розмінування відновлення екосистем та заповідних територій; 2) циркулярна економіка та якість життя: управління відходами, технологій очищення води, зменшення викидів вуглецю; 3) запобігання змінам клімату та адаптація: процеси декарбонізації, забезпечення стійкості міст до кліматичних змін; 4) перехід до чистої енергії: підвищення рівня енергоефективності та розширення можливостей використання відновлюваних джерел енергії.

У межах програми LIFE відбувається реалізація проєкту Debris2Resource, що фокусується на переробці будівельного сміття від руйнувань у містах Ірпінь і Бородянка Київській області [35]. Серед ключових досягнень проєкту — утворення регенеративних хабів, переробка 5 тис. тон відходів, організація навчання представників владних інституцій та муніципалітетів основам управління відходами, розробка механізмів циклічної економіки та системних рішень з управління відходами на рівні українських громад, поглиблення співпраці з європейськими партнерам у контексті післявоєнної відбудови. Залученість до проєкту Debris2Resource сприяє імплементації в Україні передового досвіду управління відходами руйнувань. Це стратегічний крок до формування екологічної безпеки громад, збереження ресурсів та практичного втілення євроінтеграційних прагнень у сфері зеленої відбудови.

Ініціатива New European Bauhaus (NEB) — це інноваційна платформа активізації політичного діалогу зі стейкхолдерами, спрямована на залучення ресурсного потенціалу науки, культури й інноваційних технологій для створення екологічного та інклюзивного середовища життєдіяльності [36]. У межах реалізації проєктів NEB

значна увага приділяється залученню громадської ініціативи до стратегування сталого екологічного розвитку громад, враховуючи їх ключові інтереси. Проєкти NEB отримують фінансову підтримку через програму Horizon Europe та прямі бюджетні асигнування ЄС, що дозволяє залучати масштабні інвестиції для модернізації громад в умовах глобальних кліматичних викликів.

Проєкт громади Львова «Над джерелом» отримав престижну нагороду New European Bauhaus Prize 2024 як взірець ревіталізації занедбаної території виробничого кар'єру на екологічний та інклюзивний простір психологічної реабілітації [37]. Проєкт спрямований на вирішення важливого соціального завдання — розширення можливостей інтеграції внутрішньо переміщених осіб, забезпечення їхньої психологічної реабілітації через гармонійне поєднання природного ландшафту з екологічною інфраструктурою на основі натуральних матеріалів.

ЄС активно ініціює проведення спеціальних PR-подій, спрямованих на глобальне позиціювання ключових трендів європейського екологічного порядку денного та залучення ініціативи стейкхолдерів до стратегічної комунікації. Цьому сприяє участь у роботі щорічних кліматичних конференцій ООН (COP) [38]. У межах роботи COP29 в Азербайджані ЄС відігравав провідну роль у стратегічній комунікації зі стейкхолдерами щодо угоди про нову колективну кількісну мету у фінансуванні кліматичних заходів після 2025 року. Зокрема, учасники конференції дійшли згоди у питаннях: 1) збільшення фінансування третіх країн з метою забезпечення справедливого зеленого переходу; 2) функціонування міжнародних ринків вуглецю у контексті Паризької кліматичної угоди. Міністри з кліматичних питань напередодні COP30 у Бразилії погодили єдиний європейський внесок у скорочення викидів парникових газів до 2035 року на 66,25 % порівняно з 72,5 % у 1990 році.

У ході роботи COP30 у Бразилії українські урядовці за підтримки європейських партнерів представили світовій громадськості: 1) плани скорочення вуглецевих викидів на 65 % до 2035 року; 2) звітність щодо виконання кліматичних зобов'язань у рамках Паризької кліматичної угоди; 3) візію Довгострокової стратегії низьковуглецевого розвитку [39]. Україна активно співпрацює з ЄС під час роботи щорічних COP з метою актуалізації на глобальному порядку денному проблем, пов'язаних із значними екологічними наслідками повномасштабного російського вторгнення. У межах роботи національного павільйону COP30 відбулася низка панельних дискусій зі стейкхолдерами. Серед ключових питань: 1) механізми забезпечення післявоєнної відбудови та сталого розвитку України; 2) ресурсний потенціал екологічної стійкості в умовах війни; 3) залучення громадської ініціативи до реалізації основних цілей кліматичної політики; 4) перспективи упровадження інноваційних зелених технологій.

Представники українських муніципалітетів були запрошені на 4-ту Конференцію «Використання успіхів міст: просування кліматичних дій до 2030 року» у межах реалізації Місії ЄС [40]. У ході конференції проведено декілька панельних дискусій щодо: 1) особливостей забезпечення стійкості міст в умовах війни, зокрема, можливості врахування у європейській практиці українського досвіду; 2) розширення форматів політичного діалогу та співпраці українських міст з європейськими містами-партнерами; 3) механізмів реагування на сучасні кліматичні виклики. Представництвом SUN4Ukraine було також організовано семінар з метою активізації політичного діалогу стейкхолдерів щодо надання підтримки українським муніципалітетам на шляху до кліматичної нейтральності. Йдеться про розширення можливостей технічної підтримки, навчання, активізацію обміну досвідом з містами-партнерами, організацію низки багаторівневих діалогів щодо оптимізації моделей сталого міського розвитку.

Активізації участі українських міст у Місії ЄС сприяє низка тематичних заходів у межах Партнерської програми SUN4Ukraine [41]. Її мета — надати консультативну підтримку у стратегуванні сталого міського розвитку шляхом обміну досвідом та узгодження з амбітними цілями Місії ЄС. Під час візиту до міста-ментора Мюнхена представники українських муніципалітетів були долучені до панельної дискусії «Об'єднання зеленого майбутнього: міські інновації ЄС зустрічаються зі стійкістю України». Серед питань, які викликали інтерес учасників, європейський досвід у формуванні кліматичних контрактів та механізми забезпечення стійкості й адаптивного управління українських міст в умовах надзвичайних ситуацій.

Отже, ЄС активно використовує ресурсний потенціал стратегічних комунікацій для позиціонування екологічного порядку денного та залучення широкого кола стейкхолдерів до розв'язання екологічних викликів сьогодення. Активізація стратегічних комунікацій з європейськими партнерами розширює можливості здійснення зеленого переходу в умовах української політичної дійсності, сприяючи залученню ініціативи громадськості до імплементації передового досвіду упровадження інноваційних зелених технологій у різних сферах життєдіяльності.

4. Висновки

Реалізація публічних інтересів в екологічній сфері є одним із ключових факторів забезпечення трансгенераційної справедливості та сталого розвитку сучасних держав. Водночас адекватне реагування на екологічні виклики сьогодення потребує залучення ініціативи громадськості та ресурсного потенціалу широкого кола стейкхолдерів, формування відповідної нормативно-правової бази, а також упровадження інноваційних зелених технологій.

Зміст публічних інтересів ЄС в екологічній сфері конкретизовано в ЄЗК, що спрямований на підвищення рівня

конкурентоспроможності економіки через упровадження технологічних інновацій. Йдеться про досягнення кліматичної нейтральності до 2050 року, розвиток циркулярної економіки, підвищення рівня енергоефективності, збереження біорізноманіття. Ефективність реалізації вказаних ініціатив досягається балансом приватних і публічних інтересів в екологічній сфері. У цьому контексті важливим є залучення громадської ініціативи до обговорення ключових засад екологічної політики та інструментів її реалізації.

Інституції ЄС активно використовують стратегічні комунікації для формування екологічного порядку денного, активізації політичного діалогу та співпраці зі стейкхолдерами. По-перше, ресурсний потенціал публічної дипломатії сприяє активізації глобального політичного діалогу з питань клімату та ініціюванню різних форматів міжнародного зеленого партнерства. По-друге, застосування PR-інструментів забезпечує перехід від простого інформування до формування колективної відповідальності на основі балансу інтересів. Стратегічні комунікації роблять екологічний порядок денний основою нового суспільного договору, де усвідомлення індивідуальної вигоди нерозривно пов'язане з відповідальністю за трансгенераційну справедливість.

Екологічні наслідки російського повномасштабного вторгнення мають системний характер, впливаючи на кількісно-якісні показники розвитку людського капіталу та демографічну стійкість України. Відповідно, інноваційні зелені технології мають стати основою повоєнної відбудови та сталого економічного розвитку. Євроінтеграційний вектор України посилює ці завдання через необхідність виконання умов 4-го переговорного кластеру. Синхронізація законодавства у сфері кліматичної політики, посилення захисту біорізноманіття та сприяння декарбонізації — це не лише зобов'язання для вступу, але й розширення можливостей доступу до глобальних інноваційних ресурсів та фінансових інструментів для зеленої трансформації.

Стратегічні комунікації ЄС та України передбачають активізацію політичного діалогу з питань упровадження ключових принципів ЄЗК, залучення ініціативи українських владних інституцій та громадськості до реалізації екологічних проєктів, спрямованих на розширення можливостей зеленого переходу у контексті євроінтеграції та повоєнного відновлення. Участь у тематичних конференціях та партнерських програмах сприяє позиціюванню екологічних інтересів України та залученню ініціативи стейкхолдерів до післявоєнної зеленої відбудови.

Список використаних джерел:

1. Dewey J. The Public and Its Problems: An Essay in Political Inquiry. URL: https://ia802907.us.archive.org/3/items/in.ernet.dli.2015.190550/2015.190550.The-Public-And-Its-Problemms.pdf

2. Giddens A. The politics of climate change. National responses to the challenge of global warming. URL: https://fcampalans.cat/images/noticias/The_politics_of_climate_change_Anthony_Giddens%282%29.pdf

3. Pieraccini M. The Public Interest in Environmental Decision-Making: A Pragmatist Turn, *Journal of Environmental Law*, Volume 36, Issue 3, 2024, P. 363–383, https://doi.org/10.1093/jel/eqae026 URL: https://academic.oup.com/jel/article/36/3/363/7762140

4. Consolidated version of the treaty on the functioning of the European Union. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

5. Декларація про державний суверенітет України, від 16 липня 1990 р. № 55-XII / Верховна Рада УРСР. URL: https://zakon.rada.gov.ua/laws/show/55-12#Text

6. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/ 254%D0%BA/96-%D0%B2%D1%80#Text

7. Кримінальний кодекс України : Закон України від 05 квітня 2001 р. № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

8. Про основні засади державної кліматичної політики : Закон України від 08 жовтня 2024 р. № 3991-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3991-20#Text

9. The European Green Deal. Striving to be the first climate-neutral continent. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

10. Press remarks by President von der Leyen on the occasion of the adoption of the European Green Deal Communication. URL: https://ec.europa.eu/commission/presscorner/detail/fr/speech_19_6749

11. Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003L0004

12. Directive 2003/35/EC of the European Parliament and of the Council of 26 May 2003 providing for public participation in respect of the drawing up of certain plans and programmes relating to the environment and amending with regard to public participation and access to justice Council Directives 85/337/EEC and 96/61/EC — Statement by the Commission. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003L0035

13. The Aarhus Convention and the EU. URL: https://environment.ec.europa.eu/law-and-governance/aarhus_en

14. Про оцінку впливу на довкілля : Закон України від 23 травня 2017 р. № 2059-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2059-19#Text

15. Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021establishing the framework for achieving climate neutrality and amending Regulations (EC) № 401/2009 and (EU) 2018/1999 (European Climate Law). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1119

16. Fit for 55. URL: https://www.consilium.europa.eu/en/policies/fit-for-55/

17. Російська агресія вже спричинила екологічні руйнування в Україні більше 6 трлн гривень. URL: https://me.gov.ua/News/Detail/6fab61dd-28e9-4b18-8b22-ef06f10498a2?lang=uk-UA&title=EkologichniRuinuvanniaVUkraini

18. План впровадження Ukraine Facility (2024-2027). URL: https://www.ukrainefacility.me.gov.ua/en/home/

19. EU Climate Action Progress Report 2025. Strengthening competitiveness on the road to climate neutrality. Chapter 1. Climate action: advances and challenges. URL: https://climate.ec.europa.eu/eu-action/climate-strategies-targets/progress-climate-action/eu-climate-action-progress-report-2025/chapter-1-climate-action-advances-and-challenges_en

20. EU Climate Action Progress Report 2025. Strengthening competitiveness on the road to climate neutrality. Quote & Foreword. URL: https://climate.ec.europa.eu/eu-action/climate-strategies-targets/progress-climate-action/eu-climate-action-progress-report-2025/quote-foreword_en

21. 2025 State of the Union Address by President von der Leyen. URL: https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053

22. Hallahan K., Holtzhausen D., Ruler B., Verčič D., Sriramesh K. Defining Strategic Communication. *International Journal of Strategic Communication*. № 1. 2007. P. 3–35. URL: https://www.researchgate.net/publication/241730557_Defining_Strategic_Communication

23. Cornish P., Lindley-French J., Yorke C. Strategic Communications and National Strategy. Chatham House Report. September 2011. P. 4. URL: https://www.chathamhouse.org/sites/default/files/r0911stratcomms.pdf

24. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf

25. Leonard M. Public diplomacy. London : The Foreign Policy Centre, 2002. 183 c.

26. Хорішко Л. С. Стратегічні комунікації в політиці: підходи до розуміння та основні види / Стратегічні комунікації суб'єктів політики в умовах сучасної політичної дійсності : колективна монографія / за заг. ред. Л. С. Хорішко. Запоріжжя : Видавничий дім «Гельветика», 2021. С. 111–133.

27. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions EU global climate and energy vision: securing Europe's competitive role in world markets and accelerating the clean transition. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0025

28. EU4ClimateResilience. Decarbonization, and climate resilience in the Eastern Partnership. URL: https://eu4climate.eu/about-us

29. Strengthening the capacity of regional and local administrations for implementation and enforcement of EU environmental and climate change legislation and development of infrastructure projects. URL: https://euneighbourseast.eu/uk/projects/eu-project-page/?id=1302

30. Covenant of Mayors. URL: https://ukrainian-climate-office.org/en/project/covenant-of-mayors/

31. EU Mission: Climate-Neutral and Smart Cities. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/climate-neutral-and-smart-cities_en

32. Climate ambition continues to grow across Europe: Dortmund, Sarajevo and Elbasan awarded the EU Mission Label. URL: https://netzerocities.eu/2026/02/16/climate-ambition-continues-to-grow-across-europe-elbasan-dortmund-and-sarajevo-awarded-the-eu-mission-label/

33. SUN4Ukraine. Контекст. URL: https://www.sun4ukraine.eu/uk/context

34. LIFE Programme EU's funding instrument for the environment and climate action. URL: https://cinea.ec.europa.eu/programmes/life_en#about

35. Partnership Initiative for the Green Reconstruction of Ukraine. URL: https://www.d2r.com.ua/about#about-cities

36. New European Bauhaus. URL: https://new-european-bauhaus.europa.eu/index_en

37. Львів став переможцем конкурсу New European Bauhaus Prize 2024. URL: https://city-adm.lviv.ua/news/architecture-and-historic-heritage/lviv-stav-peremozhtsem-konkursu-new-european-bauhaus-prize-2024/

38. Chapter 8. International climate action. URL: https://climate.ec.europa.eu/eu-action/climate-strategies-targets/progress-climate-action/eu-climate-action-progress-report-2025/chapter-8-international-climate-action_en

39. Результати України на COP30: коротко про головне. URL: https://cop.ukrainian-climate-office.org/uk/rezultaty-ukrayiny-na-sor30-korotko-pro-holovne/

40. Cities Mission Conference 2025. URL: https://www.sun4ukraine.eu/uk/news-Cities-Mission-Conference-2025

41. SUN4Ukraine Launches its Partnership Programme in Munich: Ukrainian and European Cities Chart Their Joint Path to Climate Neutrality. URL: https://www.sun4ukraine.eu/uk/news-SUN4Ukraine-Launches-its-Partnership-Programme-in-Munich

References:

1. Dewey, J. (1946). The Public and Its Problems: An Essay in Political Inquiry. Retrieved from https://ia802907.us.archive.org/3/items/in.ernet.dli.2015.190550/2015.190550.The-Public-And-Its-Problemms.pdf

2. Giddens, A. (2008). The politics of climate change. National responses to the challenge of global warming. Retrieved from https://fcampalans.cat/images/noticias/The_politics_of_climate_change_Anthony_Giddens%282%29.pdf

3. Pieraccini, M. (2024). The Public Interest in Environmental Decision-Making: A Pragmatist Turn, *Journal of Environmental Law*, 36 (3), 363-383, https://doi.org/10.1093/jel/eqae026

4. Consolidated version of the treaty on the functioning of the European Union. (2012). Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

5. Verkhovna Rada of the Ukrainian SSR. (1990). Deklaratsiia pro Derzhavnyi suverenitet Ukrainy, № 55-XII [Declaration of State Sovereignty of Ukraine, 55-XII]. Retrieved from https://zakon.rada.gov.ua/laws/show/55-12#Text

6. Verkhovna Rada Ukrainy. (1996). Zakon Ukrainy: Konstytutsiia Ukrainy, № 254к/96-ВР [Law of Ukraine: Constitution of Ukraine, № 254к/96-ВР]. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

7. Verkhovna Rada Ukrainy. (2001). Zakon Ukrainy: Kryminalnyi kodeks Ukrainy, № 2341-III [Law of Ukraine: Criminal Code of Ukraine, № 2341-III]. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text

8. Verkhovna Rada Ukrainy. (2024) Zakon Ukrainy: Pro osnovni zasady derzhavnoi klimatychnoi polityky, № 3991-IX [Law of Ukraine: On the basic principles of state climate policy, № 3991-IX]. Retrieved from https://zakon.rada.gov.ua/laws/show/3991-20#Text

9. European Commission. (2019). The European Green Deal. Striving to be the first climate-neutral continent. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

10. European Commission (2020). Press remarks by President von der Leyen on the occasion of the adoption of the European Green Deal Communication. Retrieved from https://ec.europa.eu/commission/presscorner/detail/fr/speech_19_6749

11. European Parliament and European Council. (2003). Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003L0004

12. European Parliament and European Council. (2003). Directive 2003/35/EC of the European Parliament and of the Council of 26 May 2003 providing for public participation in respect of the drawing up of certain plans and programmes relating to the environment and amending with regard to public participation and access to justice Council Directives 85/337/EEC and 96/61/EC — Statement by the Commission. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003L0035

13. European Commission. The Aarhus Convention and the EU. Retrieved from https://environment.ec.europa.eu/law-and-governance/aarhus_en

14. Verkhovna Rada Ukrainy. (2017). Zakon Ukrainy: Pro otsinku vplyvu na dovkillia, № 2059-VIII [Law of Ukraine: On Environmental Impact Assessment]. Retrieved from https://zakon.rada.gov.ua/laws/show/2059-19#Text

15. European Parliament and European Council. (2021). Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 (European Climate Law). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1119

16. European Council. (2021). Fit for 55. Retrieved from https://www.consilium.europa.eu/en/policies/fit-for-55/

17. Ministerstvo ekonomiky, dovkillia ta silskoho hospodarstva Ukrainy. (2025). Rosiiska ahresiia vzhe sprychynyla ekolohichni ruinuvannia v Ukraini bilshe 6 trln hryven. [Russian aggression has already caused more than 6 trillion hryvnias in environmental destruction in Ukraine]. Retrieved from https://me.gov.ua/News/Detail/6fab61dd-28e9-4b18-8b22-ef06f10498a2?lang=uk-UA&title=EkologichniRuinuvaniaVUkraini

18. Kabinet Ministriv Ukrainy. (2024). Plan vprovadzhennia Ukraine Facility (2024-2027) [Implementation plan Ukraine Facility

(2024–2027)]. Retrieved from https://www.ukrainefacility.me.gov.ua/en/home/

19. EU Climate Action Progress Report 2025. Strengthening competitiveness on the road to climate neutrality. Chapter 1. Climate action: advances and challenges. Retrieved from https://climate.ec.europa.eu/eu-action/climate-strategies-targets/progress-climate-action/eu-climate-action-progress-report-2025/chapter-1-climate-action-advances-and-challenges_en

20. European Commission. (2025). EU Climate Action Progress Report 2025. Strengthening competitiveness on the road to climate neutrality. Quote & Foreword. Retrieved from https://climate.ec.europa.eu/eu-action/climate-strategies-targets/progress-climate-action/eu-climate-action-progress-report-2025/quote-foreword_en

21. European Commission. (2025). 2025 State of the Union Address by President von der Leyen. Retrieved from https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053

22. Hallahan, K., Holtzhausen, D., Ruler, B., Verčič, D., Sriramesh, K. (2007). Defining Strategic Communication. *International Journal of Strategic Communication*. 1. 3–35. Retrieved from https://www.researchgate.net/publication/241730557_Defining_Strategic_Communication

23. Cornish P., Lindley-French J., Yorke C. (2011). Strategic Communications and National Strategy. Chatham House Report. Retrieved from https://www.chathamhouse.org/sites/default/files/r0911stratcomms.pdf

24. European Parliament. (2016). European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties. Retrieved from https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf

25. Leonard M. (2002). Public diplomacy. London: The Foreign Policy Centre.

26. Khorishko, L. S. (2021). Stratehichni komunikatsii v politytsi: pidkhody do rozuminnia ta osnovni vydy [Strategic communications in politics: approaches to understanding and main types]. In L. S. Khorishko (Ed.), Stratehichni komunikatsii subiektiv polityky v umovakh suchasnoi politychnoi diisnosti: kolektyvna monohrafiia (pp. 111–133). Zaporizhzhia: Publishing House "Helvetyka".

27. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions EU global climate and energy vision: securing Europe's competitive role in world markets and accelerating the clean transition. (2025). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0025

28. EU4ClimateResilience. (2023). Decarbonization, and climate resilience in the Eastern Partnership. Retrieved from https://eu4climate.eu/about-us

29. EU NeighboursEast. (2020). Strengthening the capacity of regional and local administrations for implementation and enforcement of EU environmental and climate change legislation and development of infrastructure projects. Retrieved from https://euneighbourseast.eu/uk/projects/eu-project-page/?id=1302

30. Ukrainian Climate Office. (2021). Covenant of Mayors. Retrieved from https://ukrainian-climate-office.org/en/project/covenant-of-mayors/

31. European Commission. (2024). EU Mission: Climate-Neutral and Smart Cities. Retrieved from https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/climate-neutral-and-smart-cities_en

32. Net Zero Cities. (2026). Climate ambition continues to grow across Europe: Dortmund, Sarajevo and Elbasan awarded the EU Mission Label. Retrieved from https://netzerocities.eu/2026/02/16/climate-ambition-continues-to-grow-across-europe-elbasan-dortmund-and-sarajevo-awarded-the-eu-mission-label/

33. SUN4Ukraine. (2024) Kontekst. [Context]. Retrieved from https://www.sun4ukraine.eu/uk/context

34. European Commission. (2021). LIFE Programme EU's funding instrument for the environment and climate action. Retrieved from https://cinea.ec.europa.eu/programmes/life_en#about

35. D2R — Debris to Resource. (2025). Partnerska initsiatyva dlia zelenoi vidbudovy Ukrainy. [Partnership Initiative for the Green Reconstruction of Ukraine]. Retrieved from https://www.d2r.com.ua/about#about-cities

36. European Union. (2020). New European Bauhaus. Retrieved from https://new-european-bauhaus.europa.eu/index_en

37. Lvivska miska rada. (2024). Lviv stav peremozhtsem konkursu New European Bauhaus Prize 2024. [Lviv became the winner of the competition New European Bauhaus Prize 2024]. Retrieved from https://city-adm.lviv.ua/news/architecture-and-historic-heritage/lviv-stav-peremozhtsem-konkursu-new-european-bauhaus-prize-2024/

38. European Commission. (2024). Chapter 8. International climate action. Retrieved from https://climate.ec.europa.eu/eu-action/climate-strategies-targets/progress-climate-action/eu-climate-action-progress-report-2025/chapter-8-international-climate-action_en

39. Ukrainian Climate Office. (2025). Rezultaty Ukrainy na COP30: korotko pro holovne. [Ukraine's results at COP30: a brief summary]. Retrieved from https://cop.ukrainian-climate-office.org/uk/rezultaty-ukrayiny-na-sor30-korotko-pro-holovne/

40. SUN4Ukraine.Cities. (2025). Mission Conference 2025. Retrieved from https://www.sun4ukraine.eu/uk/news-Cities-Mission-Conference-2025

41. SUN4Ukraine (2025). Launches its Partnership Programme in Munich: Ukrainian and European Cities Chart Their Joint Path to Climate Neutrality. Retrieved from https://www.sun4ukraine.eu/uk/news-SUN4Ukraine-Launches-its-Partnership-Programme-in-Munich

СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ВИМІРІ ПУБЛІЧНОГО ІНТЕРЕСУ: ПРАВОВА КОНВЕРГЕНЦІЯ УКРАЇНИ ТА ЄВРОПЕЙСЬКОГО СОЮЗУ ЗА ДИРЕКТИВОЮ (ЄС) 2022/2557 (CER)

CRITICAL INFRASTRUCTURE RESILIENCE IN THE DIMENSION OF PUBLIC INTEREST: LEGAL CONVERGENCE OF UKRAINE AND THE EUROPEAN UNION UNDER DIRECTIVE (EU) 2022/2557 (CER)

Chernyavska B. V.,
Candidate of Law, Associate Professor,
Department of Theory and History of State and Law,
National Academy of Management,
Kyiv, Ukraine
Visiting Researcher, Faculty of Law,
Vrije Universiteit Amsterdam, Netherlands,
Visiting Researcher, Blavatnik School of Government,
University of Oxford,
Oxford, United Kingdom,

Hubacheva D. V.,
Candidate of Legal Sciences,
Member of the Non-Governmental Organization
"Center for Security, Legal, and Political Studies",
Odesa, Ukraine

Abstract. The resilience of critical infrastructure in the twenty-first century has become a fundamental element in safeguarding public interests, national security, and sustainable state development. In the context of armed aggression against Ukraine, as well as hybrid threats, cyberattacks, energy coercion, and technological risks, the establishment of a comprehensive legal framework for the protection and resilience of critical infrastructure has become particularly urgent.

This study emphasizes the need to align Ukrainian legislation with European Union standards, particularly through the implementation of Directive (EU) 2022/2557 [1] on the resilience of critical entities (CER), which introduces a modern model of risk management, cross-sectoral coordination, and shared responsibility between the state and operators of essential services. It also takes into account the interaction between Directive (EU) 2022/2557 [1] and Directive (EU) 2022/2555 (NIS2) [2], ensuring a comprehensive approach to both the physical and cyber resilience of critical infrastructure.

Particular attention is paid to the functioning of the legal framework for critical infrastructure resilience under martial law in Ukraine. This legal regime was introduced pursuant to the Decree of the President of Ukraine No. 64/2022 of 24 February 2022, approved by the Law of Ukraine No. 2102-IX [3], which establishes a special framework for public administration and the protection of critical infrastructure under conditions of armed aggression.

The study further considers the implications of Ukraine's status as a candidate country for European Union membership, which requires not only the formal transposition of EU legal acts but also substantive institutional and administrative convergence. In this context, resilience is conceptualized as a cross-border and transnational legal phenomenon, reflecting the growing interdependence of critical services within the European security and economic space.

The subject of the study comprises the legal norms of Ukrainian national legislation and European Union law governing the resilience of critical entities, as well as the mechanisms of public administration, supervision, and liability in this field. It also encompasses the processes of legal harmonization and convergence between Ukraine and the EU in the sphere of critical infrastructure resilience.

The purpose of the study is to conduct a comprehensive analysis of the legal foundations for ensuring the resilience of Ukraine's critical infrastructure within the framework of public interest and to substantiate the directions of legal convergence with the European Union in accordance with Directive (EU) 2022/2557 [1], taking into account the current Ukrainian legislation as of 2026.

The methodological basis of the research combines general scientific and special legal methods. The dialectical method was applied to examine the transformation of approaches from a static "protection" model to a dynamic concept of resilience. A systemic approach enabled the consideration of critical infrastructure resilience as an integral component of national security, public governance, human rights protection, and economic stability. The formal-legal method was used to analyze the provisions of Ukrainian legislation and the CER Directive. The comparative legal method facilitated the identification of similarities and differences between Ukrainian and EU regulatory models and determined directions for legal convergence. The interpretative method was employed to clarify legislative provisions in light of the rule of law and public interest principles. The prognostic method was used to formulate recommendations for further legislative development in accordance with Ukraine's European integration commitments.

The conclusion substantiates that the resilience of critical infrastructure should be understood not merely as a technical or security category but as a legal guarantee of the continuity of essential

services, protection of constitutional rights and freedoms, and functioning of democratic institutions. The conceptual contribution of the research lies in framing resilience as a normative category that shapes the scope of state responsibility in times of multidimensional crises. This approach expands the doctrinal understanding of critical infrastructure protection by integrating constitutional guarantees, administrative coordination, and European legal standards into a unified legal model. The proposed framework is particularly relevant for Ukraine's post-war recovery and long-term institutional modernization. It argues that resilience constitutes an independent principle of public governance, defining the scope of the state's positive obligations under conditions of military and hybrid threats. The research demonstrates the need for further harmonization of Ukrainian legislation with EU standards, particularly regarding risk assessment procedures, intersectoral coordination, state supervision, operator responsibility, and international cooperation. A conceptual model for the legal convergence of Ukraine with the European Union in the field of critical infrastructure resilience is proposed, contributing to the development of a modern legal framework aligned with European standards and capable of ensuring the stability of the state and society amid multidimensional threats.

Keywords: critical infrastructure resilience; public interest; legal convergence; Directive (EU) 2022/2557; national security; Ukraine; European Union.

1. Вступ

Стійкість критичної інфраструктури у XXI столітті перетворюється на один із ключових елементів забезпечення публічного інтересу, національної безпеки та сталого розвитку держави. Умови збройної агресії проти України, гібридні загрози, кібератаки, енергетичний шантаж і техногенні ризики актуалізували необхідність

формування комплексної системи правового регулювання захисту об'єктів критичної інфраструктури. При цьому правове регулювання забезпечення стійкості критичної інфраструктури функціонує в умовах правового режиму воєнного стану, що суттєво впливає на порядок оцінки ризиків, здійснення державного нагляду та організацію кризової координації.

В умовах воєнного стану відбувається суттєва трансформація механізмів публічного управління у сфері критичної інфраструктури, що проявляється у концентрації повноважень органів виконавчої влади, спрощенні процедур прийняття управлінських рішень та посиленні ролі безпекових інституцій. Водночас така трансформація не повинна призводити до нівелювання принципів верховенства права, пропорційності та правової визначеності. Забезпечення стійкості критичної інфраструктури в умовах воєнного стану потребує збереження балансу між імперативами національної безпеки та гарантіями прав і свобод людини. Це відповідає положенням статей 3, 8 та 64 Конституції України [4], які визначають пріоритет прав і свобод людини та межі їх можливого обмеження в умовах воєнного стану.

Особливої ваги набуває інтеграція українського законодавства до стандартів Європейського Союзу, зокрема в контексті імплементації Directive (EU) 2022/2557 про стійкість критичних суб'єктів (CER) [1], що встановлює сучасну модель управління ризиками, міжсекторної координації та відповідальності держави й операторів критичних послуг. Водночас слід враховувати взаємозв'язок цієї Директиви з Directive (EU) 2022/2555 (NIS2) [2], що регулює кібербезпеку мереж та інформаційних систем і формує комплексний підхід до стійкості критичних суб'єктів.

Правове забезпечення стійкості критичної інфраструктури в Україні здійснюється на основі положень Закону України «Про критичну інфраструктуру» [5], законодавства у сфері національної

безпеки, цивільного захисту, кібербезпеки, енергетики, транспорту та зв'язку, а також Закону України «Про основні засади забезпечення кібербезпеки України» [6] та Кодексу цивільного захисту України [7]. Енергетичний сектор при цьому залишається найбільш уразливим складником критичної інфраструктури, що потребує впровадження посиленого планування стійкості з урахуванням європейських стандартів управління ризиками. Забезпечення їх стійкості безпосередньо пов'язане з реалізацією права на життя, безпеку, доступ до медичних послуг, водопостачання, електроенергії та інших базових благ.

По-друге, у Європейському Союзі відбулася концептуальна еволюція підходів до захисту критичної інфраструктури — від моделі «захисту» до моделі «стійкості», що передбачає превентивність, управління ризиками, багаторівневу взаємодію та відповідальність як державних органів, так і приватних операторів. Прийняття Directive (EU) 2022/2557 [1] стало відображенням цієї трансформації, заклавши нові вимоги щодо оцінки ризиків, ідентифікації критичних суб'єктів, планування безперервності діяльності та державного нагляду. Особливого значення набувають положення щодо транскордонних критичних суб'єктів та механізмів координації на рівні Європейського Союзу, що мають стратегічне значення для України в умовах євроінтеграційних трансформацій.

По-третє, імплементація європейських стандартів у національну правову систему України потребує гармонізації термінології, процедур і механізмів координації між суб'єктами забезпечення критичної інфраструктури. Чинний Закон України «Про критичну інфраструктуру» [5] закладає базові принципи функціонування національної системи, однак потребує подальшого розвитку з урахуванням положень CER, зокрема щодо міжсекторного взаємодії, контролю, обміну інформацією та міжнародного співробітництва, а також запровадження механізмів обміну інформацією про інциденти відповідно до вимог законодавства ЄС.

По-четверте, у контексті євроінтеграційного курсу України стійкість критичної інфраструктури стає елементом виконання зобов'язань у сфері безпеки та правової державності. Це також пов'язано з виконанням зобов'язань у межах Угоди про асоціацію між Україною та Європейським Союзом [8].

По-п'яте, формування довгострокової моделі стійкості критичної інфраструктури має стратегічне значення для післявоєнного відновлення України та забезпечення її економічної стабільності. Відбудова зруйнованих об'єктів повинна супроводжуватися впровадженням сучасних стандартів управління ризиками, цифрової трансформації та інтеграції до європейських інфраструктурних мереж, що підвищує рівень адаптивності держави до майбутніх криз.

Наукова новизна дослідження полягає у комплексному теоретико-правовому осмисленні стійкості критичної інфраструктури як форми реалізації публічного інтересу та елементу конституційного обов'язку держави гарантувати безпеку і безперервність життєво важливих послуг. У роботі обґрунтовується підхід до стійкості критичної інфраструктури як міжгалузевої правової категорії, що інтегрує норми конституційного, адміністративного, безпекового та європейського права, а також розкривається зміст правової конвергенції України та ЄС у сфері забезпечення стійкості критичних суб'єктів через призму імплементації Directive (EU) 2022/2557 [1]. Запропоновано концептуальну модель гармонізації національного законодавства з урахуванням положень Закону України «Про критичну інфраструктуру» [5] та суміжних нормативно-правових актів. Уперше на національному рівні обґрунтовано необхідність розгляду стійкості критичної інфраструктури як окремого принципу публічного управління, що визначає зміст позитивних зобов'язань держави відповідно до практики Європейського суду з прав людини щодо позитивних зобов'язань держави у сфері захисту життя та безпеки в умовах воєнних та гібридних загроз. Визначено

співвідношення публічного інтересу, національної безпеки та прав людини у системі забезпечення стійкості критичної інфраструктури, сформульовано пропозиції щодо вдосконалення механізмів державного нагляду, відповідальності операторів критичних послуг та міжвідомчої координації відповідно до стандартів ЄС.

Таким чином, дослідження формує новий теоретичний підхід до розуміння стійкості як юридичної гарантії функціонування держави та суспільства в умовах багатовимірних загроз.

Метою дослідження є комплексний аналіз правових засад забезпечення стійкості критичної інфраструктури України у вимірі публічного інтересу та обґрунтування напрямів правової конвергенції з Європейським Союзом відповідно до положень Directive (EU) 2022/2557 [1] з урахуванням чинного законодавства України станом на 2026 рік, а також з урахуванням правозастосовної практики.

Об'єктом дослідження є суспільні відносини у сфері забезпечення стійкості критичної інфраструктури України як складник національної безпеки та публічного інтересу в умовах євроінтеграційних трансформацій.

Предметом дослідження є норми національного законодавства України та права Європейського Союзу, що регулюють питання стійкості критичних суб'єктів, механізми державного управління, контролю та відповідальності у цій сфері, а також правові засади їх гармонізації відповідно до стандартів Європейського Союзу, включаючи підзаконні нормативно-правові акти та практику їх застосування.

Для досягнення поставленої мети визначено такі **завдання**:

— розкрити теоретико-правову природу поняття «стійкість критичної інфраструктури» та її співвідношення з категоріями «публічний інтерес», «національна безпека», «безперервність надання послуг»;

— проаналізувати еволюцію підходів Європейського Союзу, включаючи взаємодію Directive (EU) 2022/2557 [1] та Directive (EU) 2022/2555 (NIS2) [2];

— дослідити чинне законодавство України у сфері критичної інфраструктури, насамперед Закон України «Про критичну інфраструктуру» [5], та визначити ступінь його відповідності стандартам ЄС;

— визначити інституційні та процедурні механізми забезпечення стійкості критичних суб'єктів в Україні;

— сформулювати пропозиції щодо вдосконалення нормативно-правової бази України з метою забезпечення ефективної імплементації положень CER;

— окреслити роль державного контролю, відповідальності операторів і міжнародної співпраці у забезпеченні публічного інтересу.

Методологічну основу дослідження становить поєднання загальнонаукових та спеціально-юридичних методів. Діалектичний метод застосовано для аналізу трансформації підходів до захисту критичної інфраструктури — від статичної моделі безпеки до динамічної концепції стійкості. Системний підхід дозволив розглянути стійкість критичної інфраструктури як елемент єдиної системи національної безпеки та публічного управління, що функціонує у взаємозв'язку з правами людини та економічною стабільністю. Формально-юридичний метод використано для аналізу положень Закону України «Про критичну інфраструктуру» [5], підзаконних нормативно-правових актів та положень Directive (EU) 2022/2557 [1]. Доктринальний метод застосовано для систематизації наукових підходів до розуміння стійкості критичної інфраструктури як правової категорії, а функціональний аналіз — для оцінки ефективності чинних механізмів правового регулювання, а також елементів risk-based approach, що застосовується у праві Європейського Союзу. Порівняльно-правовий метод дав змогу зіставити національну модель регулювання з правом ЄС та визначити напрями

правової конвергенції. Інтерпретаційний метод застосовано для тлумачення норм законодавства та визначення їх змісту у світлі принципу верховенства права та публічного інтересу. Прогностичний метод використано для формування рекомендацій щодо подальшого розвитку законодавства України у сфері стійкості критичної інфраструктури з урахуванням євроінтеграційних зобов'язань. Дослідження має міждисциплінарний характер, поєднуючи підходи публічного права, безпекових студій та європейської інтеграції, що дозволяє комплексно оцінити феномен стійкості критичної інфраструктури як багатовимірну правову категорію.

Практичне значення одержаних результатів полягає у можливості використання сформульованих у монографії висновків і рекомендацій:

— у нормотворчій діяльності Верховної Ради України при вдосконаленні положень законодавства у сфері критичної інфраструктури;

— у діяльності органів виконавчої влади під час розроблення підзаконних нормативно-правових актів та програм забезпечення стійкості критичних суб'єктів;

— у процесі імплементації положень Directive (EU) 2022/2557 [1] у національну правову систему України;

— у наукових дослідженнях проблем публічного інтересу, національної безпеки та європейської інтеграції;

— у навчальному процесі підготовки здобувачів вищої освіти за спеціальністю «Право» та «Публічне управління та адміністрування».

Логіка викладу матеріалу зумовлена метою та завданнями дослідження. У першому розділі розкриваються теоретико-правові засади стійкості критичної інфраструктури у вимірі публічного інтересу. У другому розділі аналізуються положення Directive (EU) 2022/2557 [1] та стан їх імплементації в Україні. У третьому розділі

досліджуються напрями вдосконалення національного законодавства та механізми забезпечення правової конвергенції з Європейським Союзом.

Така структура забезпечує послідовний перехід від теоретичного осмислення проблеми до вироблення практичних рекомендацій щодо вдосконалення правового регулювання у сфері стійкості критичної інфраструктури України. Таким чином, дослідження безпосередньо розкриває секторну специфіку публічних інтересів у сфері критичної інфраструктури як складника національної безпеки.

2. Теоретико-правові засади функціонування критичної інфраструктури

Поняття критичної інфраструктури у сучасному праві визначається як сукупність об'єктів, систем та мереж, функціонування яких має вирішальне значення для забезпечення життєдіяльності населення, національної безпеки, економічної стабільності та функціонування державної влади. У національному правопорядку нормативне закріплення цього поняття здійснено у Законі України «Про критичну інфраструктуру» [5], який запроваджує інституційну модель системи захисту критичної інфраструктури, що включає суб'єктів управління, операторів та механізми державного нагляду. Визначення узгоджується з підходом Directive (EU) 2022/2557 [1], де критичні суб'єкти розглядаються крізь призму надання життєво необхідних послуг, а не лише існування інфраструктурних об'єктів.

Правова природа критичної інфраструктури має комплексний характер. Вона поєднує:

— публічно-правовий компонент (регулювання з боку держави, спеціальний режим безпеки);

— приватноправовий компонент (участь суб'єктів господарювання як операторів);

— безпековий (security and resilience) компонент (інтеграція до системи національної безпеки);

— євроінтеграційний компонент (гармонізація із правом ЄС).

На відміну від традиційного підходу до об'єктів підвищеної небезпеки, критична інфраструктура характеризується не лише технічними параметрами, а функціональною значущістю для суспільства. Її правовий режим передбачає спеціальні вимоги до управління ризиками, категоризації, забезпечення безперервності сервісів та державного нагляду, що корелює з переходом у праві ЄС від об'єктно-орієнтованої до сервісно-орієнтованої моделі регулювання.

Таким чином, критична інфраструктура є особливим об'єктом публічно-правового регулювання, який функціонує на перетині публічного інтересу та приватної господарської діяльності.

У теоретико-правовому вимірі критична інфраструктура може розглядатися як різновид об'єктів із підвищеним ступенем соціальної значущості, щодо яких держава реалізує спеціальну регуляторну функцію. Її правовий режим формується через поєднання імперативного регулювання, спеціального адміністративного контролю та елементів договірної автономії операторів. Такий комплексний характер зумовлює необхідність застосування міжгалузевого підходу до визначення її правового статусу.

У дослідженні застосовано системний, функціональний та порівняльно-правовий підходи. Застосування зазначених методологічних підходів дозволяє розкрити зміст стійкості критичної інфраструктури як комплексної правової категорії.

Стійкість критичної інфраструктури в сучасному праві формується як міжгалузева категорія, що поєднує елементи конституційного, адміністративного, безпекового та європейського права. Її зміст безпосередньо пов'язаний із забезпеченням публічного інтересу, гарантуванням фундаментальних прав і свобод людини, а також ефективністю функціонування державних та приватних систем відповідно

до принципу належного врядування (good governance), що забезпечують життєдіяльність суспільства [9]. У цьому вимірі стійкість виступає не лише техніко-організаційною характеристикою інфраструктурних об'єктів, а нормативно визначеним обов'язком держави формувати правові механізми запобігання ризикам, мінімізації наслідків криз та забезпечення безперервності основних сервісів.

Права людини, як фундаментальна правова категорія, визначаються світовим співтовариством як блага й умови життя, на які може розраховувати особа від держави та суспільства, у яких вона проживає, і забезпечення яких є реальним у межах досягнутого прогресу людства [10]. Ідея прав людини, пройшовши крізь століття страждань, конфліктів і масового насильства, становить основу сучасного світового правопорядку, водночас залишаючись ключовим викликом для сучасного суспільства. У контексті критичної інфраструктури права людини набувають прикладного виміру: без належного функціонування енергетики, систем охорони здоров'я, транспорту чи зв'язку реалізація навіть класичних громадянських і соціальних прав стає неможливою, що підтверджується практикою Європейський суд з прав людини, зокрема у рішеннях у справах Öneryıldız v. Turkey (2004) [11], Budayeva and Others v. Russia (2008) [12], у яких сформульовано підхід до позитивних зобов'язань держави щодо запобігання ризикам для життя та здоров'я людини.

Права людини, разом із принципами демократії та верховенства права, утворюють фундаментальні цінності європейського правового простору [13]. Як зазначає Ю. Шемшученко, права людини є історично мінливою категорією, що еволюціонує разом із розвитком держави та суспільства [14, с. 5]. У цифрову епоху ці права набувають нових змістових характеристик, адже сучасні технології створюють як нові можливості реалізації прав, так і додаткові ризики їх обмеження. Саме тому питання стійкості критичної інфраструктури перебуває у центрі наукових дискусій як

у площині загальної теорії права, так і в межах галузевих юридичних наук [15, с. 42]. Воно інтегрує концепції позитивних зобов'язань держави щодо захисту прав людини, принцип належного урядування та стандарти належної обачності (due diligence) у сфері безпеки. У контексті функціонування критичної інфраструктури позитивні зобов'язання держави означають обов'язок створити ефективну нормативну, інституційну та організаційну систему запобігання загрозам, що можуть поставити під ризик життя, здоров'я та безпеку населення.

У цьому контексті стійкість критичної інфраструктури слід розглядати не лише як безпековий інструмент, а як правову гарантію реалізації конституційних прав — передусім права на життя (ст. 27), безпеку (ст. 3), охорону здоров'я (ст. 49) та достатній життєвий рівень (ст. 48), гарантованих Конституцією України [4]. Безперервність функціонування енергетики, транспорту, систем водопостачання, охорони здоров'я та цифрових мереж створює матеріальну основу здійснення прав і свобод. Таким чином, стійкість набуває значення інструменту реалізації позитивних обов'язків держави щодо забезпечення умов гідного існування людини.

Публічний інтерес у сфері критичної інфраструктури у доктринальному вимірі розглядається як юридично значуща категорія, що легітимує встановлення спеціального правового режиму щодо об'єктів підвищеної соціальної значущості. Йдеться не про абстрактний суспільний інтерес, а про інституціоналізовану форму вираження потреб безпеки, стабільності та безперервності життєво необхідних сервісів. Саме публічний інтерес виступає підставою для імперативного регулювання, запровадження спеціального нагляду та встановлення підвищених обов'язків для операторів критичної інфраструктури.

Концептуальна трансформація підходів до регулювання критичної інфраструктури на рівні Європейського Союзу відбулася

з прийняттям Directive (EU) 2022/2557 (CER) [1], яка закріпила перехід від моделі «захисту об'єктів» до моделі «стійкості сервісів». Філософія Директиви CER полягає у зміщенні акценту з фізичної охорони периметра та інженерного захисту окремих об'єктів на забезпечення безперервності надання основних послуг як суспільного блага [16]. Якщо попередня Directive 2008/114/ЕС [17] зосереджувалася переважно на ідентифікації та захисті європейської критичної інфраструктури від терористичних загроз, то нова модель передбачає комплексне управління всіма видами ризиків — природними, техногенними, гібридними, кібернетичними та воєнними [16].

Європейська модель регулювання критичної інфраструктури ґрунтується на поєднанні двох ключових нормативних актів — Directive (EU) 2022/2557 (CER) [1] та Directive (EU) 2022/2555 (NIS2) [2]. Їх комплексне застосування формує нову парадигму забезпечення стійкості, засновану на системному управлінні ризиками та відповідальності критичних суб'єктів. Особливого значення набувають транскордонні критичні суб'єкти та механізми координації на рівні ЄС, що є стратегічно важливими для України в контексті інтеграції до європейського енергетичного та цифрового простору.

Для України транскордонний вимір стійкості набуває особливого значення у зв'язку з інтеграцією до енергетичної системи ENTSO-E, розвитком транспортних коридорів та цифрових мереж, що функціонують у межах європейського ринку. Це зумовлює необхідність гармонізації процедур оцінки ризиків та кризового реагування із загальноєвропейськими механізмами координації.

Директива CER встановлює обов'язок держав-членів здійснювати національні оцінки ризиків, визначати критичні суб'єкти, встановлювати для них обов'язки щодо впровадження заходів управління ризиками, забезпечення безперервності діяльності та проходження

зовнішніх перевірок [1]. Натомість NIS2 деталізує вимоги до кіберстійкості, зокрема щодо управління кіберризиками, звітності про інциденти та персональної відповідальності керівництва суб'єктів [2].

Імплементація цих стандартів в українське законодавство передбачає: 1) перехід до ризикоорієнтованої моделі регулювання; 2) нормативне закріплення обов'язкових планів безперервності; 3) створення механізмів зовнішнього аудиту; 4) посилення санкційної відповідальності операторів.

Таким чином, інтеграція CER та NIS2 формує комплексну модель фізичної та кіберстійкості, що відповідає сучасним європейським підходам до захисту критичних сервісів.

Правове регулювання у сфері критичної інфраструктури ґрунтується на системі спеціальних принципів, серед яких ключове значення мають: принцип безперервності надання життєво необхідних послуг; принцип превентивності та ризикоорієнтованості; принцип координації між суб'єктами сектору безпеки; принцип державно-приватного партнерства; принцип пропорційності втручання у сферу господарської діяльності. Саме ці принципи формують нормативну архітектуру сучасної моделі стійкості.

Важливим є підхід CER до системного управління ризиками: держави-члени зобов'язані здійснювати регулярну національну оцінку ризиків, визначати критичні суб'єкти, встановлювати для них обов'язки щодо впровадження заходів управління ризиками, розроблення планів безперервності діяльності, кризових протоколів та механізмів внутрішнього контролю [1]. Отже, охорона периметра трансформується у концепцію організаційної, функціональної та операційної стійкості, де ключовим є не збереження об'єкта як такого, а здатність сервісу продовжувати функціонування або швидко відновлюватися.

Таким чином, парадигма зміщується з реактивного захисту на превентивне управління ризиками, системну готовність

до надзвичайних ситуацій та підвищення адаптивності систем. У національному праві основи формування такої системи закладено у Закон України «Про критичну інфраструктуру» [5], який визначає правові та організаційні засади функціонування системи захисту критичної інфраструктури, принципи державної політики, повноваження органів влади та обов'язки операторів. Водночас подальша гармонізація із CER передбачає нормативне закріплення обов'язкових стандартів безперервності сервісів, процедур тестування стійкості, механізмів зовнішнього аудиту та посилення відповідальності за невиконання вимог.

Особливого значення набуває публічний інтерес як правова основа встановлення спеціальних обов'язків для операторів критичної інфраструктури. Більшість таких операторів є суб'єктами приватного права або функціонують у змішаних формах власності. Водночас їх діяльність безпосередньо впливає на реалізацію базових прав людини та національну безпеку. У цьому аспекті публічний інтерес виконує функцію конституційного критерію допустимості втручання у сферу приватної власності та свободи підприємництва. Обмеження можуть визнаватися правомірними лише за умови їх законодавчого закріплення, спрямованості на легітимну мету захисту безпеки та прав інших осіб, а також відповідності принципу пропорційності. Отже, конституційна модель балансу передбачає не домінування публічного інтересу, а його узгодження з гарантіями економічної свободи.

Такий баланс виявляється у встановленні для операторів обов'язків щодо управління ризиками, впровадження систем внутрішнього контролю, інвестування у заходи фізичної та кібербезпеки, обов'язкового інформування державних органів про інциденти. Водночас держава зобов'язана забезпечити правову визначеність, недискримінаційність регулювання та механізми компенсації у випадку надмірного втручання у сферу приватної господарської діяльності.

Отже, спеціальні обов'язки операторів не є свавільним втручанням, а виступають формою реалізації соціальної функції власності та елементом конституційного компромісу між свободою підприємництва і потребами суспільства.

У контексті практики Європейського суду з прав людини позитивні зобов'язання держави включають не лише утримання від свавільного втручання, але й активні дії щодо створення ефективних механізмів запобігання ризикам для життя і здоров'я осіб. У сфері критичної інфраструктури це означає належне нормативне регулювання, контроль за діяльністю операторів, створення систем раннього попередження та забезпечення ефективного реагування на надзвичайні ситуації. Невиконання таких обов'язків може розглядатися як порушення, зокрема у контексті статей 2 та 8 Конвенції про захист прав людини і основоположних свобод [18], конвенційних стандартів захисту прав людини.

У сучасній правовій доктрині поняття resilience (стійкість) набуває філософського виміру як характеристика постмодерної державності. Якщо класична модерна держава формувалася як "security state" — держава безпеки, орієнтована на контроль, запобігання та нейтралізацію загроз через централізовані механізми влади, — то сучасна модель поступово трансформується у «resilience state» — державу стійкості, що функціонує в умовах постійної невизначеності та багатовимірних ризиків.

У парадигмі security state домінує ідея передбачуваності та усунення загроз як таких. Натомість концепція resilience виходить з усвідомлення неминучості криз, катастроф та системних збоїв. Завдання держави полягає не лише у запобіганні ризикам, а у формуванні здатності суспільства, інституцій та інфраструктур адаптуватися, функціонувати в умовах порушень та відновлюватися після них. У цьому сенсі стійкість постає як правова категорія постмодерного права, що інтегрує принципи гнучкості, адаптивності,

багаторівневого врядування та спільної відповідальності держави й приватних акторів.

Філософія resilience state відображає зміну самої природи публічної влади: від моделі гарантування абсолютної безпеки до моделі управління ризиками та підвищення здатності систем до самовідновлення. Такий підхід корелює з розвитком європейського права, зокрема із закріпленням у Directive (EU) 2022/2557 [1] концепції безперервності критичних сервісів як суспільного блага, що має підтримуватися навіть в умовах кризових подій.

Таким чином, resilience state не заперечує функції безпеки, а трансформує її зміст. Безпека перестає бути статичною категорією «захищеності від загроз» і набуває динамічного характеру — як здатність систем адаптуватися до змін, витримувати навантаження та відновлюватися після криз. У правовому вимірі це означає перехід від централізованої моделі контролю до багаторівневої системи управління ризиками, в якій відповідальність розподіляється між державою, операторами критичної інфраструктури та суспільством, а ключову роль відіграють механізми координації, стратегічного планування та корпоративної відповідальності.

Сучасні загрози мають гібридний характер, включаючи фізичні руйнування, кібератаки, технологічні аварії та соціальні потрясіння. Це зумовлює необхідність інтегрованого підходу до фізичної та кіберстійкості. У цьому контексті Directive (EU) 2022/2555 (NIS2) [2] встановлює вимоги до управління кіберризиками, обов'язкової звітності про інциденти, запровадження технічних та організаційних заходів безпеки, а також персональної відповідальності керівних органів суб'єктів. На відміну від попередніх актів, NIS2 підсилює вимоги до корпоративного управління ризиками та вводить санкційні механізми за їх невиконання.

Поєднання CER та NIS2 формує комплексну модель управління ризиками, у межах якої фізична та цифрова безпека розглядаються

як взаємопов'язані складники єдиного механізму забезпечення безперервності критичних сервісів. Для України така інтеграція є не лише обов'язковою умовою виконання євроінтеграційних зобов'язань, а й необхідною умовою зміцнення національної безпеки в умовах воєнних і кіберзагроз. Важливу роль у цьому процесі відіграє також Національний план забезпечення стійкості критичної інфраструктури на 2025–2030 роки [19], який закріплює пріоритет переходу до моделі ризик-орієнтованого управління, розвитку державно-приватного партнерства та запровадження стандартів стійкості, сумісних із правом ЄС.

Законодавча практика 2022–2025 років продемонструвала ефективність системного підходу та його прогалини. Масовані ракетні обстріли енергетичної інфраструктури засвідчили, що саме здатність до швидкого відновлення сервісів, резервування потужностей та децентралізація систем управління є ключовими елементами стійкості. Енергетичний сектор залишається найбільш вразливим компонентом критичної інфраструктури, що обумовлює необхідність впровадження стандартів резервування потужностей, децентралізації генерації та інтеграції до європейських механізмів ризик-підготовки. Водночас кібератаки на цифрові системи управління показали критичну необхідність синхронізації фізичної та кібербезпеки відповідно до стандартів NIS2 [2].

Правове регулювання функціонування критичної інфраструктури в Україні здійснюється в умовах правового режиму воєнного стану, що істотно впливає на характер державного управління, процедури кризового реагування, мобілізаційне планування та координацію між суб'єктами сектору безпеки й оборони. Воєнний контекст зумовлює посилення ролі держави та розширення меж допустимого регуляторного втручання у сферу приватної господарської діяльності відповідно до Закону України «Про правовий режим воєнного стану» [20].

Воєнний стан актуалізував питання співвідношення конституційних гарантій і безпекових обмежень. У сфері критичної інфраструктури це проявляється у спрощенні процедур ухвалення управлінських рішень, можливості тимчасового обмеження окремих майнових прав, мобілізації ресурсів приватних операторів та централізації координації. Водночас такі заходи повинні зберігати тимчасовий характер і відповідати конституційним стандартам правової визначеності та пропорційності.

Період 2022–2026 років характеризується активним розвитком нормативної бази у сфері критичної інфраструктури. Практичні виклики воєнного часу зумовили необхідність конкретизації положень Закону України «Про критичну інфраструктуру» [5] та прийняття низки підзаконних актів щодо категоризації об'єктів, ведення Реєстру критичної інфраструктури та організації міжвідомчої взаємодії.

Було посилено координаційну роль органів сектору безпеки, зокрема в частині кіберзахисту та реагування на гібридні загрози. Важливого значення набули положення Закону України «Про національну безпеку України» [21] та Закону України «Про основні засади забезпечення кібербезпеки України» [6], які забезпечують інтеграцію сфери критичної інфраструктури до загальної системи стратегічного планування безпеки.

Водночас нормативна практика засвідчила наявність певних проблемних аспектів, зокрема недостатню деталізацію механізмів зовнішнього аудиту стійкості, нечіткість меж відповідальності операторів у разі системних збоїв, а також обмеженість фінансових інструментів підтримки модернізації інфраструктурних об'єктів, що обмежує реалізацію принципу ефективності публічного управління. Ці питання потребують подальшого доктринального осмислення та нормативного врегулювання.

Воєнна практика продемонструвала необхідність нормативного закріплення:

— механізмів резервування та відновлення потужностей;
— процедур кризового управління;
— інтеграції фізичної та кібербезпеки;
— посилення відповідальності операторів.

Отже, воєнний досвід засвідчив необхідність трансформації системи захисту критичної інфраструктури від декларативної моделі до практично функціонуючого механізму забезпечення стійкості.

Таким чином, стійкість критичної інфраструктури постає як правовий стандарт функціонування сучасної держави, що поєднує захист публічного інтересу, гарантування прав людини та інтеграцію до європейського правового простору. Її реалізація вимагає комплексної міжгалузевої взаємодії, чіткого нормативного закріплення принципу безперервності сервісів, забезпечення балансу між публічним інтересом і правом приватної власності, а також адаптації європейських стандартів до національної специфіки післявоєнного відновлення [1; 2; 5].

3. Гармонізація законодавства України з вимогами CER: стан та виклики 2026 року

Теоретико-правовий аналіз категорії стійкості критичної інфраструктури, здійснений у попередньому підрозділі, дозволяє розглядати її не лише як безпекову характеристику, а як комплексний принцип публічного управління. Станом на 2026 рік гармонізація перебуває на етапі часткової імплементації, що поєднує нормативне наближення до стандартів ЄС зі збереженням структурних розбіжностей у процедурному та інституційному вимірах. У цьому контексті гармонізація законодавства України з вимогами Directive (EU) 2022/2557 [1] про стійкість критичних суб'єктів (CER) постає не технічною імплементацією окремих норм, а трансформацією

правового режиму критичної інфраструктури відповідно до стандартів ЄС та практичного досвіду воєнного періоду.

Гармонізація у цьому контексті має розглядатися не як формальна адаптація норм, а як процес функціональної конвергенції правових систем, що передбачає узгодження принципів, процедур і інституційних моделей управління ризиками. Йдеться про інтеграцію української системи забезпечення стійкості до європейського регуляторного простору на основі спільних стандартів належного врядування та правової визначеності.

Відповідно до статті 3 Директиви (EU) 2022/2557 [1] держави-члени зобов'язані забезпечити функціонування системи ідентифікації критичних суб'єктів на основі національної оцінки ризиків, що підкреслює процедурний характер імплементації, а не лише декларативне наближення законодавства. Отже, імплементація CER передбачає не лише адаптацію термінології, а створення процедурної інфраструктури управління ризиками, що має нормативно закріплений характер.

Закон України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX започаткував національну систему захисту та визначив базові принципи політики у цій сфері [5], проте події 2022–2025 років засвідчили необхідність поглиблення цієї моделі з урахуванням стандартів ЄС та фактичного досвіду функціонування держави в умовах масштабної збройної агресії [1]. Зазначений період трансформував саму філософію захисту КІ — від декларативного забезпечення безпеки до системної моделі управління стійкістю, що поєднує превенцію, реагування та відновлення [10; 13].

Повномасштабна збройна агресія проти України зумовила суттєву трансформацію нормативно-правового регулювання у сфері забезпечення стійкості критичної інфраструктури. Період 2022–2025 років характеризується переходом від формального запровадження базових положень Закону України «Про критичну

інфраструктуру» [5] до практичного розгортання інституційних і процедурних механізмів його реалізації.

Насамперед було розширено підзаконне нормативне регулювання, спрямоване на деталізацію порядку ідентифікації, категоризації та обліку об'єктів критичної інфраструктури. Кабінетом Міністрів України затверджено низку актів, що визначають порядок формування та ведення Реєстру об'єктів критичної інфраструктури, критерії віднесення об'єктів до відповідних категорій критичності, процедури взаємодії суб'єктів забезпечення КІ та алгоритми обміну інформацією про загрози та інциденти.

Особливе значення має створення та нормативне закріплення порядку ведення Реєстру об'єктів критичної інфраструктури [22]. Реєстр виступає центральним інструментом державного управління у сфері КІ, забезпечуючи систематизацію інформації про об'єкти та операторів, визначення рівня їх критичності, координацію між суб'єктами сектору безпеки та формування основи для ризикоорієнтованого планування.

У 2022–2024 роках відбулося уточнення процедур внесення інформації до Реєстру, розмежування повноважень відповідальних органів та посилення режиму захисту інформації з обмеженим доступом [22; 23]. Водночас потребує подальшої нормативної конкретизації питання періодичного перегляду статусу об'єктів та інтеграції Реєстру з галузевими інформаційними системами.

Важливим елементом реформування стало запровадження більш деталізованих критеріїв категоризації об'єктів КІ [23]. Якщо Закон України «Про критичну інфраструктуру» [5] встановлює загальні засади віднесення об'єктів до критичних, то підзаконні акти конкретизують систему оцінки значущості об'єкта за кількісними та якісними показниками.

Серед ключових критеріїв визначено: 1) кількість населення, що залежить від функціонування об'єкта; 2) масштаб економічних

втрат у разі припинення діяльності; 3) тривалість можливого переривання надання послуг; 4) потенційні наслідки для національної безпеки; 5) кумулятивний ефект повторюваних атак.

Такий підхід наближає українську модель до стандартів Directive (EU) 2022/2557 [1], де ключовим є критерій «значного деструктивного ефекту».

Після 2022 року було уточнено та розширено повноваження суб'єктів системи забезпечення стійкості критичної інфраструктури.

Національний координаційний центр кібербезпеки (НК ЦК) здійснює координацію діяльності суб'єктів кібербезпеки у сфері захисту об'єктів критичної інфраструктури та забезпечує стратегічне планування реагування на кіберінциденти [24].

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) реалізує повноваження щодо аудиту захищеності інформаційно-комунікаційних систем операторів КІ, впровадження стандартів кіберзахисту та методичного супроводу суб'єктів господарювання [25].

Служба безпеки України (СБУ) здійснює контррозвідувальний захист об'єктів КІ, протидію диверсійним та терористичним загрозам, а також бере участь у міжвідомчій оцінці ризиків в умовах воєнного стану [26].

Узгодження повноважень зазначених органів здійснюється відповідно до законодавства у сфері національної безпеки та критичної інфраструктури [5], що спрямовано на формування цілісної багаторівневої моделі управління стійкістю.

Таким чином, 2022–2025 роки стали періодом інституційної операціоналізації національної системи забезпечення стійкості критичної інфраструктури. Було створено нормативну основу функціонування Реєстру КІ, деталізовано механізми категоризації об'єктів, посилено повноваження координаційних і контрольних органів

та започатковано наближення національної моделі до стандартів Європейського Союзу [1].

Водночас подальшого розвитку потребує гармонізація підзаконного регулювання з вимогами CER, зокрема у частині уніфікації критеріїв оцінки ризиків, процедур перевірки стійкості та транскордонного обміну інформацією.

У 2026 році питання гармонізації постає не лише як імплементація окремих положень CER, а як комплексна трансформація правового режиму критичної інфраструктури (КІ) в умовах воєнного та післявоєнного стану. Йдеться про поєднання трьох вимірів: безпекового (стійкість до фізичних та кіберзагроз); відновлювального (правові механізми реконструкції та компенсації); інтеграційного (відповідність acquis ЄС та взаємне визнання стандартів стійкості) [1; 2]. Така триєдина модель фактично формує нову парадигму публічно-правового регулювання, у якій категорія «стійкість» набуває міжгалузевого характеру та інтегрує норми адміністративного, конституційного, інформаційного та міжнародного права [9; 10; 13].

Безпековий вимір передбачає не лише фізичний захист об'єктів, а й інституційну спроможність до прогнозування ризиків на основі сценарного аналізу, включаючи воєнні та гібридні загрози. У цьому аспекті концепція resilience у праві ЄС виходить із розуміння безпеки як процесу, а не стану: стійкість означає не відсутність загроз, а здатність системи адаптуватися до них без втрати основних функцій [2]. При цьому реалізація принципу субсидіарності гарантує багаторівневу відповідальність — на рівні оператора, сектора та держави, що дозволяє поєднати превентивні, оперативні та стратегічні заходи [14]. Відновлювальний аспект пов'язаний із формуванням спеціальних правових механізмів реконструкції та компенсації у випадку масштабного пошкодження інфраструктури. Практика 2022–2025 років продемонструвала, що без правового

регламентування процедур прискореного відновлення, спрощених закупівель та фінансових гарантій оператори КІ не здатні забезпечити швидке повернення до нормального функціонування [19]. Інтеграційний вимір означає приведення національних критеріїв оцінки ризиків та категоризації суб'єктів у відповідність до acquis ЄС, що забезпечує сумісність систем моніторингу, транскордонний обмін інформацією та взаємне визнання аудитів стійкості [1; 2].

Така триєдина модель відповідає концепції функціональної державності, в межах якої публічна влада оцінюється не за формальним обсягом повноважень, а за здатністю забезпечувати безперервність суспільно значущих функцій.

У межах цієї моделі стійкість набуває ознак нормативного стандарту публічного адміністрування, що підлягає перевірці через критерії ефективності, передбачуваності та адаптивності регуляторних механізмів. Це означає, що оцінці підлягає не лише наявність нормативної бази, а її здатність забезпечити реальний захист суспільно значущих функцій у кризових умовах.

CER закріплює концепцію «значного деструктивного ефекту» як ключовий критерій ідентифікації критичних суб'єктів [1]. Український досвід воєнного періоду розширює зміст цієї категорії, оскільки ураження інфраструктури відбувалося системно, повторювано та з кумулятивним ефектом [19]. Масовані ракетні атаки на енергетичний сектор у 2022–2023 роках продемонстрували каскадний вплив на транспорт, зв'язок, медичні заклади та водопостачання. У 2024–2025 роках аналогічні ризики виникали щодо портової інфраструктури та логістичних вузлів, що мали транскордонне значення. Таким чином, практичні кейси підтвердили необхідність формалізації в методиках оцінки ризику таких параметрів, як повторюваність атак, кумулятивність руйнувань та міжсекторна залежність. Додатково постає питання врахування фактору навмисності ураження як окремої ознаки воєнного ризику, що відрізняє його

від природних або техногенних катастроф та вимагає окремих юридичних індикаторів [13].

Доцільним є нормативне закріплення в національному законодавстві визначення «значного деструктивного ефекту» як такого, що охоплює: кількість постраждалого населення; тривалість порушення сервісу; масштаб економічних втрат; транскордонні наслідки; кумулятивність та повторюваність впливу. Закріплення такого визначення на рівні закону забезпечить єдність практики категоризації та мінімізує дискреційність адміністративних органів. Крім того, законодавча конкретизація цього критерію сприятиме формуванню єдиної судової практики та підвищить передбачуваність правозастосування, що є ключовою вимогою принципу правової визначеності в умовах воєнного стану.

У теоретико-доктринальному вимірі категорія "resilience" у праві ЄС формується як інтегративний принцип, що поєднує безпекову політику, внутрішній ринок та захист прав людини [9; 10; 13]. Вона корелює з концепцією "good governance", оскільки передбачає прозорість управління ризиками, підзвітність операторів і державних органів, а також участь приватного сектору в системі колективної безпеки [14; 15]. Стійкість у цьому розумінні виступає функціональною гарантією реалізації основних прав, адже безперервність енергопостачання, транспорту чи цифрових сервісів прямо впливає на здійснення права на життя, охорону здоров'я, підприємницьку діяльність і доступ до інформації [15]. Реалізація принципів субсидіарності та багаторівневого врядування гарантує, що відповідальність за resilience поділяється між державою, секторальними органами та операторами, а не концентрується лише на центральних органах влади [19]. Відтак імплементація CER має розглядатися як інструмент позитивних зобов'язань держави щодо забезпечення належних умов реалізації прав людини, а не виключно як технічна безпекова реформа [14; 15].

В українському праві Закон «Про критичну інфраструктуру» закріплює категоризацію об'єктів за секторним принципом та визначає загальні критерії віднесення до критичних об'єктів залежно від їх значення для національної безпеки [5]. Проте чинна модель менш деталізована у частині оцінки потенційних наслідків порушення функціонування суб'єктів, що створює нормативну прогалину в порівнянні з вимогами CER [1; 19]. Українське законодавство допускає розроблення методичних підходів до оцінки ризиків та визначення критичних суб'єктів через підзаконні акти та стандарти, проте відсутність чітко виписаного критерію «значного деструктивного ефекту» як самостійного юридичного поняття може призводити до неоднорідної практики ідентифікації [10; 13]. У перспективі гармонізації доцільним є законодавче визначення цього поняття із встановленням переліку кількісних та якісних індикаторів, включаючи соціально-економічні та гуманітарні наслідки [19].

Перша відмінність між CER та національним законом полягає у підходах до формування реєстру критичних суб'єктів:

— CER застосовує ризикоорієнтовану модель, яка враховує мультидоменні загрози та потенційний транскордонний вплив [1; 2];

— національне законодавство покладається на об'єктно-галузевий принцип, визначаючи критичні суб'єкти за їх статусом та значенням для держави [5].

Цей аспект має практичне значення. Наприклад, масовані удари по енергетичній інфраструктурі у 2022–2023 роках демонстрували, що наслідки для населення, економіки та критично важливих об'єктів держави можуть бути значними незалежно від формальної галузевої категорії об'єкта [19]. CER у таких випадках вимагає попередньої ідентифікації та оцінки потенційного впливу на всіх рівнях, що дозволяє запроваджувати превентивні заходи та оперативні плани реагування [1]. Українська практика показала необхідність подальшого розвитку інтегрованого реєстру з можливістю

оперативного оновлення статусу об'єкта залежно від зміни безпекової ситуації [19].

Друга відмінність стосується обов'язків операторів критичної інфраструктури та процедур управління ризиками. CER прямо визначає вимоги щодо регулярної оцінки ризиків, впровадження заходів з управління ними, розробки та тестування планів безперервності діяльності та повідомлення компетентних органів про інциденти у встановлені строки [1; 2]. Закон України містить лише загальні положення про обов'язки операторів щодо взаємодії з державними органами та забезпечення захисту, без деталізації процедурних аспектів, стандартів оцінки ризиків або конкретних термінів повідомлення [5]. Це створює правову невизначеність для операторів і підвищує ризики неузгодженого реагування [19]. Гармонізація потребує розроблення уніфікованих стандартів оцінки ризиків та запровадження механізмів відповідальності за їх недотримання [2].

Третя відмінність полягає в інтеграції фізичної та кіберстійкості. Directive (EU) 2022/2555 встановлює загальні вимоги до управління кіберризиками, процедур звітності та мінімальних стандартів безпеки для критичних мереж і систем [2]. В українському законодавстві фізична та кібербезпека врегульовані окремо, що зумовлює потребу у формуванні єдиної нормативної рамки [5]. Синхронізація має включати уніфіковані строки повідомлення про інциденти, спільні критерії оцінки впливу та інтегровані аудити стійкості [1; 2; 19].

Практичні кейси підтверджують необхідність інтегрованого підходу. Під час кібератак на телекомунікаційні системи 2023–2024 рр. цифрові інциденти безпосередньо впливали на фізичне функціонування об'єктів, зокрема електромереж та енергетичних систем, підкреслюючи потребу формального поєднання процедур оцінки ризиків, планів безперервності та обміну інформацією між уповноваженими органами [2].

Координація та роль уповноважених органів є критичною для ефективної гармонізації. Закон визначає компетентні органи та механізми узгодженого управління КІ [5], тоді як CER вимагає наявності єдиного координаційного центру для моніторингу ризиків, обміну інформацією та контролю за виконанням вимог. У національній моделі функції координації розподілені між декількома суб'єктами — Кабінетом Міністрів України, профільними міністерствами, НК ЦК та ДССЗЗІ, що створює ризик дублювання повноважень та процедурної невизначеності. У 2022–2025 рр. національна практика включала створення оперативних штабів, посилення міжвідомчої взаємодії та розширення повноважень у сфері кібербезпеки [19]. Водночас залишається необхідність інституційного закріплення єдиного механізму оцінки ризиків, централізованого моніторингу та стандартизованого обміну інформацією. Такий орган повинен діяти на засадах прозорості, підзвітності та процесуальної визначеності. Доцільним є законодавче визначення єдиного координатора системи оцінки ризиків із чітким переліком його компетенції та процедурної підзвітності.

Важливо також забезпечити відповідність діяльності уповноважених органів конституційним принципам законності, пропорційності та правової визначеності, а посилення контролю супроводжувати чіткими гарантіями прав операторів, включаючи можливість оскарження рішень та доступ до процедур перегляду. Паралельно реалізація позитивних зобов'язань держави передбачає, що забезпечення безперервності КІ є не лише безпековим, а й соціальним і правовим пріоритетом, безпосередньо пов'язаним із правом громадян на життя, охорону здоров'я та доступ до основних послуг. Питання позитивних зобов'язань безпосередньо пов'язане з проблематикою юридичної відповідальності держави за належну організацію системи стійкості. Аналіз викликів гармонізації неможливий без оцінки меж та змісту публічно-правової відповідальності держави у сфері забезпечення стійкості.

Публічно-правова відповідальність держави у сфері забезпечення стійкості критичної інфраструктури є логічним продовженням концепції позитивних зобов'язань, що випливають із Конституції України та європейських стандартів належного врядування. У світлі практики Європейського суду з прав людини позитивні зобов'язання держави передбачають не лише утримання від втручання, а й активні дії щодо організації ефективної системи запобігання загрозам, що може поширюватися й на сферу критичної інфраструктури [10; 13]. Якщо на операторів критичних суб'єктів покладаються спеціальні обов'язки щодо управління ризиками, планування безперервності діяльності та повідомлення про інциденти, то держава, своєю чергою, несе відповідальність за належну організацію системи координації, регулювання та контролю у цій сфері.

По-перше, відповідальність держави може мати конституційно-правовий вимір. Неналежна організація системи забезпечення стійкості, відсутність чітких процедур реагування або несвоєчасне прийняття нормативних актів можуть розглядатися як порушення позитивних зобов'язань держави щодо гарантування права на життя, безпеку та охорону здоров'я, закріплених у Конституції України [4]. У цьому аспекті забезпечення безперервності функціонування критичних сервісів є складником обов'язку держави діяти належним чином та добросовісно. У перспективі це може актуалізувати питання конституційного контролю за нормативними актами у сфері стійкості критичної інфраструктури, якщо їх недосконалість або відсутність створює системні ризики для реалізації основних прав людини.

По-друге, можливим є деліктний вимір відповідальності. У випадках, коли шкода завдана фізичним або юридичним особам унаслідок неправомірних рішень чи бездіяльності органів державної влади щодо організації системи захисту та координації КІ, може поставати питання про відшкодування шкоди відповідно

до принципів публічно-правової деліктної відповідальності. Йдеться не про відповідальність за сам факт настання воєнних дій чи форс-мажорних обставин, а про відповідальність за неналежне нормативне чи організаційне забезпечення системи управління ризиками, якщо буде доведено причинно-наслідковий зв'язок між бездіяльністю держави та завданою шкодою [27].

По-третє, особливого значення набуває бюджетно-правовий аспект відповідальності. Забезпечення стійкості критичної інфраструктури потребує стабільного фінансування, формування резервних фондів, програм модернізації та аудиту стійкості. Невиконання бюджетних зобов'язань, нецільове використання коштів або відсутність фінансування передбачених законом заходів може тягнути фінансово-правові санкції та контрольні механізми з боку органів державного фінансового нагляду, відповідно до Бюджетного кодексу України [28]. У цьому контексті відповідальність держави проявляється як обов'язок забезпечити належне ресурсне підґрунтя функціонування системи стійкості.

У цьому контексті доцільним є створення цільових фондів стійкості критичної інфраструктури з чітким нормативним режимом використання коштів та парламентським контролем.

У межах гармонізації з Directive (EU) 2022/2557 [1] особливого значення набуває інституційна підзвітність компетентних органів. CER передбачає створення національних механізмів координації та контролю, що мають діяти прозоро, ефективно та з дотриманням принципів верховенства права. Отже, відповідальність держави у сфері забезпечення стійкості має розглядатися як системна — вона охоплює нормативний, організаційний та фінансовий рівні й виступає гарантією балансу між публічними повноваженнями та правами суб'єктів господарювання.

Практичні кейси 2022–2025 рр. підтвердили: 1) масовані удари по енергетичній інфраструктурі створювали значні перебої

в електропостачанні, показавши необхідність попереднього тестування та стандартизації планів безперервності; 2) кібератаки на телекомунікаційні системи продемонстрували прямий вплив цифрових загроз на фізичне функціонування КІ, підкресливши необхідність інтеграції NIS2 та CER; 3) порушення роботи транспортних коридорів і морських портів підтвердили потребу формалізації процедур транскордонної оцінки наслідків і міжнародної координації. Особливого значення набувають об'єкти подвійного призначення (dual-use), ураження яких одночасно впливає на цивільну економіку та обороноздатність держави [19]. Чинне законодавство не виділяє їх як окрему категорію, що створює нормативну прогалину в умовах воєнного стану [5]. Водночас у контексті воєнного стану об'єкти подвійного призначення фактично виконують функцію інфраструктурної підтримки обороноздатності, що обґрунтовує необхідність встановлення для них спеціального режиму категоризації та фінансування [21].

Таким чином, гармонізація законодавства України з вимогами CER повинна передбачати не лише посилення обов'язків операторів, а й нормативне закріплення чітких стандартів належної діяльності держави, включаючи механізми контролю, відповідальності та судового захисту у випадках неналежного виконання публічних функцій у сфері забезпечення стійкості критичної інфраструктури.

У розвиток зазначеної проблематики доцільним є нормативне закріплення поняття «об'єкти критичної інфраструктури подвійного призначення» з визначенням: спеціального режиму доступу; окремих вимог до планування відновлення; особливого порядку фінансування реконструкції [19].

У післявоєнний період правовий режим КІ має трансформуватися з надзвичайного у стабільний, але з урахуванням накопиченого досвіду. Зазначені вище виміри гармонізації набувають конкретного нормативного наповнення у післявоєнний період.

Гармонізація з CER означає:

— закріплення обов'язкових процедур регулярної оцінки ризиків з урахуванням воєнних сценаріїв [1; 2];

— інтеграцію фізичної та кіберстійкості відповідно до вимог Directive (EU) 2022/2555 [2];

— формалізацію поняття кумулятивного ефекту та повторюваності загроз [1; 19];

— створення правового режиму спеціального відновлення dual-use об'єктів із чітким розмежуванням джерел фінансування та прозорими процедурами контролю [5; 19].

Важливим елементом гармонізації є також узгодження процедур повідомлення про інциденти, аудитів стійкості та міжнародної координації. Події 2022–2025 років засвідчили, що критична інфраструктура України фактично стала частиною європейського безпекового простору, адже порушення її функціонування впливало на енергетичну стабільність сусідніх держав [19]. Це підтверджує необхідність інституціоналізації транскордонного обміну інформацією, спільного планування реагування та участі України у механізмах колективної стійкості ЄС [1; 2].

Модель CER є ризикоорієнтованою, процедурно деталізованою та інституційно централізованою, тоді як українська модель — об'єктно-секторною, рамковою та фрагментарно імплементованою.

У цьому контексті держава виступає не лише регулятором, а й гарантом системної ефективності моделі стійкості. Гармонізація з CER має здійснюватися не шляхом механічного відтворення норм директиви, а через системну адаптацію її принципів до умов воєнного та післявоєнного відновлення, із закріпленням процедурної визначеності, чіткої ієрархії компетенцій та механізмів юридичної відповідальності.

Узагальнення наведених аспектів дозволяє систематизувати ключові проблеми гармонізації, що мають як нормативний, так і інституційний характер.

Станом на 2026 рік можна виокремити такі виклики:

1. Відсутність законодавчо визначеного критерію «значного деструктивного ефекту» як самостійної юридичної категорії [1; 5].
2. Недостатня процедурна деталізація обов'язків операторів, зокрема щодо строків і стандартів управління ризиками [5; 19].
3. Фрагментарність інтеграції NIS2 та CER, що потребує єдиної нормативної рамки [2].
4. Нечіткість розмежування повноважень компетентних органів, що може створювати управлінські дисбаланси [5; 19].
5. Необхідність правового врегулювання статусу dual-use об'єктів та особливого режиму їх відновлення [19].
6. Баланс безпеки та гарантій прав суб'єктів господарювання, включаючи процедури оскарження рішень державних органів.

Таким чином, гармонізація законодавства України з вимогами CER у 2026 році набуває системного характеру та виходить за межі формальної імплементації європейських директив. Вона передбачає трансформацію національної моделі критичної інфраструктури з об'єктно-секторної та рамкової у ризикоорієнтовану, процедурно деталізовану та інституційно підзвітну систему управління стійкістю. Досвід 2022–2025 років підтвердив актуальність підходів ЄС, водночас виявивши потребу їх адаптації з урахуванням воєнних загроз та специфіки об'єктів подвійного призначення [19]. У цьому контексті Україна виступає не лише як держава-реципієнт стандартів ЄС, а як суб'єкт формування нової практики правового регулювання стійкості в умовах тривалих гібридних і воєнних ризиків, що може впливати на подальшу еволюцію європейської моделі захисту критичних суб'єктів. У цьому сенсі досвід України формує прецедент правового осмислення стійкості в умовах тривалого воєнного конфлікту, що здатний модифікувати традиційні підходи ЄС до оцінки ризиків та інституційної координації. Це підтверджує, що стійкість критичної інфраструктури є безпосереднім проявом публічного інтересу як основи національної безпеки України.

4. Секторальний аналіз та ідентифікація критичних суб'єктів

Стійкість критичної інфраструктури значною мірою залежить від здатності держави та операторів критичних послуг ідентифікувати ті суб'єкти, чиє порушення функціонування може завдати значної шкоди життєво важливим суспільним і економічним процесам. У контексті імплементації Directive (EU) 2022/2557 (CER) [1] і національного законодавства ключовою стає методологія оцінки ризиків, що дозволяє встановити критерії значного деструктивного ефекту за міжнародними стандартами ЄС і адаптувати їх до національних умов. При цьому надзвичайно важливо розглянути специфіку окремих секторів, що визначені законодавством та актами ЄС, оскільки саме вони забезпечують базові функції держави. Не менш важливим є питання транскордонної критичної інфраструктури, що вимагає особливих правових механізмів взаємодії з країнами-сусідами ЄС, оскільки функціонування таких об'єктів виходить за межі національної юрисдикції й потребує узгоджених процедур міждержавної координації, відповідно до механізмів співпраці, передбачених правом Європейського Союзу у сфері стійкості критичних суб'єктів.

У межах CER поняття значного деструктивного ефекту є фундаментальним для ідентифікації критичних суб'єктів та визначення обсягу заходів, які держава повинна застосовувати для забезпечення їхньої стійкості [1]. Відповідно до цього стандарту, значний деструктивний ефект охоплює потенційний вплив порушення діяльності суб'єктів на базові функції суспільства, серйозні економічні збитки, загрозу життю та здоров'ю населення, а також потенційний транскордонний вплив у сусідніх державах. Такий підхід має багатовимірну природу: він інтегрує показники фізичного збитку, соціально-економічного впливу та стратегічного значення для національної безпеки. Методологія оцінки ризиків у рамках CER є ризикоорієнтованою, що передбачає не лише технічний аналіз загроз, але й кількісну оцінку ймовірності їх реалізації та наслідків.

Така оцінка має базуватися на об'єктивних показниках, включно з кількістю населення, яке може постраждати, обсягом економічних втрат, тривалістю переривання критичних послуг, потенційними екологічними наслідками та можливістю подальшого розповсюдження наслідків у суміжні сфери [1], що відповідає підходу all-hazards risk assessment у праві ЄС. Закріплення таких критеріїв на рівні закону або підзаконного нормативного акта сприятиме уніфікації адміністративної практики ідентифікації критичних суб'єктів та мінімізує ризики надмірної дискреції уповноважених органів. Такий підхід відповідає принципу правової визначеності як складнику верховенства права, оскільки встановлення чітких критеріїв значного деструктивного ефекту унеможливлює довільне тлумачення статусу критичного суб'єкта та забезпечує передбачуваність правозастосування. Крім того, нормативне закріплення критеріїв сприятиме формуванню єдиної адміністративної практики та підвищить рівень довіри між державою й операторами критичних послуг.

У цьому контексті особливого значення набуває можливість судового перегляду рішень щодо віднесення суб'єкта до категорії критичних. Наявність чітких критеріїв значного деструктивного ефекту створює процесуальні передумови для ефективного судового контролю, що зміцнює гарантії прав суб'єктів господарювання та забезпечує баланс між публічним інтересом і свободою підприємницької діяльності, відповідно до статті 55 Конституції України [4].

У національному контексті, хоча Закон України «Про критичну інфраструктуру» надає загальні засади оцінки загроз і ризиків [5], CER вимагає більш детальної методики, що включає кількісні та якісні параметри оцінювання. Одним із головних викликів гармонізації є створення національного стандарту оцінки ризиків, який би узгоджувався з європейськими вимогами, водночас враховував специфіку національних секторів та ризиків, притаманних Україні. Такий стандарт має визначати процедури збирання інформації,

алгоритми обробки даних, критерії визначення рівнів ризику та механізми прийняття рішень щодо заходів забезпечення стійкості. Важливо також передбачити періодичний перегляд такого стандарту з урахуванням змін безпекового середовища, розвитку технологій та практики застосування Директиви CER у державах-членах ЄС [1]. Динамічний характер ризиків вимагає нормативної гнучкості, яка водночас не повинна підривати стабільність правового регулювання. Водночас він повинен бути системно пов'язаний із законодавством у сфері національної безпеки та кібербезпеки, а також із зобов'язаннями України у межах Угоди про асоціацію з ЄС [8], що передбачають поступову імплементацію європейських стандартів у сфері захисту критичних систем.

Окремого розгляду потребує методологія стрес-тестування критичної інфраструктури як інструмент імплементації статті 12 Директиви CER, яка встановлює обов'язок держав забезпечити перевірку стійкості критичних суб'єктів. Відповідно до цієї норми, держави повинні забезпечити регулярне тестування стійкості критичних суб'єктів шляхом проведення сценарного моделювання кризових ситуацій, оцінки готовності до надзвичайних подій та перевірки ефективності планів безперервності діяльності [1]. Імплементація цієї вимоги в українське законодавство передбачає нормативне закріплення обов'язку проведення періодичних стрес-тестів для суб'єктів КІ з урахуванням галузевої специфіки. Такі стрес-тести мають включати: моделювання фізичних атак, масштабних техногенних аварій, тривалих відключень енергопостачання, а також комплексних кіберінцидентів; оцінку швидкості відновлення послуг; перевірку координації між оператором, органами державної влади та службами реагування. Інституційне закріплення цієї процедури може здійснюватися через внесення змін до підзаконних актів на виконання Закону «Про критичну інфраструктуру» [5], а також шляхом узгодження з положеннями законів

у сфері кібербезпеки та національної безпеки, включаючи сценарії комбінованих (multi-hazard) загроз. Стрес-тестування повинно стати не формальною перевіркою, а постійним елементом стратегічного управління ризиками, результати якого використовуються для коригування державної політики та інвестиційних пріоритетів. Доцільним є нормативне визначення органу, відповідального за координацію та методичне забезпечення стрес-тестування (наприклад, на базі уповноваженого органу у сфері критичної інфраструктури), а також встановлення вимог до періодичності оприлюднення узагальнених результатів з урахуванням режиму обмеженого доступу до інформації.

Практична імплементація зазначених підходів передбачає розроблення національних сценаріїв ризику, що симулюють різні варіанти складних надзвичайних ситуацій, включно з комбінованими (гібридними) загрозами. Це дозволяє не лише встановити ризикові профілі окремих суб'єктів, а й виробити адаптивні стратегії реагування в умовах обмеженої ресурсної спроможності, що є критично важливим у період післявоєнного відновлення. Таким чином, методологія оцінки ризиків і стрес-тестування за стандартами ЄС виступає не лише інструментом ідентифікації, а й механізмом стратегічного управління стійкістю на національному рівні.

Водночас ефективність стрес-тестування безпосередньо пов'язана з наявністю фінансових ресурсів для реалізації виявлених рекомендацій. Результати сценарного моделювання мають враховуватися під час формування бюджетної політики у сфері відновлення та модернізації критичної інфраструктури, що забезпечить зв'язок між оцінкою ризиків та ресурсним плануванням, відповідно до принципів середньострокового бюджетного планування.

Критична інфраструктура є сукупністю взаємопов'язаних систем, серед яких енергетичний, транспортний та цифровий сектори мають вирішальне значення для нормального функціонування

держави та суспільства. Водночас у сучасних умовах особливого значення набувають енергетика, водопостачання та цифрова інфраструктура як пріоритети стійкості, оскільки саме вони забезпечують базові потреби населення та функціонування інших секторів.

Енергетичний сектор, як один із найуразливіших, зазнав масованих атак на об'єкти генерації, передачі та розподілу електроенергії. Масовані ракетні удари призвели до масштабних перебоїв у функціонуванні електромереж, що суттєво вплинуло на життєдіяльність населення, систем охорони здоров'я, комунальних послуг та критичних державних структур. Відповідно до CER, енергетичні суб'єкти мають мати чітко визначені плани безперервності діяльності та механізми резервування мереж, що дозволяють швидко відновлювати функціонування після фізичних ушкоджень [1]. В українських реаліях такі плани були не завжди уніфіковані, що ускладнювало координацію між операторами енергосистеми різного рівня. Імплементація процедур перевірки стійкості у цій сфері дозволяє оцінити здатність енергосистеми витримувати пікові навантаження, втрату ключових вузлів та кіберінциденти, а також визначити мінімально допустимі параметри резервування потужностей. Водночас інтеграція енергетичної системи України до європейської мережі ENTSO-E посилює значення транскордонного виміру енергетичної стійкості та потребує синхронізації процедур оцінки ризиків із регіональними планами готовності до кризових ситуацій [29].

Сектор водопостачання та водовідведення є не менш критичним, оскільки безперервний доступ до питної води прямо пов'язаний із правом на життя і здоров'я, гарантованими статтею 3 Конституції України. Пошкодження систем водозабору, очисних споруд або мереж транспортування може спричинити масштабні санітарно-епідеміологічні ризики та гуманітарні кризи. У межах ризикоорієнтованого підходу цей сектор повинен підлягати обов'язковій оцінці відновлювальної спроможності та сценарному моделюванню

кризових ситуацій щодо стійкості до відключень електроенергії, забруднення джерел води, кібератак на системи автоматизованого управління та фізичних диверсій. Гармонізація із законодавством ЄС у цій частині передбачає запровадження єдиних стандартів оцінки ризиків для підприємств водопостачання, визначення мінімальних вимог до резервних систем і створення механізмів оперативного інформування населення про надзвичайні ситуації [1].

Цифрова інфраструктура, що включає телекомунікації, дата-центри, хмарні сервіси та системи управління критичними об'єктами, є основою функціонування сучасної економіки та державного управління. Кібератаки на об'єкти цифрового сектору не лише порушували безперервність надання послуг, але й мали фізичний вплив на інші сектори, зокрема енергетику та водопостачання. У цьому контексті вимоги щодо управління кіберризиками та інтеграції фізичної й цифрової стійкості набувають визначального значення [2]. Перевірка стійкості цифрової інфраструктури повинна включати тестування захищеності мереж, стійкості до DDoS-атак, сценарії компрометації даних та втрати зв'язку з резервними центрами обробки інформації. Координація цих процесів має здійснюватися з урахуванням загальних засад національної безпеки.

Особливу увагу у сучасних підходах до управління критичною інфраструктурою привертає транскордонна критична інфраструктура, функціонування якої виходить за межі однієї держави. CER наголошує, що критичні суб'єкти, розташовані поблизу кордонів або інтегровані з інфраструктурою сусідніх країн, повинні оцінюватись з урахуванням потенційного впливу на суміжні юрисдикції [1]. Взаємодія з країнами-сусідами ЄС у сфері транскордонної критичної інфраструктури передбачає розроблення механізмів обміну інформацією про ризики й інциденти, узгодження стандартів управління безперервністю діяльності, а також спільне планування реагування на загрози, що можуть поширюватися за межі одного державного

кордону. Україна, виконуючи зобов'язання у межах європейської інтеграції [8], повинна нормативно закріпити процедури взаємного визнання оцінок ризиків, синхронізувати формати звітності та забезпечити участь у спільних навчаннях і механізмах координації. Така взаємодія має здійснюватися на підставі двосторонніх або багатосторонніх угод, що визначають процедури обміну інформацією, взаємного інформування про інциденти та координації кризового реагування. Особливого значення набуває інституціоналізація контактних пунктів для оперативної взаємодії між компетентними органами держав, що відповідає вимогам CER щодо міждержавної координації [1], зокрема через механізми контактних пунктів (single points of contact). Такий механізм дозволить забезпечити своєчасний обмін інформацією про загрози, узгоджене реагування на інциденти та мінімізацію кумулятивного транскордонного ефекту.

Таким чином, секторальний аналіз та ідентифікація критичних суб'єктів у сучасних умовах повинні ґрунтуватися на поєднанні ризикоорієнтованої методології, обов'язкового стрес-тестування відповідно до статті 12 CER, урахування галузевої специфіки енергетики, водопостачання та цифрової інфраструктури, а також розвитку транскордонної координації. Саме такий комплексний підхід дозволить сформувати в Україні системну модель управління стійкістю критичної інфраструктури, синхронізовану з європейськими стандартами та адаптовану до національних викликів.

Порівняльний аналіз імплементації стандартів Directive (EU) 2022/2557 [1] у державах-членах ЄС дозволяє конкретизувати методологічні підходи до ідентифікації критичних суб'єктів та оцінки значного деструктивного ефекту, а також визначити напрями вдосконалення національної моделі. Хоча Директива встановлює уніфіковані вимоги до ризикоорієнтованої оцінки, стрес-тестування та транскордонної координації, держави ЄС реалізують ці положення з урахуванням власних правових традицій,

інституційної структури та безпекового контексту. Спільною рисою є поєднання кількісних критеріїв впливу, якісної оцінки стратегічного значення суб'єкта, обов'язковості регулярного тестування стійкості та інтеграції фізичної й кібербезпеки відповідно до Directive (EU) 2022/2555 [2]. Для оцінки ефективності запропонованих підходів доцільно звернутися до практики держав-членів ЄС, які вже завершили або перебувають на завершальному етапі імплементації Директиви CER.

Перехід від національної моделі до порівняльного аналізу дозволяє виявити універсальні та варіативні елементи регулювання, що мають значення для адаптації українського законодавства. Саме зіставлення різних моделей імплементації CER дає змогу визначити оптимальний баланс між централізацією управління та секторальною автономією.

Німецька модель (KRITIS) базується на нормативно визначених порогах значущості, закріплених у законодавстві про ІТ-безпеку та підзаконних актах [30]. Суб'єкт відноситься до критичних у разі перевищення встановлених кількісних показників — зокрема щодо обсягу обслуговуваного населення, частки ринку або обсягу виробництва / постачання. Такий підхід забезпечує високий рівень правової визначеності та мінімізує дискреційність адміністративних органів, що відповідає принципам верховенства права і пропорційності. Одночасно німецьке регулювання передбачає обов'язковість регулярних аудитів безпеки, документування заходів управління ризиками та своєчасного повідомлення про інциденти у строки, гармонізовані з вимогами NIS2 [2]. В енергетичному секторі додатково застосовується режим готовності до ризиків відповідно до Регламенту (EU) 2019/941 [31], який вимагає сценарного аналізу, транскордонних консультацій і регіональних планів реагування. Ця практика демонструє, як секторальні регламенти ЄС інтегруються з вимогами CER через механізм ризик-оцінки та стрес-тестування, формуючи

багаторівневу систему управління стійкістю. Федеральна структура Німеччини передбачає розподіл компетенції між федерацією та землями, що зумовлює багаторівневу систему координації KRITIS.

Французька модель, побудована навколо інституту "Opérateurs d'importance vitale" (OIV), закріпленого у Кодексі оборони [32], поєднує кількісні індикатори з якісною оцінкою стратегічної ролі суб'єкта для національної безпеки. На відміну від суто порогового підходу, французька система передбачає індивідуалізоване визначення обов'язків оператора з урахуванням його місця у державному управлінні та суспільних процесах. Для кожного OIV розробляються галузеві та індивідуальні плани захисту і безперервності діяльності, що підлягають періодичному тестуванню. Координація здійснюється централізовано із залученням органів безпеки, але із дотриманням процесуальних гарантій і балансу публічного інтересу та прав суб'єктів господарювання, що узгоджується з доктринальними положеннями щодо прав людини й належного врядування [13]. Водночас інтеграція фізичної та кіберстійкості відповідає вимогам CER [1] і NIS2 [2], а у випадку об'єктів подвійного призначення враховуються норми міжнародного гуманітарного права щодо захисту цивільних об'єктів та механізми відшкодування шкоди [33]. Така модель є показовою для України з огляду на потребу врахування воєнних ризиків і кумулятивного ефекту повторюваних атак. Французька модель демонструє поєднання адміністративного регулювання та елементів публічно-приватного партнерства у сфері безпеки із значною роллю державного стратегічного контролю.

Польський підхід, закріплений у Законі про кризове управління [34], репрезентує секторну модель ідентифікації з деталізацією критеріїв для енергетики, транспорту, водопостачання та цифрової інфраструктури. З огляду на схожість безпекових викликів, польський досвід є особливо релевантним для України з огляду на спільні безпекові виклики та геополітичний контекст. Практика Польщі

передбачає розроблення регіональних планів реагування, інтеграцію з Механізмом цивільного захисту ЄС [35], а також координацію транскордонних процедур у межах енергетичної та транспортної інфраструктури з урахуванням Регламенту про готовність до ризиків [31]. Нормативне забезпечення узгоджується із зобов'язаннями у межах Угоди про асоціацію [8], що передбачають поступову імплементацію acquis ЄС. Польська модель демонструє практичну реалізацію вимоги CER щодо врахування потенційного транскордонного впливу [1] через механізми взаємного інформування, спільних навчань і координації дій під час надзвичайних ситуацій.

Порівняльний аналіз свідчить, що в усіх розглянутих державах поєднуються п'ять ключових елементів: по-перше, встановлення нормативно визначених або методично обґрунтованих порогів «значного деструктивного ефекту»; по-друге, обов'язковість періодичної перевірки стійкості із застосуванням сценарного моделювання; по-третє, інтеграція фізичної та кіберстійкості в єдиній системі управління ризиками відповідно до NIS2 [2] і національного законодавства у сфері безпеки [6]; по-четверте, транскордонна координація та участь у механізмах ЄС [35]; по-п'яте, забезпечення процесуальних гарантій для операторів з урахуванням принципів законності та пропорційності. Такий підхід узгоджується зі стратегічними документами щодо стійкості та колективної безпеки, формуючи інтегровану модель публічно-правового регулювання, що формує єдину європейську модель resilience governance.

Узагальнення секторальних та порівняльних підходів свідчить, що ідентифікація критичних суб'єктів не може бути статичною процедурою, а має функціонувати як постійний процес динамічного оновлення ризикових профілів з урахуванням безпекових трансформацій.

Для України доцільним є запровадження гібридної моделі, що поєднує чітко визначені кількісні критерії (кількість населення,

яке залежить від послуг; обсяг економічних втрат; тривалість переривання; екологічні наслідки; показники кумулятивності та повторюваності атак) із ризикоорієнтованою експертною оцінкою стратегічної ролі суб'єкта з урахуванням воєнних сценаріїв і особливостей dual-use інфраструктури. Така модель забезпечить баланс між правовою визначеністю та адаптивністю, відповідатиме принципам верховенства права і позитивним зобов'язанням держави щодо захисту прав людини, а також сприятиме виконанню міжнародних зобов'язань України у межах європейської інтеграції [8]. Отже, запровадження гібридної моделі ідентифікації критичних суб'єктів, що поєднує нормативну визначеність і ризикоорієнтовану адаптивність, створює передумови для формування в Україні системної, доказової та транскордонно сумісної моделі управління стійкістю відповідно до стандартів ЄС. У довгостроковій перспективі така модель сприятиме формуванню в Україні інтегрованої системи публічного управління стійкістю, заснованої на поєднанні правової визначеності, ризик-орієнтованого підходу та міжнародної кооперації. Це відповідає сучасному розумінню функціональної державності, у межах якої ефективність публічної влади вимірюється здатністю забезпечувати безперервність суспільно значущих функцій в умовах криз та воєнних викликів [12]. Це підтверджує, що ідентифікація критичних суб'єктів є інструментом реалізації публічного інтересу як основи національної безпеки.

5. Міжнародне співробітництво, публічно-приватне партнерство та правова відповідальність

У сучасних умовах функціонування критичної інфраструктури (КІ) держави центральну роль відіграє ефективна взаємодія держави та приватного сектору. Публічно-приватне партнерство (ППП) у сфері КІ є не лише організаційно-економічним інструментом, а й стратегічним механізмом управління ризиками та забезпечення

безперервності життєво важливих послуг. Належне поєднання інституційних, фінансових та правових ресурсів держави й приватних операторів дозволяє мінімізувати наслідки природних, техногенних, кібер- та гібридних загроз, забезпечуючи реалізацію конституційних прав громадян, гарантованих Конституцією України [4].

Згідно з Directive (EU) 2022/2557 (CER) [1], оператори критичних суб'єктів мають забезпечувати системне управління ризиками, включаючи ідентифікацію загроз, оцінку їхнього впливу, розроблення заходів мінімізації ризиків, а також підтримку планів безперервності діяльності, що охоплюють фізичну та цифрову складники. CER зосереджується на комплексності підходу: оператори повинні не лише забезпечувати захист об'єктів, а й гарантувати безперервність надання життєво важливих послуг у всіх можливих кризових сценаріях, включаючи сценарії воєнного характеру. Регулярне тестування та оновлення планів безперервності діяльності є обов'язковим елементом системи управління ризиками.

В Україні Закон «Про критичну інфраструктуру» [5] визначає основні обов'язки операторів щодо забезпечення безпеки та співпраці з державними органами. Проте на практиці залишається низка прогалин: нормативно не деталізовано форми та зміст планів безперервності діяльності, критерії оцінки ризиків, строки та формат звітності про інциденти. Це створює потенційну невизначеність для операторів і потребує додаткового регламентування через підзаконні акти, методичні рекомендації та стандарти, що узгоджуються з CER і NIS2, що свідчить про необхідність підзаконної деталізації [1; 2].

Практичні кейси воєнного періоду 2022–2025 рр. засвідчили критичну важливість уніфікованих процедур: масовані ракетні удари по енергетичній інфраструктурі спричинили нерівномірність реагування між операторами через відсутність чітких вимог до планів безперервності. CER передбачає, що будь-який критичний суб'єкт має попередньо розроблені, адаптовані та протестовані

плани, що дозволяють оперативно відновити функціонування систем у разі інцидентів [1]. Відтак імплементація європейських стандартів в українському праві має забезпечити чіткі й формальні механізми відповідальності операторів за невиконання вимог, а також створити систему державного моніторингу їх виконання.

При цьому система відповідальності у сфері критичної інфраструктури повинна мати багаторівневий характер і включати адміністративну, цивільно-правовий та, у визначених законом випадках, кримінальну відповідальність. Адміністративні санкції можуть застосовуватися за порушення процедур звітності, невиконання вимог щодо оцінки ризиків або відсутність планів безперервності діяльності. Цивільно-правова відповідальність пов'язується із відшкодуванням шкоди, завданої споживачам або державі внаслідок неналежного забезпечення стійкості. Кримінально-правові механізми мають застосовуватися лише у випадках грубого порушення вимог безпеки або умисного ігнорування встановлених стандартів, що спричинило тяжкі наслідки, у тому числі загибель людей або значну шкоду довкіллю. Така градація відповідає принципу пропорційності та доктрині позитивних зобов'язань держави щодо захисту життя і безпеки, що випливають із статті 3 Конституції України [4].

Важливим є баланс між обов'язками та правами операторів. Підходи CER передбачають, що держава може накладати санкції та контрольні заходи, але вони мають бути пропорційними, передбачуваними та обґрунтованими [1]. Застосування контрольних та санкційних механізмів у сфері КІ повинно відповідати принципу пропорційності, який вимагає співмірності втручання публічної влади з легітимною метою захисту національної безпеки. Надмірне регуляторне навантаження може призвести до зниження інвестиційної активності операторів та гальмування модернізаційних процесів. Водночас недостатність контролю створює ризики системної вразливості. Отже, законодавче врегулювання має забезпечувати

баланс між безпекою та свободою підприємницької діяльності. В Україні цей аспект потребує чіткого врегулювання, щоб не порушувати економічні свободи та інші права суб'єктів господарювання, гарантовані Конституцією України [4] та національними законами. У сучасній доктрині публічного права стійкість критичної інфраструктури розглядається як елемент позитивного зобов'язання держави щодо забезпечення безпеки людини та суспільства [10; 13]. Гармонізація із правом ЄС має здійснюватися з урахуванням принципів правової визначеності та належного врядування. Водночас імплементація відповідних норм має здійснюватися з урахуванням принципу належного врядування, що передбачає прозорість процедур, передбачуваність рішень та ефективність адміністративного контролю. Водночас механізми державного нагляду повинні передбачати процесуальні гарантії для операторів, включаючи право на участь у перевірках, доступ до матеріалів контролю, можливість подання заперечень та судового оскарження рішень органів контролю. Запровадження таких гарантій забезпечує відповідність регулювання стандартам верховенства права та зміцнює довіру між державою й приватним сектором.

ППП виступає ключовим механізмом стимулювання інвестицій у модернізацію критичної інфраструктури. У CER держави мають сприяти фінансовій стабільності операторів та модернізації систем через податкові пільги, цільові гранти, кредитні програми та гарантії [1]. Такі механізми дозволяють оператору інвестувати у заходи підвищення стійкості, розробку та тестування планів безперервності діяльності, модернізацію кіберзахисту та фізичного захисту.

В Україні, окрім загальних державних програм розвитку стратегічних секторів, відсутні комплексні механізми фінансового стимулювання підвищення стійкості критичної інфраструктури відповідно до CER. Для досягнення високого рівня

відповідності європейським стандартам доцільно впровадити такі інструменти [19]:

— цільові фонди стійкості для фінансування проєктів з управління ризиками;

— державні гарантії та кредитні лінії для приватних операторів, що модернізують системи захисту;

— податкові пільги на інвестиції в технології безперервності та кіберзахисту;

— державно-приватні консорціуми для реалізації проєктів критичного значення, що включають спільне планування та обмін інформацією.

Ефективність таких інструментів значною мірою залежить від нормативної визначеності процедур відбору проєктів, прозорості використання коштів та системи парламентського й аудиторського контролю. Інституціоналізація цільових фондів стійкості з чітким правовим режимом використання ресурсів дозволить мінімізувати корупційні ризики та забезпечити довгострокову сталість інвестиційних програм, відповідно до стандартів публічних фінансів ЄС [5; 19].

Залучення держави в цю сферу забезпечує баланс між ефективністю економічної діяльності та національною безпекою, стимулює інновації та дозволяє інтегрувати найкращі міжнародні практики в національне законодавство.

Особливого значення набуває транскордонна взаємодія у сфері КІ. Україна є складником східного сегмента європейської інфраструктурної мережі, оскільки її енергетичні, транспортні та цифрові системи інтегровані з інфраструктурою держав-членів ЄС. Після синхронізації енергосистеми України з Європейською мережею операторів систем передачі електроенергії (ENTSO-E) [29] та розширення транспортних коридорів до країн ЄС питання стійкості української КІ стало елементом загальноєвропейської безпеки. У цьому контексті транскордонна взаємодія повинна включати: узгодження стандартів

управління ризиками; спільні протоколи реагування на інциденти; обмін інформацією про загрози; проведення спільних навчань і стрес-тестів. Такий підхід відповідає логіці CER і NIS2 щодо координації на рівні ЄС [1; 2]. Порівняльний аналіз законодавства держав-членів ЄС засвідчує, що ефективність правового регулювання у сфері КІ забезпечується через деталізацію статусу операторів та запровадження чітких механізмів контролю. Зокрема, у Німеччині відповідні положення конкретизовані в IT-Sicherheitsgesetz 2.0 [30], що встановлює обов'язковість аудиту та повідомлення про інциденти. У Франції норми Code de la défense щодо операторів життєво важливого значення передбачають спеціальний режим державного нагляду та координації [32]. У Польщі Ustawa o zarządzaniu kryzysowym закріплює системний підхід до управління кризами із чітким розподілом компетенції між органами влади та операторами [34]. Порівняльний досвід свідчить, що законодавча деталізація знижує правову невизначеність та підвищує ефективність реагування та зменшує регуляторні ризики.

Механізми відшкодування збитків, завданих КІ внаслідок збройної агресії, мають комплексний міжнародно-правовий характер. Вони ґрунтуються на принципі відповідальності держави за міжнародно-протиправні діяння, нормах міжнародного гуманітарного права щодо захисту цивільної інфраструктури, а також механізмах міжнародних компенсацій. Реалізація такого підходу передбачає як індивідуалізацію шкоди конкретним об'єктам КІ, так і формування консолідованої доказової бази на міждержавному рівні. Створення міжнародного Реєстру збитків, завданих агресією проти України, та обговорення спеціального компенсаційного механізму формують правову основу для майбутнього відшкодування шкоди об'єктам КІ [8]. У цьому контексті інтеграція критеріїв оцінки шкоди відповідно до стандартів ЄС дозволяє документувати наслідки руйнування об'єктів КІ та обґрунтовувати міжнародні позови. Водночас формування єдиної методики документування шкоди об'єктам

критичної інфраструктури відповідно до стандартів ЄС і міжнародного права має ключове значення для доведення причинно-наслідкового зв'язку між актом агресії та конкретними матеріальними втратами. Гармонізація критеріїв оцінки шкоди з європейськими підходами підвищує доказову силу таких матеріалів у міжнародних юрисдикційних інституціях.

Роль НАТО та ЄС у забезпеченні фізичної безпеки об'єктів КІ в Східній Європі є системоутворюючою. НАТО розглядає захист критичної інфраструктури як елемент колективної безпеки та стійкості (resilience) як базового принципу [36], приділяючи особливу увагу захисту енергетичних мереж, транспортних вузлів і цифрових систем від гібридних загроз. Європейський Союз, своєю чергою, розвиває механізми цивільного захисту, координації кризового реагування та фінансування відновлення пошкоджених об'єктів КІ через відповідні фонди та інструменти [37]. Для України співпраця з НАТО та ЄС означає доступ до спільних стандартів безпеки, навчальних програм, технічної допомоги та механізмів стратегічної координації, що посилює фізичний захист об'єктів КІ та інтегрує національну систему безпеки до ширшого євроатлантичного простору.

Український кейс свідчить, що інтеграція національного законодавства із CER [1] і NIS2 [2] дозволяє формувати чіткі критерії оцінки шкоди, процедурні алгоритми реагування та координацію із міжнародними партнерами. Це створює правову основу для притягнення до відповідальності не лише національних операторів, а й держав або неурядових суб'єктів у разі порушень міжнародного права.

Отже, міжнародне співробітництво та публічно-приватне партнерство у сфері критичної інфраструктури формують єдину систему багаторівневої відповідальності, що передбачає: а) формування чітких обов'язків операторів; б) законодавче закріплення механізмів стимулювання інвестицій; в) інтеграцію фізичного та кіберзахисту; г) розвиток транскордонної взаємодії України

як складник європейської інфраструктурної мережі; ґ) визначення міжнародно-правових процедур відшкодування збитків і притягнення до відповідальності; д) посилення співпраці з НАТО та ЄС у сфері фізичної безпеки КІ.

Таке комплексне регулювання створює передумови для стабільного функціонування критичних систем навіть в умовах воєнних та гібридних викликів, забезпечуючи реалізацію конституційного пріоритету безпеки людини [4], відповідність міжнародним стандартам та зобов'язанням України щодо євроінтеграції [1; 2].

У концептуальному вимірі така модель поєднує функції превенції, реагування та відновлення, формуючи інтегровану систему багаторівневої відповідальності держави, операторів і міжнародних партнерів. Стійкість критичної інфраструктури в цьому контексті виступає не лише елементом безпекової політики, а й складником конституційного обов'язку держави забезпечувати належні умови для реалізації прав і свобод людини. Таким чином, публічно-приватне партнерство та міжнародна координація виступають інструментами реалізації публічного інтересу як фундаменту національної безпеки України.

6. Висновки

Дослідження показало, що стійкість критичної інфраструктури є міжгалузевою правовою категорією, яка поєднує конституційно-правові, адміністративно-правові, безпекові та європейсько-правові елементи. Вона безпосередньо пов'язана із забезпеченням і гарантуванням фундаментальних прав людини — права на життя, безпеку, охорону здоров'я, доступ до енергії, води, транспорту та цифрових послуг, що випливають із положень Конституції України [4] та доктринальних підходів національної правової науки [10; 13]. Європейський правовий простір, сформований на засадах прав людини, демократії та верховенства права, зумовлює

необхідність гармонізації українського законодавства із сучасними стандартами захисту критичних сервісів.

У цьому контексті стійкість критичної інфраструктури набуває ознак функціонального конституційно-правового принципу, що конкретизує позитивні зобов'язання держави щодо забезпечення належних умов життя людини. Вона виступає функціональним критерієм оцінки ефективності публічної влади, оскільки саме здатність гарантувати безперервність життєво важливих сервісів у кризових умовах визначає реальний зміст соціальної та правової держави, відповідно до статті 1 Конституції України [4].

У результаті дослідження обґрунтовано, що стійкість критичної інфраструктури повинна розглядатися не лише як об'єкт охоронного регулювання, а як відносно самостійний принцип публічного управління, що інтегрує превентивні, координаційні та відновлювальні механізми правового впливу. Запропоновано трактувати її як багаторівневу систему позитивних зобов'язань держави, спрямованих на гарантування безперервності життєво важливих сервісів в умовах воєнних і гібридних загроз.

Аналіз положень Directive (EU) 2022/2557 [1] засвідчив перехід від концепції охорони об'єктів до концепції стійкості сервісів, що орієнтована на забезпечення безперервності функціонування життєво важливих послуг навіть у кризових умовах. У взаємодії з Directive (EU) 2022/2555 [2] формується інтегрована модель фізичної та кіберстійкості, яка передбачає обов'язкову оцінку ризиків, планування безперервності діяльності, запровадження стандартів реагування на інциденти та транскордонну координацію. В українському праві відповідні підходи імплементуються через Закон України «Про критичну інфраструктуру» [5], однак потребують подальшої деталізації критеріїв «значного деструктивного ефекту», стандартизації планів безперервності та врегулювання процедур обміну інформацією з інституціями ЄС. Подальший розвиток національної моделі

потребує кодифікаційної систематизації підзаконних актів, що регулюють категоризацію об'єктів КІ, порядок ведення реєстрів та механізми координації між секторальними регуляторами, відповідно до принципу правової визначеності. Уніфікація таких процедур дозволить уникнути фрагментарності правового регулювання та забезпечить прозорість управлінських рішень у сфері стійкості.

Секторальний аналіз подій 2022–2025 років в умовах правового режиму воєнного стану продемонстрував особливу вразливість енергетичного, транспортного й цифрового секторів до комплексних гібридних загроз. Масовані ракетні удари по енергетичній інфраструктурі та системні кібератаки підтвердили, що відсутність уніфікованих вимог до планів безперервності й управління кіберризиками знижує ефективність реагування та створює ризики порушення базових соціальних прав громадян, гарантованих Конституцією України [4]. Практичний досвід воєнного періоду довів необхідність запровадження єдиних стандартів оцінки ризиків, регулярного тестування кризових сценаріїв і централізованого моніторингу стану критичних сервісів. Воєнний досвід також продемонстрував необхідність переходу від реактивної моделі управління до проактивної, що передбачає стратегічне прогнозування ризиків, сценарне моделювання та довгострокове планування резервних спроможностей. Такий підхід відповідає сучасним стандартам ЄС щодо інтегрованої оцінки загроз і формує основу для системної модернізації секторів КІ.

Публічно-приватне партнерство визначено одним із системоутворюючих механізмів забезпечення стійкості. Обов'язки операторів критичної інфраструктури мають охоплювати комплексну ідентифікацію ризиків, розробку та оновлення планів захисту, впровадження технічних і організаційних заходів безпеки, а також своєчасне інформування про інциденти. Водночас держава повинна забезпечити передбачувані та пропорційні механізми контролю, відповідно до принципу верховенства права, фінансові стимули,

страхування ризиків і підтримку модернізації. У цьому контексті значення мають інструменти ЄС, зокрема механізми енергетичної готовності та солідарності, закріплені в Regulation (EU) 2019/941 [31], а також програми відновлення та стійкості, передбачені Regulation (EU) 2021/241 [37].

Транскордонний вимір стійкості набуває стратегічного значення з огляду на роль України як складника східного сегмента європейської інфраструктурної мережі. Інтеграція до енергетичних, транспортних та цифрових систем ЄС передбачає гармонізацію процедур реагування, участь у механізмах цивільного захисту та координацію в межах спільних платформ обміну інформацією [35]. Важливу роль у цьому процесі відіграють положення Association Agreement between the European Union and Ukraine [8], які формують правову основу для адаптації українських стандартів до acquis ЄС та розвитку спільної політики безпеки.

Механізми відшкодування збитків, завданих критичній інфраструктурі внаслідок збройної агресії, ґрунтуються на нормах міжнародного гуманітарного права та принципах міжнародної відповідальності держав. Положення Женевські конвенції 1949 року [33] та Додаткового протоколу I (1977) [38] до Женевських конвенцій встановлюють заборону атак на цивільні об'єкти та інфраструктуру, необхідну для виживання населення. Загальні принципи відповідальності закріплено в Articles on Responsibility of States for Internationally Wrongful Acts [27], що створює правові підстави для міжнародних позовів і компенсаційних механізмів. Важливим елементом є функціонування Реєстру збитків, створеного під егідою Council of Europe [39], який документує шкоду та формує основу для майбутнього відшкодування. Систематизація доказової бази щодо руйнування об'єктів КІ має не лише компенсаційне, а й превентивне значення, оскільки формує міжнародно-правові механізми стримування майбутніх порушень. У цьому вимірі стійкість

критичної інфраструктури інтегрується до ширшої концепції міжнародної безпеки та захисту цивільного населення.

Безпекова координація на регіональному рівні пов'язана з діяльністю NATO, що розвиває політику стійкості та захисту критичної інфраструктури, а також із механізмами цивільного захисту Європейського Союзу [36]. Їхня діяльність сприяє зміцненню фізичної безпеки об'єктів КІ у Східній Європі, розвитку спільних стандартів реагування та підвищенню рівня колективної безпеки та стійкості (resilience) [35].

Інституційна ефективність національної системи залежить від належної координації між уповноваженими органами, зокрема відповідно до законів України у сфері національної безпеки та кібербезпеки з урахуванням міжвідомчої взаємодії, а також від забезпечення балансу між вимогами безпеки та гарантіями прав людини, визначених у Конституції України [4].

Перспективи подальшого розвитку правового регулювання у цій сфері пов'язані з формуванням довгострокової стратегії стійкості, що поєднуватиме нормативну стабільність з адаптивністю до нових викликів безпекового середовища. Комплексна реалізація стратегічних документів щодо стійкості України до 2030 року має поєднувати імплементацію стандартів ЄС, розвиток публічно-приватного партнерства, фінансові механізми підтримки, транскордонну взаємодію, міжнародно-правові інструменти відповідальності та інтеграцію фізичної й кіберстійкості в єдину систему національної безпеки.

Такий підхід формує цілісну модель захисту критичної інфраструктури, що відповідає європейським зобов'язанням України, у межах євроінтеграційного процесу, та сприяє довгостроковій стабільності держави. Таким чином, стійкість критичної інфраструктури постає як системна категорія сучасного публічного права, що поєднує національний та європейський виміри регулювання і визначає стратегічний напрям трансформації української правової системи в умовах воєнних

і післявоєнних викликів та виступає інструментом реалізації публічного інтересу як основи національної безпеки України.

Список використаних джерел:

1. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. 2022. L 333. P. 164–198. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

3. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022, затверджений Законом України № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text

4. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

5. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради України*. 2022. № 5. Ст. 37. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. Кодекс цивільного захисту України : Закон України від 02.10.2012 № 5403-VI. *Відомості Верховної Ради України*. 2013. № 34–35. Ст. 458. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text

8. Угода про асоціацію між Україною та Європейським Союзом: Міжнародний договір від 27.06.2014. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

9. Плахотнюк Р. Забезпечення стійкості критичної інфраструктури в Україні в умовах сучасних викликів. *Економічний простір*. 2024. № 195. С. 47–54. DOI: https://doi.org/10.30838/EP.195.47-54.

10. Рабінович П. М. Основи загальної теорії права та держави. Львів : Світ, 2012. 320 с.

11. Öneryıldız v. Turkey. European Court of Human Rights. Judgment of 30.11.2004 (Application no. 48939/99). URL: https://hudoc.echr.coe.int/eng?i=001-67614

12. Budayeva and Others v. Russia. European Court of Human Rights. Judgment of 20.03.2008 (Applications nos. 15339/02 et al.). URL: https://hudoc.echr.coe.int/eng?i=001-85436

13. Шемшученко Ю. С. Права людини в умовах глобалізації. Київ : Юридична думка, 2015. 512 с.

14. Шемшученко Ю. С. Теоретичні проблеми прав людини. Київ : Наукова думка, 2014. 240 с.

15. Барабаш Ю. Г. Цифрові права людини: сучасні виклики. *Право України*. 2021. № 5. С. 40–52.

16. Горбачова В. Правове забезпечення захисту та стійкості критичної інфраструктури в Європейському Союзі. *Пропілеї права та безпеки*. 2025. № 6–7. С. 67–78.

17. Directive 2008/114/EC on the identification and designation of European critical infrastructures. *Official Journal of the European Union*. 2008. L 345. P. 75–82. URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj

18. Конвенція про захист прав людини і основоположних свобод: Міжнародний договір від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

19. Українська стратегія стійкості критичної інфраструктури 2025–2030. Київ, 2025. URL: https://www.mil.gov.ua/critical-infrastructure

20. Про правовий режим воєнного стану : Закон України від 03.04.2015 № 389-VIII. *Відомості Верховної Ради України*. 2015. № 28. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

21. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

22. Про затвердження Порядку формування та ведення Реєстру об'єктів критичної інфраструктури : Постанова КМУ від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text

23. Про затвердження критеріїв віднесення об'єктів до критичної інфраструктури : Постанова КМУ від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text

24. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

25. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. *Відомості Верховної Ради України*. 2006. № 30. Ст. 258. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

26. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

27. Articles on Responsibility of States for Internationally Wrongful Acts. *Yearbook of the International Law Commission*. 2001. Vol. II, Part Two. URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

28. Бюджетний кодекс України : Закон України від 08.07.2010 № 2456-VI. *Відомості Верховної Ради України*. 2010. № 46–47. Ст. 401. URL: https://zakon.rada.gov.ua/laws/show/2456-17#Text

29. ENTSO-E. Ukraine's integration into the European electricity network and regional crisis preparedness plans (analytical material). URL: https://www.entsoe.eu/news/ukraine-integration/

30. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021. Bundesgesetzblatt I. 2021. S. 1122–1154.

31. Regulation (EU) 2019/941 on risk-preparedness in the electricity sector. *Official Journal of the European Union*. 2019. L 158. P. 1–21. URL: https://eur-lex.europa.eu/eli/reg/2019/941/oj

32. Code de la défense (France). Partie L. 1332-1 et seq. URL: https://www.legifrance.gouv.fr

33. Geneva Conventions of 12 August 1949. *United Nations Treaty Series*. Vol. 75. 1950. P. 31–287. URL: https://ihl-databases.icrc.org

34. Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. *Dziennik Ustaw*. 2007. Nr 89 poz. 590. URL: https://isap.sejm.gov.pl

35. Regulation (EU) 2021/836 amending the Union Civil Protection Mechanism. *Official Journal of the European Union*. 2021. L 185. P. 1–13. URL: https://eur-lex.europa.eu/eli/reg/2021/836/oj

36. NATO. Resilience and Critical Infrastructure Protection Policy Documents. Brussels, n.d. URL: https://www.nato.int

37. Regulation (EU) 2021/241 establishing the Recovery and Resilience Facility. *Official Journal of the European Union*. 2021. L 57. P. 17–75. URL: https://eur-lex.europa.eu/eli/reg/2021/241/oj

38. Додатковий протокол I до Женевських конвенцій: Міжнародний договір від 08.06.1977. URL: https://zakon.rada.gov.ua/laws/show/995_221#Text

39. Council of Europe. Register of Damage Caused by the Aggression of the Russian Federation against Ukraine. 2023. URL: https://www.coe.int/en/web/rd4u

References:

1. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. 2022. L 333. Pp. 164–198. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2557/oj (in English).

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official*

Journal of the European Union. 2022. L 333. Pp. 80–152. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj (in English).

3. On the Introduction of Martial Law in Ukraine : Decree of the President of Ukraine of 24 February 2022 No. 64/2022, approved by Law of Ukraine No. 2102-IX. Retrieved from https://zakon.rada.gov.ua/laws/show/64/2022#Text (in Ukrainian).

4. Constitution of Ukraine: Law of Ukraine of 28 June 1996 No. 254k/96-VR. *Bulletin of the Verkhovna Rada of Ukraine*. 1996. No. 30. Art. 141. Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (in Ukrainian).

5. On Critical Infrastructure: Law of Ukraine of 16 November 2021 No. 1882-IX. *Bulletin of the Verkhovna Rada of Ukraine*. 2022. No. 5. Art. 37. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text (in Ukrainian).

6. On the Basic Principles of Cybersecurity of Ukraine: Law of Ukraine of 5 October 2017 No. 2163-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2017. No. 45. Art. 403. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).

7. Civil Protection Code of Ukraine: Law of Ukraine of 2 October 2012 No. 5403-VI. *Bulletin of the Verkhovna Rada of Ukraine*. 2013. No. 34–35. Art. 458. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text (in Ukrainian).

8. Association Agreement between Ukraine and the European Union: International Treaty of 27 June 2014. Retrieved from https://zakon.rada.gov.ua/laws/show/984_011#Text (in Ukrainian).

9. Plakhotniuk, R. Ensuring the resilience of critical infrastructure in Ukraine under modern challenges. *Economic Space*. 2024. No. 195. Pp. 47–54. DOI: https://doi.org/10.30838/EP.195.47-54 (in Ukrainian).

10. Rabinovych, P. M. Fundamentals of General Theory of Law and State. Lviv: Svit, 2012. 320 p. (in Ukrainian).

11. Öneryıldız v. Turkey. European Court of Human Rights. Judgment of 30 November 2004 (Application no. 48939/99). Retrieved from https://hudoc.echr.coe.int (in English).

12. Budayeva and Others v. Russia. European Court of Human Rights. Judgment of 20 March 2008 (Applications nos. 15339/02 et al.). Retrieved from https://hudoc.echr.coe.int (in English).

13. Shemshuchenko, Yu. S. Human Rights in the Context of Globalization. Kyiv : Yurydychna Dumka, 2015. 512 p. (in Ukrainian).

14. Shemshuchenko, Yu. S. Theoretical Problems of Human Rights. Kyiv : Naukova Dumka, 2014. 240 p. (in Ukrainian).

15. Barabash, Yu. H. Digital human rights: modern challenges. *Law of Ukraine*. 2021. No. 5. Pp. 40–52 (in Ukrainian).

16. Horbachova, V. Legal support for the protection and resilience of critical infrastructure in the European Union. *Propylei of Law and Security*. 2025. No. 6–7. Pp. 67–78 (in Ukrainian).

17. Directive 2008/114/EC on the identification and designation of European critical infrastructures. *Official Journal of the European Union*. 2008. L 345. Pp. 75–82. Retrieved from https://eur-lex.europa.eu/eli/dir/2008/114/oj (in English).

18. Convention for the Protection of Human Rights and Fundamental Freedoms: International Treaty of 4 November 1950. Retrieved from https://zakon.rada.gov.ua/laws/show/995_004#Text (in Ukrainian).

19. Ukraine's Critical Infrastructure Resilience Strategy 2025–2030. Kyiv, 2025. Retrieved from https://www.mil.gov.ua (in Ukrainian).

20. On the Legal Regime of Martial Law: Law of Ukraine of 3 April 2015 No. 389-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2015. No. 28. Art. 131. Retrieved from https://zakon.rada.gov.ua/laws/show/389-19#Text (in Ukrainian).

21. On National Security of Ukraine : Law of Ukraine of 21 June 2018 No. 2469-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2018. No. 31. Art. 241. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text (in Ukrainian).

22. On Approval of the Procedure for the Formation and Maintenance of the Register of Critical Infrastructure Facilities: Resolution of the Cabinet of Ministers of Ukraine of 28 April 2023 No. 415. Retrieved from https://zakon.rada.gov.ua/laws/show/415-2023-п#Text (in Ukrainian).

23. On Approval of Criteria for Classifying Objects as Critical Infrastructure: Resolution of the Cabinet of Ministers of Ukraine of 9 October 2020 No. 1109. Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text (in Ukrainian).

24. On the National Coordination Center for Cybersecurity: Decree of the President of Ukraine of 7 June 2016 No. 242/2016. Retrieved from https://zakon.rada.gov.ua/laws/show/242/2016#Text (in Ukrainian).

25. On the State Service for Special Communications and Information Protection of Ukraine: Law of Ukraine of 23 February 2006 No. 3475-IV. *Bulletin of the Verkhovna Rada of Ukraine*. 2006. No. 30. Art. 258. Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text (in Ukrainian).

26. On the Security Service of Ukraine: Law of Ukraine of 25 March 1992 No. 2229-XII. *Bulletin of the Verkhovna Rada of Ukraine*. 1992. No. 27. Art. 382. Retrieved from https://zakon.rada.gov.ua/laws/show/2229-12#Text (in Ukrainian).

27. Articles on Responsibility of States for Internationally Wrongful Acts. *Yearbook of the International Law Commission*. 2001. Vol. II, Part Two. Retrieved from https://legal.un.org (in English).

28. Budget Code of Ukraine: Law of Ukraine of 8 July 2010 No. 2456-VI. *Bulletin of the Verkhovna Rada of Ukraine*. 2010. No. 46–47. Art. 401. Retrieved fromhttps://zakon.rada.gov.ua/laws/show/2456-17#Text (in Ukrainian).

29. ENTSO-E. Ukraine's integration into the European electricity network and regional crisis preparedness plans. Retrieved from https://www.entsoe.eu (in English).

30. Second Act on Increasing the Security of Information Technology Systems (IT Security Act 2.0) of 18 May 2021. Bundesgesetzblatt I. 2021. Pp. 1122–1154 (in German).

31. Regulation (EU) 2019/941 on risk-preparedness in the electricity sector. *Official Journal of the European Union*. 2019. L 158. Pp. 1–21. Retrieved from https://eur-lex.europa.eu (in English).

32. Defence Code (France). Partie L. 1332-1 et seq. Retrieved from https://www.legifrance.gouv.fr (in French).

33. Geneva Conventions of 12 August 1949. *United Nations Treaty Series*. 1950. Vol. 75. Pp. 31–287. Retrieved from https://ihl-databases.icrc.org (in English).

34. Act on Crisis Management of 26 April 2007. Dziennik Ustaw. 2007. No. 89. Item 590. Retrieved from https://isap.sejm.gov.pl (in Polish).

35. Regulation (EU) 2021/836 amending the Union Civil Protection Mechanism. Official Journal of the European Union. 2021. L 185. Pp. 1–13. Retrieved from https://eur-lex.europa.eu (in English).

36. NATO. Resilience and Critical Infrastructure Protection Policy Documents. Brussels, n.d. Retrieved from https://www.nato.int (in English).

37. Regulation (EU) 2021/241 establishing the Recovery and Resilience Facility. *Official Journal of the European Union*. 2021. L 57. Pp. 17–75. Retrieved from https://eur-lex.europa.eu (in English).

38. Additional Protocol I to the Geneva Conventions of 12 August 1949: International Treaty of 8 June 1977. Retrieved from https://zakon.rada.gov.ua/laws/show/995_221#Text (in Ukrainian).

39. Council of Europe. Register of Damage Caused by the Aggression of the Russian Federation against Ukraine. 2023. URL: https://www.coe.int/en/web/rd4u (in English).

ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ УНІТАРИЗМУ: ВІТЧИЗНЯНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД

PROBLEMS AND PROSPECTS OF THE DEVELOPMENT OF UNITARISM: DOMESTIC AND FOREIGN EXPERIENCE

Shatilo V. A.,
Doctor of Science of Law, Professor,
Head of the Department of Constitutional
and Administrative Law,
National Transport University,
Kyiv, Ukraine

Abstract. The section of V. Shatilo monograph "Problems and Prospects for the Development of Unitarism: Domestic and Foreign Experience" explores the phenomenon of unitarism as a constitutional and legal category, its essence, functions and challenges in the conditions of modern socio-political processes. The author emphasizes that the territory and its integrity are the basic feature of statehood, and unitarism acts as an integrating factor for Ukraine, which historically did not have the prerequisites for federalization. The Constitution of Ukraine enshrines the principles of unity and indivisibility of the state territory, a combination of centralization and decentralization, and balanced development of regions taking into account historical, cultural and ethnic characteristics.

Particular attention is paid to discussions on federalization, which periodically arose in Ukrainian society, but after 2014 acquired

a dangerous political connotation that threatens the territorial integrity of the state. The author cites the position of the retired judge of the Constitutional Court of Ukraine V. Campo, who considers federalization to be political speculation without legal grounds. In this context, the development of the territorial system is possible only within the framework of a unitary model.

The monograph analyzes unitarism as a multifaceted concept that goes beyond constitutional law and encompasses municipal studies, regional studies, and global studies. O. Batanov even proposes the separation of an interdisciplinary science — "unitaristics," which would systematize knowledge about the territory, its political models, and social significance. Unitarism is considered as a principle of constitutional order, a form of state structure, a way of life, a basic value, and a principle of territorial governance. It ensures the concentration of power and finances at the state level, while allowing for decentralization processes.

The author emphasizes that unitarism as a constitutional value has an axiological dimension, forming worldviews about the political and territorial structure of the state. It correlates with general legal values enshrined in the Constitution of Ukraine, such as life, dignity, freedom, democracy, sovereignty and territorial integrity. At the same time, unitarism is not a universal category, because the political and territorial organization allows for variability — from unitarism to federalism.

Among the current challenges of unitarism in Ukraine are: finding a balance between local self-government and central government, continuing the decentralization reform in the context of European integration, as well as the problems of martial law and reintegration of temporarily occupied territories. The author concludes that unitarism remains a key principle of the constitutional order of Ukraine, which ensures the unity of the state and its stability in difficult political and social conditions.

Keywords: Unitarism, State Structure, Decentralization of Power, Comparative Legal Experience, Public Administration, Constitutional Development.

1. Вступ

Наявність території — простору, на який поширюється суверенітет держави, є однією з основних ознак держави. Впорядкування території здійснюється шляхом встановлення певного територіального устрою — регламентованої національним законодавством територіальної організації держави з метою забезпечення найбільш оптимального вирішення завдань та здійснення функцій суспільства і держави [1, с. 42].

Згідно з ч. 2 ст. 2 Конституції України Україна є унітарною державою (від лат. "unitas" — «єдність», «цілісність»), тобто державою, в якій адміністративно-територіальні одиниці (частини території держави), виокремлені юридично та організаційно для виконання завдань державної влади, і які не мають статусу державних утворень [1, с. 213–213; 2]. Засади територіального устрою України, як унітарної держави, визначені у ст. 132 Конституції України, згідно з якою територіальний устрій України ґрунтується на засадах єдності та цілісності державної території, поєднанні централізації і децентралізації у здійсненні державної влади, збалансованості і соціально-економічного розвитку регіонів, з урахуванням їх історичних, економічних, екологічних, географічних і демографічних особливостей, етнічних і культурних традицій [2].

Незважаючи на те, що в українському суспільстві на різних етапах його розвитку порушувалось питання про федералізацію, здебільшого в контексті політичних чинників, слід визнати, що в Україні відсутні історичні передумови такої форми державного устрою. Зокрема, до історичних передумов федералізації належить поступове формування національно-територіальних утворень.

Протягом тривалого історичного періоду, від Київської Русі до перебування України земель у складі іноземних імперій та СРСР, на українські землі поширювався територіальний устрій відповідного державного утворення. Тому унітаризм для українських земель передусім здійснює інтегруючу функцію.

Крім цього, в контексті ст. 157 Конституції України виникає питання розмежування між курсом на федералізацію та потенційним порушенням територіальної цілісності України як єдності, неподільності та автономності території України.

Проте після 2014 року будь-яка тенденція до федералізації видається потенційно небезпечною для України не лише як для унітарної держави, а й як для держави взагалі. Тому немає підстав не погоджуватись з думкою В. Кампо, судді Конституційного Суду України у відставці: «Сьогоднішня ідея федералізації має чисто політичний і спекулятивний підтекст. З правової точки зору передумов для федералізації немає, тим більше виникає серйозна загроза територіальній цілісності України. Адже не зупиняються розмови за кордоном, в деяких навіть країнах Європейського Союзу, за відторгнення в України частини її території. Зокрема окремі партії в сусідніх країнах ЄС вимагають відторгнення від України Закарпаття, Буковини, частини Одеської області. Тому, звичайно, з федералізацією в цих умовах виступати це дуже небезпечно» [3].

Виходячи з викладеного, розвиток та вдосконалення територіального устрою в Україні можливий лише в рамках унітарної держави.

Нині основні виклики унітаризму зумовлені внутрішніми та зовнішніми чинниками. До перших слід віднести продовження пошуку оптимального балансу між органами місцевого самоврядування та органами центральної влади в умовах децентралізації, продовження реформи децентралізації в умовах євроінтеграційних процесів, до других — воєнний стан і необхідність концептуальної

розробки нормативно-правового забезпечення реінтеграційних процесів тимчасово окупованих територій.

Унітаризм та його окремі аспекти неодноразово становили предмет досліджень науковців, серед яких В. О. Антонов, М. О. Баймуратов, О. В. Батанов, І. Е. Берестова, Н. В. Воротіна, Б. П. Гдичинський, В. П. Горбатенко, Р. В. Губань, О. П. Іщенко, В. М. Кампо, О. А. Колодій, О. Л. Копиленко, Т. А. Костецька, І. О. Кресіна, А. Р. Крусян, В. С. Куйбіда, О. Ю. Курцев, І. Й. Магновський, Н. Л. Омельченко, М. О. Пухтинський, О. В. Скрипнюк, Т. М. Слінько, С. О. Телешун, А. Ф. Ткачук, В. М. Шаповал, Ю. С. Шемшученко, В. А. Явір та інші.

Проте, незважаючи на значну кількість наукових публікацій, окремі аспекти вітчизняного та зарубіжного досвіду унітаризму висвітлені недостатньо, що, на нашу думку, пов'язано зі складнощами суспільних процесів, за яких відбувається розвиток унітаризму в Україні у контексті одночасних процесів євроінтеграції та особливостей воєнного стану.

2. Унітаризм як конституційно-правовий феномен та поняття у конституційному праві

Терміни і поняття є основними інструментами наукових досліджень. Кожна наука характеризується наявністю понятійно-термінологічного апарату — сукупності понять та відповідних їхньому змісту термінів. У тлумачному словнику української мови слово «термін» (від лат. "terminus", тобто «межа», «закінчення») має декілька значень, одне з яких пов'язане з визначеним проміжком часу, а друге означає слово або словосполучення, яке характеризує певний вислів або є «чітко окресленим спеціальним поняттям будь-якої галузі науки, техніки, мистецтва, суспільного життя тощо» [4]. Р. В Стацюк, узагальнюючи визначення терміну, наводить такі його ознаки: 1) точність; 2) дефінітивність;

3) системність; 4) номінативність; 5) стилістична нейтральність; 6) мотивованість [5, с. 115].

Ці ознаки повною мірою є притаманними і юридичним термінам, які становлять одиниці термінологічної системи права. Юридичний термін — це слово або словосполучення, що виражає поняття з правової сфери суспільного життя і має визначення (дефініцію) у юридичній літературі (законодавчих актах, юридичних словниках, науково-правових працях) [6, с. 1].

«Термін» та «поняття» не є тотожними. «Поняття», будучи формою мислення, становить спосіб відображення дійсності, за якого предмет розкривається через сукупність його суттєвих ознак [7, с. 1]. Тому юридичний термін є способом вираження юридичного поняття.

І хоча багато юридичних термінів має нормативно-правове визначення, при цьому, як зазначає Н. В. Артикуца, «термін, який створюється і функціонує у правовій науці, може не фіксуватися в законах, а мати власне науковий характер». У науковій літературі, яка віддзеркалює процес формування правового знання, такий юридичний термін може мати декілька наукових дефініцій, які презентують різні наукові підходи і школи, різні аспекти вивчення одного й того ж правового поняття [6, с. 1].

В цьому контексті унітаризм потрібно розглядати з позицій поняття, так як термін «унітаризм» наразі не є усталеним в українському конституційному праві. На нашу думку, слід погодитись з О. Батановим, який акцентує увагу на тому, що «таким поняттям, що і на сьогодні ще не стало загальновизнаним та залишається малозрозумілим з погляду сутності, змісту, принципів та функцій, є «унітаризм», яке використовується у наукових працях з питань конституційного права вкрай рідко» [8, с. 21].

Разом з тим, як зазначає науковець, унітаризм як принцип конституційного ладу, форма державного устрою, філософія державності та права є універсальним інструментом розв'язання протиріч

між центром та місцями, тенденціями централізації та децентралізації всередині відповідної унітарної держави [8, с. 22]. Тлумачення унітаризму виключно як «принципу державного устрою» та/або «одну з форм державного устрою», обґрунтовує О. Батанов, є ключовою теоретичною проблемою визначення суті унітаризму, хоча б з тих міркувань, що унітаризм є міждисциплінарним поняттям, значення якого виходить за межі конституційного права, охоплюючи проблеми наук [8, с. 25]:

1) муніципалістики — щодо ролі та значення території у процесах формування місцевого самоврядування, об'єднання територіальних громад, зіставлення адміністративно-територіального та муніципально-територіального устрою, інші питання, які відіграють суттєву роль у процесах демократизації на місцях та зміцнення територіальної цілісності держави [8, с. 28];

2) регіоналістики — щодо об'єктивних процесів регіоналізації (географічної, історичної, політичної, економічної, культурної) [8, с. 29];

3) глобалістики — щодо сутності, тенденцій та причин процесів глобалізації, інших глобальних процесів і проблем, пошук шляхів утвердження позитивних і подолання негативних для людини та біосфери наслідків цих процесів [8, с. 29].

З огляду на це науковець порушує питання про виокремлення міждисциплінарної науки — унітаристики, яка акумулювала б знання про територію, її політичні моделі, функціональну роль та соціальне значення, вплив економічних, управлінських, історичних, етнонаціональних, географічних, кліматичних, інфраструктурних та інших чинників на її функціонування [8, с. 27].

Під цим кутом багатогранність унітаризму дає змогу розглядати його конституційно-правовий феномен, який можна розглядати у таких аспектах:

1) як принцип конституційного ладу [9, с. 132];

2) як форма державного устрою [10, с. 31];

3) як спосіб життя, що поєднує територіальну єдність й невіддільність у конституційних відносинах різних форм державності — від централізованих до децентралізованих, деконцентрованих, регіональних держав і місцевого самоврядування [11, с. 88];

4) як базова цінність конституційного ладу [12, с. 17];

5) як принцип територіального управління (В. В. Міщук) та принцип територіального устрою (Т. М. Слінько, Л. І. Летнянчин, Ф. В. Веніславський) [16, с. 18].

Хоча у науковій літературі відсутнє єдине визначення поняття конституційного ладу, його можна розглядати як сукупність основоположних правовідносин, закріплених у Конституції відповідної держави, що наділені найвищим ступенем юридичної жорсткості, тобто убезпечені від скасування чи змін. Традиційно термін «конституційний лад» пов'язаний з тими положеннями Конституції, зміни до яких можуть бути прийняті лише шляхом всеукраїнського референдуму. Зокрема, це розділи I («Загальні положення»), III («Вибори. Референдум»), XIII («Внесення змін до Конституції України») Конституції України [13, с. 279]. За таких умов унітаризм як принцип конституційного ладу відображений у положеннях саме цих розділів Конституції України, зокрема у ст. 2, згідно з якою Україна є унітарною державою.

Також у науці представлено ширше розуміння конституційного ладу, під яким пропонується розглядати «систему суспільних відносин, передбачених і гарантованих Конституцією та законами, прийнятими на її основі та відповідно до неї. За своїм змістом конституційний лад опосередковує державний і суспільний лад, конституційно-правовий статус людини і громадянина, систему безпосередньої демократії, систему органів державної влади та місцевого самоврядування, основи національної безпеки, територіальний устрій та інші найважливіші суспільні відносини, що визначають

зміст конституційно-правових інститутів» (Д. В. Ковальов, А. В. Пономаренко) [14, с. 12].

На думку О. Ю. Курцева, унітаризм як принцип конституційного ладу відображений у п. 13 ч. 1 ст. 92 Конституції України, згідно з якою територіальний устрій України визначається виключно законом, що є однією з важливих гарантій єдності і цілісності державної території України, а також у п. 29 ст. 85 Конституції України, згідно з яким утворення і ліквідація районів, встановлення і зміна меж районів і міст, віднесення населених пунктів до категорії міст, найменування і перейменування населених пунктів і районів відносяться до функцій Верховної Ради України як єдиного законодавчого та представницького органу [15, с. 78]. Вважаємо, що інші положення Конституції України також можуть бути віднесені до таких, що розкривають зміст унітаризму, тобто можна вести мову про конституційні засади унітаризму, який охоплює ключові ідею побудови держави та її політико-правові відносини з суспільством. Як зазначає О. Ю. Курцев, «особливостями принципу унітаризму є те, що він передбачає чітку ієрархічну централізацію всього державного апарату, прямий або непрямий контроль над місцевими органами влади та органами місцевого самоврядування, які утворюються в адміністративно-територіальних одиницях. У широкому сенсі унітаризм — це концентрація влади, фінансів, а також засобів прийняття рішень і управління на рівні всієї держави» [16, с. 17]. В цілому, погоджуючись з наведеною характеристикою унітаризму як принципу конституційного ладу, зазначимо, що вона за своїми ознаками є спорідненою з розумінням унітаризму як «способу життя, що поєднує територіальну єдність й невіддільність у конституційних відносинах різних форм державності — від централізованих до децентралізованих, деконцентрованих, регіональних держав і місцевого самоврядування», запропонованою О. В. Батановим, і ґрунтується на широкому розумінні

конституційного ладу, який поєднує елементи як державного, так і суспільно-політичного устрою [11, с. 88].

Розглядаючи унітаризм як конституційну цінність, потрібно виходити з універсального розуміння конституційних цінностей, тобто якісних характеристик державно-правових явищ вищого порядку, які пов'язані з усвідомлення самим суспільством ідей добра, справедливості, людської гідності, фундаментальних ідей і норм [17, с. 45]. На думку авторів «Малої енциклопедії конституційного права» конституційна цінність становить «результат суспільного консенсусу щодо необхідності правового захисту усталених соціальних цінностей, які виражають усталені стереотипи поведінки, структуру соціальних зв'язків та визначають зміст конституційних принципів і норм; зумовлюють природу конституції як нормативного акта та певного типу легітимного соціального порядку [18, с. 443]. Проте у цьому разі виникає питання про співвідношення між конституційними цінностями та загально-правовими цінностями, які також закріплені у положеннях конституційних актів. Зокрема, до загально-правових цінностей, закріплених у Конституції України, слід віднести людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку (статті 3, 27, 49 Конституції України); гідність та свободу людини (статті 21, 28 Конституції України); право на вільний розвиток особистості (статті 23, 34, 35, 53 Конституції України); правову рівність (статті 21, 24 Конституції України); верховенство права (ст.ст. 1, 8 Конституції України); демократію (статті 1, 5 Конституції України); суверенітет та територіальну цілісність України (статті 1, 2, 17 Конституції України); республіканську форму правління (ст. 5 Конституції України) тощо [19]. З огляду на те, що саме наявність території та здійснення ефективного контролю над нею, є обов'язковою ознакою держави, територіальна цілісність є загально-правовою цінністю, яка має універсальний характер, незалежно від територіального устрою, історично

сформованого у певній державі. Натомість унітаризм позбавлений універсального характеру, оскільки політико-територіальна організація суспільства допускає варіативність, що охоплює як унітарний територіальний устрій, так і федералізм.

Іншими словами унітаризм, як конституційна цінність, розглядається у аксіологічному вимірі як принцип конституційного ладу, що полягає у формуванні певної світоглядної системи уявлень про політико-територіальний устрій держави, що набуває ознак конституційно-правової та політичної ідеології [9, с. 189].

Однією з найпоширеніших точок зору на сутність унітаризму є його ототожнення з формою державного устрою. Передусім це зумовлено тим, що унітаризм, як форма державного устрою, базується на адміністративно-територіальному поділі, який, як вказує М. В. Савчин, передбачає уніфікацію законодавства про місцеву владу та уніфікацію системи органів державної влади та органів місцевого самоврядування [20, с. 221]. Вважаємо, що це слушно лише стосовно держав з симетричним територіальним устроєм, за якого усі адміністративно-територіальні одиниці мають рівний статус. Натомість у державах з асиметричним територіальним устроєм їх статус може відрізнятись, що спростовує висновок про уніфікацію законодавства та системи державного управління та місцевого самоврядування. Вважаємо, що такий підхід фактично ототожнює поняття унітаризму та унітарної держави. Проте, хоча ці поняття є пов'язаними між собою за змістом, все ж характеризують різні правові явища.

Як зазначає В. В. Міщук, унітарною є держава, яка характеризується такими ознаками: 1) територія держави поділена на адміністративно-територіальні одиниці, які не наділені державним суверенітетом; 2) єдина структура державного апарату, компетенція якого поширюється на всю територію держави; 3) єдине громадянство; 4) єдина система законодавства, основним законом якої є єдина державна конституція; 5) єдина судова система; 6) єдина

система органів конституційного контролю; 7) одноканальна система оподаткування; 8) у міжнародних відносинах виступає єдиним цілим [21, с. 9].

Унітарна держава передусім є ознакою державного устрою, яка вказує на те, що адміністративно-територіальні одиниці, які є територіальною основою для здійснення функцій держави, не мають статусу державних утворень та організація влади у яких характеризується низкою ознак, таких як: внутрішня єдність, що пов'язана з централізацією влади у тому чи іншому ступені, єдиній конституції та системі права, єдиному громадянстві. Як зазначає О. В. Батанов, «Унітарний характер держави означає, що територія у межах існуючих державних кордонів є цілісною і недоторканною, що складові частини цієї території перебувають у нерозривному взаємозв'язку, відзначаються внутрішньою єдністю і не мають ознак державності, як це властиво складовим частинам, скажімо, федеративної держави» [22, с. 22]. Крім цього, на думку науковця, основоположною характеристикою унітарної держави та унітаризму в цілому є «унітарна правосвідомість» більшості населення, що є пов'язаною з поняттям «громадянськості» — духовно-моральної цінності, що охоплює світоглядно-психологічною характеристику людини або групи людини, що зумовлена її державною самоідентифікацією, усвідомленням належності до конкретної країни [22, с. 22; 23].

Вважаємо, що унітаризм як політико-правове явище є ширшим за змістом поняттям, ніж форма державного устрою, яким є унітарна держава.

Також слід погодитись з позицією В. А. Явір, яка розглядає унітаризм як цивілізаційний вибір форми державного устрою України, який характеризує «внутрішню структуру держави, спосіб її територіального поділу, співвідношення держави (центру) з її складовими частинами (регіонами), ступінь централізації та децентралізації державної влади» [24, с. 166].

Розглядаючи унітаризм як принцип територіального управління, В. В. Міщук наголошує на тому, що його сутність полягає у централізації, «яка обов'язково знаходить свій вияв у сфері державної влади та управління, а також може об'єктивізуватися в економічній, культурній, соціальній та інших сферах державно-суспільного життя» [21, с. 18]. Проте централізація, яка полягає у зосередженні частки державної влади у центрі, також не є абсолютним мірилом унітаризму, враховуючи різноманітність моделей поєднання ознак централізації та децентралізації. Розуміння унітаризму як принципу територіального устрою, на нашу думку, звужує його зміст, оскільки територіальний устрій є лише одним з елементів, пов'язаним з державним устроєм. Як зазначив Конституційний Суд України у Рішенні у справі за конституційним поданням виконуючого обов'язки Президента України, Голови Верховної Ради України щодо відповідності Конституції України (конституційності) Постанови Верховної Ради Автономної Республіки Крим «Про Декларацію про незалежність Автономної Республіки Крим і міста Севастополя» від 20 березня 2014 року № 3-рп/2014, «Згідно зі статтею 132 Конституції України територіальний устрій України ґрунтується на засадах єдності та цілісності державної території, поєднання централізації і децентралізації у здійсненні державної влади, збалансованості і соціально-економічного розвитку регіонів, з урахуванням їх історичних, економічних, екологічних, географічних і демографічних особливостей, етнічних і культурних традицій. Зазначені конституційні принципи організації територіального устрою обумовлені формою державного устрою України як унітарної держави» [25].

На нашу думку, саме розуміння унітаризму як принципу конституційного ладу є базовим, оскільки маючи засадничу природу воно охоплює усі інші його аспекти: державний та адміністративно-територіальний устрій, принципи територіального управління та його взаємодії з органами місцевого самоврядування.

2. Конституційні засади унітаризму

У Конституції України, яка є Основним Законом України, визначено основні засади унітаризму в Україні, які з огляду на їх конституційний статус становлять підґрунтя для розвитку положень про унітаризм у інших нормативно-правових актах. Передусім, це загальні положення, передбачені у розділі І Конституції України:

1) у ст. 2 Конституції України, у якій закріплено, що суверенітет України поширюється на всю її територію. Україна є унітарною державою, а територія України в межах існуючого кордону є цілісною і недоторканною;

2) у ст. 4 Конституції України, згідно з якою в Україні існує єдине громадянство;

3) у ст. 5 Конституції України, відповідно до якої народ здійснює владу безпосередньо і через органи державної влади та органи місцевого самоврядування;

4) у ст. 7 Конституції України, яка передбачає, що Конституція України має найвищу юридичну силу, закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй;

5) у ст. 19 Конституції України, у якій визначено, що органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [2].

Отже, у цих положеннях охарактеризовані загальні засади унітаризму, які конкретизовані у наступних розділах Конституції України або набувають розвитку у інших нормативно-правових актах (наприклад, Законі України «Про громадянство України»). Їхнє значення полягає у тому, що на рівні Основного Закону держави закріплено унітарну форму державного устрою, з чого одразу випливає низка якісних характеристик української держави, зокрема, як держави з відсутніми у її складі

відокремленими державними утвореннями, що зумовлює висновок про те, що положення інших розділів Конституції України та інших нормативно-правових актів у частині громадянства, адміністративно-територіального устрою, організації та повноважень органів державної влади та місцевого самоврядування мають відповідати концептуальному положенню Конституції України про унітарну державу.

Подібні за змістом статті про унітарну форму державного устрою закріплені в Основних Законах зарубіжних держав. Наприклад, це ст. 3 Конституції Польської Республіки (далі — Конституція Польщі), у якій зазначено, що Польська Республіка є унітарною державою [26, с. 16].

У Конституції Французької Республіки (далі — Конституція Франції) не згадується формулювання «унітарна держава», хоча у ст. 1 цього акта йде мова про те, що «Франція — неподільна, світська, демократична і соціальна Республіка. Вона забезпечує рівність перед законом усіх громадян незалежно від їх походження, раси або релігії. Вона визнає всі віросповідання. Її організація є децентралізованою». З цього можна зробити висновок про те, що за формою державного устрою Франція є унітарною державою, хоча і з чіткою тенденцією до децентралізації [27, с. 17].

У ст. 5 Конституції Італійської Республіки (далі — Конституція Італії) також закріплено унітарну форму державного устрою, проте її засади визначені ще більш детально: «Єдина і неподільна Республіка визнає місцеві автономії і сприяє їх розвитку, здійснює найширшу адміністративну децентралізацію у службах, які залежать від Держави, узгоджує принципи і методи власного законотворення із завданнями автономії і децентралізації» [28, с. 20].

Також, на відміну від ст. 4 Конституції України, Конституція Польщі, Конституція Франції та Конституція Італії не містять положень про єдине громадянство.

При цьому в Основних законах усіх вказаних держав, як і у ст. 5 Конституції України, спостерігається наявність норм про здійснення влади народом. Згідно зі ст. 4 Конституції Польщі верховна влада у Польській Республіці належить народу, а народ здійснює владу через своїх представників або безпосередньо [26, с. 16].

У ст. 2 Конституції Франції зазначено, що принцип Французької Республіки — це правління народу, здійснюване народом для народу. Також згідно зі ст. 3 Конституції Франції «національний суверенітет належить народу, який здійснює його через своїх представників і шляхом референдуму» [27, с. 18].

Натомість Конституція Італії прямо не передбачає визнання народу джерелом влади, хоча фактично визнає це, як випливає з глави IV Конституції «Політичні відносини».

Окремі ідеї унітаризму також вбачаються з положень, передбачених розділом II Конституції України «Права, свободи та обов'язки людини і громадянина». З положень ст. 37 Конституції України вбачається заборона утворення і діяльності політичних партій та громадських організацій, програмні цілі або дії яких спрямовані на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, а також заборона створення і діяльності організаційних структур політичних партій в органах виконавчої та судової влади і виконавчих органах місцевого самоврядування. Також відповідно до ст. 38 Конституції України громадяни мають право брати участь в управлінні державними справами, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування, а також громадяни користуються рівним правом доступу до державної служби, а також до служби в органах місцевого самоврядування [2].

Аналогічні положення також закріплені в Основних законах зарубіжних держав. Зокрема, у ст. 5 Конституції Польщі вказано,

що Польська Республіка стоїть на сторожі незалежності і недоторканості своєї території. При цьому Конституція Польщі, передбачаючи у ст. 13 заборону діяльності окремих політичних партій та організацій, зокрема тих, які «звертаються у своїх програмах до тоталітарних методів і практики нацизму, фашизму і комунізму, а також ті, програма і діяльність яких передбачає або припускає расову і національну ненависть, застосування насильства з метою захопити владу чи впливати на політику держави, або передбачає таємність структур або членства», не допускає діяльність партій, програма яких містить положення, спрямовані на порушення суверенітету і територіальної цілісності держави [26, с. 17]. Проте ст. 58 Конституції Польщі містить заборону об'єднань, мета або діяльність яких суперечить Конституції або закону. Рішення про відмову у реєстрації або про заборону діяльності такого об'єднання приймає суд [26, с. 27]. Крім цього, у ст. 60 Конституції Польщі передбачено, що польські громадяни, які повною мірою користуються публічними правами, мають рівне право доступу до публічної служби, а у ст. 62 зазначеного акту — положення про те, що польський громадянин має право брати участь у референдумі, а також право обирати Президента Республіки, депутатів, сенаторів і представників до органів територіального самоврядування, якщо на день голосування досяг 18 років [26, с. 28].

У Конституції Франції закріплені лише загальні положення про те, що партії утворюються і функціонують вільно, але вони зобов'язані поважати принципи національного суверенітету і демократії (ст. 4 Конституції Франції) [27, с. 18]. Також ст. 3 вказаного акту передбачає, що «Виборче право завжди є загальним і рівним, голосування — таємним. Відповідно до визначених законом умов виборцями є повнолітні громадяни Франції обох статей, які користуються громадянськими і політичними правами. Проте, у частині регламентації інших політичних прав та права на державну службу,

у Конституції Франції містяться лише загальні норми про те, що ці питання регулюються законами [27, с. 23].

У Конституції Італії також лише схематично наведені положення про політичні права громадян, зокрема, про право на свободу зібрань, за винятком заборони таємних об'єднань і таких, що хоча б опосередковано переслідують політичні цілі, досяжні за допомогою організацій військового характеру (ст. 18) та право об'єднуватися у партії з метою у демократичний спосіб брати участь у визначенні національної політики (ст. 49). Також у ст. 50 Конституції Італії встановлено, що право голосу мають усі громадяни, чоловіки і жінки, які є повнолітніми, серед яких і ті, які проживають за межами країни, для чого утворюється один закордонний виборчий округ з виборів до палат парламенту, для якого передбачається кількість мандатів згідно з конституційною нормою і відповідно до критеріїв, визначених законом. На відміну від України, Франції та Польщі, Конституція Італії дозволяє доступ до публічної служби та виборних посади як для громадян і для осіб італійської національності, які не є громадянами Республіки [28, с. 30–32].

Отже, у порівнянні з Основними законами Італії, Франції та Польщі, у розділі II Конституції України виклад положень щодо взаємозв'язку між територіальною цілісністю та засобами її захисту в контексті визнання основних прав людини, видається повнішим.

У розділі IV «Верховна Рада України» закріплені положення про статус Верховної Ради України як єдиного органу законодавчого влади в Україні (ст. 37 Конституції України). Згідно з пунктами 28–29 ст. 85 Конституції України до повноважень Верховної Ради України належить: дострокове припинення повноважень Верховної Ради Автономної Республіки Крим за наявності висновку Конституційного Суду України про порушення нею Конституції України або законів України; призначення позачергових виборів до Верховної Ради Автономної Республіки Крим; утворення

і ліквідація районів, встановлення і зміна меж районів і міст, віднесення населених пунктів до категорії міст, найменування і перейменування населених пунктів і районів; призначення чергових та позачергових виборів до органів місцевого самоврядування.

На відміну від Конституції України, у Конституції Польщі лише констатується, що законодавчу владу у Польській Республіці здійснюють Сейм і Сенат (ст. 95) і докладно регламентується законодавчий процес. Тоді як безпосередньо повноваження Сейму та Сенату у розділі IV «Сейм і Сенат» не розкриваються [26, с. 37–45].

У розділі IV Конституції Франції «Парламент» також лише викладені засади діяльності парламенту, який складається з Національних зборів і Сенату (ст. 24). Причому якщо депутати Національних зборів обираються на прямих виборах, то саме Сенат, який обирається на непрямих виборах, забезпечує представництво територіальних колективів Республіки [27, с. 25].

У Конституції Італії також не висвітлені повноваження парламенту, у тому числі в частині втілення засад унітаризму. Натомість Конституція Італії передбачає низку норм, які регламентують особливості виборів до парламенту, метою яких є такий розподіл місць у парламенті, який забезпечив найповніше представництво регіонів з урахуванням кількості населення. Зокрема, під час виборів до Палати депутатів розподіл місць між виборчими округами, за винятком віднесених до закордонного виборчого округа, здійснюється шляхом поділу числа жителів Республіки, яке визначене згідно з останнім переписом населення, на шістсот вісімнадцять і пропорційно до кількості населення кожного округу на основі внутрішнього виборчого коефіцієнта і правила найбільшого залишку (ст. 56 Конституції Італії). Також відповідно до ст. 57 Конституції Італії Сенат Республіки обирається на основі регіонів, за винятком місцевостей, віднесених до закордонного виборчого округу. Причому загальна кількість сенаторів становить триста п'ятнадцять і шість

з яких обираються у закордонному виборчому округі. Конституція передбачає мінімальну кількість сенаторів від кожного регіону, що становить сім сенаторів, а також два винятки: область Молізе обирає двох сенаторів, а автономна область Валле д'Аоста — одного сенатора. Розподіл місць між регіонами, за винятком місцевостей, віднесених до закордонного виборчого округу, здійснюється пропорційно кількості населення регіонів, яка визначена за останнім переписом населення, на основі внутрішнього виборчого коефіцієнта і правила найбільшого залишку [28, с. 32].

У ст. 92 Конституції України виокремлено перелік питань, які визначаються виключно законами України, що свідчить про уніфікацію правової системи та регламентацію найважливіших суспільних відносин у межах держави. До таких питань віднесено: правовий статус людини та громадянина, громадянство, порядок застосування мов; засади використання природних ресурсів; основи соціального захисту; правовий режим власності; правові засади і гарантії підприємництва; засади зовнішніх зносин; засади утворення і діяльності політичних партій, інших об'єднань громадян, засобів масової інформації; організація і діяльність органів виконавчої влади, основи державної служби; територіальний устрій України; судоустрій, судочинство, статус суддів; організація і діяльність адвокатури, прокуратури, нотаріату, органів досудового розслідування, органів і установ виконання покарань; порядок виконання судових рішень; засади організації та діяльності адвокатури; засади місцевого самоврядування; статус столиці України; спеціальний статус інших міст; основи національної безпеки, організації Збройних Сил України і забезпечення громадського порядку; правовий режим державного кордону тощо [2]. З наведених вище Основних законів зарубіжних держав подібна стаття також закріплена у Конституції Франції та Конституції Італії. Зокрема, ст. 34 Конституції Франції передбачає, що лише законом

можуть бути визначені громадянські права і фундаментальні гарантії, які надаються громадянам для користування публічними свободами; плюралізм і незалежність засобів масової інформації; обов'язки громадян щодо їх особистих і майнових прав, здійснюваних у зв'язку з потребами національної оборони; порядок виборів до палат Парламенту і до місцевих зборів, а також до органів, які представляють французів, що проживають за межами Франції, громадянства, умови реалізації представницьких мандатів і заміщення виборних посад у територіальних колективах; установлення категорій публічних установ та інше [27, с. 28–29]. З цього вбачається, що хоча ст. 34 Конституції Франції і визначає досить широкий перелік сфер суспільного життя, відносини у яких регламентуються виключно законом, між ст. 34 Конституції Франції та ст. 92 Конституції України існують значні відмінності, з яких вбачається, що такий перелік, який визначений у ст. 92 Конституції України, є не лише детальнішим, а й таким, що охоплює більше коло відносин, що безпосередньо пов'язані з організацією здійснення публічної влади.

Ст. 117 Конституції Італії визначає сфери, регулювання яких виключною компетенцією держави, серед яких, серед іншого, адміністративний устрій і організація держави, а також відносини держави з національними меншинами; громадський порядок і безпека, за винятком місцевої адміністративної поліції; громадянство, правоздатність і облік населення; законодавство про вибори, про органи управління і про основні функції комун, провінцій і метрополітенських міст (міста, які є центром метропольного регіону — густонаселеної території, яку утворюють міська агломерація та менш урбанізовані навколишні райони); митна справа, охорона державних кордонів.

При цьому суттєві відмінності Конституції Італії від Конституцій інших держав, що розглядаються, становлять посилання на те, що регіони здійснюють законодавчу владу у будь-якій сфері,

спеціально не зарезервованій за державою, оскільки відповідно до ст. 117 Конституції Італії законодавчу владу здійснюють держава і регіони, виходячи з вимог Конституції і враховуючи положення права ЄС та міжнародні зобов'язання [28, с. 49].

Розділ VI Конституції України «Кабінет Міністрів України. Інші органи виконавчої влади» містить положення про статус і повноваження Кабінету Міністрів України. Кабінет Міністрів України є вищим органом у системі органів виконавчої влади (ст. 113). У статті 116 Конституції України закріплена система повноважень Кабінету Міністрів України, зокрема в частині забезпечення державного суверенітету і економічної самостійності України, здійсненні внутрішньої і зовнішньої політики держави, виконанні Конституції і законів України, актів Президента України; забезпеченні проведення фінансової, цінової, інвестиційної та податкової політики; політики у сферах праці й зайнятості населення, соціального захисту, освіти, науки і культури, охорони природи, екологічної безпеки і природокористування; розробки і здійснення загальнодержавних програм економічного, науково-технічного, соціального і культурного розвитку України; забезпеченні рівних умов розвитку всіх форм власності; здійсненні управління об'єктами державної власності відповідно до закону [2].

У ст. 146 Конституції Польщі, ч. 4 якої визначає повноваження Ради Міністрів Польської республіки, не зазначені повноваження, подібні за змістом Конституції України, оскільки їхній зміст охарактеризовано загальними ознаками, за винятком таких повноважень як координація і контроль за роботою органів урядової адміністрації. Зокрема, до повноважень Ради Міністрів Польської республіки віднесені забезпечення виконання законів та видання розпоряджень, внутрішньої та зовнішньої безпеки держави, а також публічного порядку, здійснення загального керівництва у сфері обороноздатності країни [26, с. 52].

Згідно зі ст. 20 Конституції Франції «Уряд визначає і проводить політику Нації. Він розпоряджається цивільною адміністрацією і збройними силами». Положень про повноваження органу виконавчої влади розділ III Конституції Франції, який має назву «Уряд», не містить [27, с. 24].

У главі III Конституції Італії визначено лише основні засади складу, призначення та функціонування Ради Міністрів Італії, але ст. 97 Конституції Італії у цьому ж розділі регламентує особливості перебування на публічній службі. Зокрема, «Публічні служби організовані відповідно до закону з метою забезпечити неупередженість в адмініструванні і його дієвість. У положеннях про різні публічні служби визначаються сфера їх компетенції, функції і відповідальність посадових осіб. Посади у публічній адміністрації заміщуються за конкурсом, крім випадків, передбачених законом» [28, с. 43]. Також у ст. 98 Конституції Італії передбачено, що посадові особи у публічній адміністрації знаходяться виключно на службі Нації. Так само Законом можуть бути встановлені обмеження у праві належати до політичних партій стосовно суддів, кадрових військових дійсної служби, посадових і службових осіб поліції, а також дипломатичних і консульських представників за кордоном [28, с. 43].

На відміну від повноважень органу законодавчої влади, що є єдиним органом, Кабінет Міністрів України є органом виконавчої влади, яка охоплює систему органів виконавчої влади на місцях у такий спосіб, уніфікуючи державну політику в усіх регіонах. Конституційні підвалини цієї системи визначені у ст. 118 Конституції України, відповідно до якої виконавчу владу в областях і районах, містах Києві та Севастополі здійснюють місцеві державні адміністрації, голови яких призначаються на посаду і звільняються з посади Президентом України за поданням Кабінету Міністрів України і які при здійсненні своїх повноважень відповідальні перед Президентом України і Кабінетом Міністрів України, підзвітні

та підконтрольні органам виконавчої влади вищого рівня. Особливості здійснення виконавчої влади у містах Києві та Севастополі визначаються окремими законами України. Повноваження місцевих державних адміністрацій визначені у ст. 119 Конституції України, зокрема, до них віднесено: 1) виконання Конституції та законів України, актів Президента України, Кабінету Міністрів України, інших органів виконавчої влади; 2) законність і правопорядок; додержання прав і свобод громадян; 3) виконання державних і регіональних програм соціально-економічного та культурного розвитку, програм охорони довкілля, а в місцях компактного проживання корінних народів і національних меншин — також програм їх національно-культурного розвитку; 4) підготовку та виконання відповідних обласних і районних бюджетів; 5) звіт про виконання відповідних бюджетів та програм; 6) взаємодію з органами місцевого самоврядування; 7) реалізацію інших наданих державою, а також делегованих відповідними радами повноважень [2].

Також у ст. 118 та 119 Конституції України закладено основу механізму співпраці, зокрема, делегування повноважень, та контролю між місцевими органами виконавчої влади та органами місцевого самоврядування. Передусім, місцеві державні адміністрації підзвітні і підконтрольні радам у частині повноважень, делегованих їм відповідними районними чи обласними радами. Також обласна чи районна рада може висловити недовіру голові відповідної місцевої державної адміністрації, на підставі чого Президент України приймає рішення і дає обґрунтовану відповідь. Якщо недовіру голові районної чи обласної державної адміністрації висловили дві третини депутатів від складу відповідної ради, Президент України приймає рішення про відставку голови місцевої державної адміністрації [2].

У Конституції Італії досить ґрунтовно викладено положення про роль регіонів у державному урядуванні. Передусім, як було зазначено вище, в Італії регіони наділені законодавчою владою.

Крім цього, як вказано у ст. 117 Конституції Італії «регіони і автономні провінції Тренто і Больцано у сфері своєї компетенції беруть участь в ухваленні рішень, співвіднесених за змістом з положеннями права ЄС. Регіони і провінції забезпечують імплементацію та виконання міжнародних зобов'язань і актів Європейського Союзу при дотриманні процедури, встановленої законом держави. Закон держави встановлює процедуру, відповідно до якої держава діє замість регіону кожного разу якщо регіон не виконує свої зобов'язання щодо співпраці» [28, с. 50]. Крім цього, ст. 118 Конституції Італії передбачає, що здійснення адміністративних функцій належить до відання комун — муніципалітетів, «за винятком тих, здійснення яких для забезпечення єдиних підходів належить до відання провінцій, метрополітенських міст, регіонів і держави при дотриманні принципів субсидіарності, диференційованості і пропорційності. Комуни, провінції і метрополітенські міста наділені власними адміністративними функціями, які визначені законом держави або законом регіону відповідно до компетенції. Також у ст. 119 Конституції Італії закріплено фінансову автономію комун, провінцій, метрополітенських міст і регіонів щодо своїх доходів та видатків, на них покладено обов'язок збалансовувати бюджет і дотримуватися відповідних актів Європейського Союзу [28, с. 51].

Натомість у Конституції Польщі практично відсутні положення про воєводства — адміністративно-територіальні одиниці, які очолюються воєводами, що є представниками Ради Міністрів Польщі. При цьому ст. 171 Конституції Польщі визначає повноваження Голови Ради міністрів та воєвод здійснювати нагляд за діяльністю одиниць територіального самоврядування [26, с. 59].

У ст. 72 Конституції Франції передбачено призначення до територіальної громади державного представника (префекта, супрефекта), на якого покладено обов'язок представляти членів, забезпечувати здійснення адміністративного контролю та виконання

законів і які призначаються Президентом після консультацій з Радою міністрів [27, с. 46].

Отже, на відміну від Конституції України та Конституції Італії, яка детально визначає засади реалізації функцій виконавчої влади на місцях, у Конституції Польщі та Конституції Франції ці питання переважно регламентовані окремими законами.

У розділі IX «Територіальний устрій України» визначено його засади, що охоплюють єдність та цілісність державної території, поєднання централізації і децентралізації у здійсненні державної влади, збалансованість і соціально-економічний розвиток регіонів, з урахуванням їх історичних, економічних, екологічних, географічних і демографічних особливостей, етнічних і культурних традицій (ст. 132 Конституції України), а також систему адміністративно-територіального устрою України, яку складають: Автономна Республіка Крим, області, райони, міста, райони в містах, селища і села (ст. 133 Конституції України). Причому міста Київ та Севастополь мають спеціальний статус, який визначається законами України [2].

Статус Автономної Республіки Крим визначено у розділі X Конституції України. Зокрема, згідно зі ст. 134 Конституції України Автономна Республіка Крим є невід'ємною складовою частиною України і в межах повноважень, визначених Конституцією України, вирішує питання, віднесені до її відання [2].

Конституція Польщі не містить норм про територіальний устрій, подібних тим, які передбачені у розділі IX Конституції України, зосереджуюсь на територіальному самоврядуванні (розділ VII Конституції Польщі) [26, с. 57]. Натомість у розділі XII Конституції Франції поєднано виклад положень про територіальний устрій та про територіальне самоврядування. У ст. 72 Конституції Франції передбачено, що територіальними громадами (колективами, collectivite) Французької Республіки є комуни, департаменти, регіони, колективи зі спеціальним статусом, а також

заморські території. Також у ст. 72-3 Конституції Франції закріплена норма про те, що «Республіка визнає частиною французького народу населення заморських територій, керуючись спільними ідеалами свободи, рівності і братерства. Гваделупа, Гвіана, Мартініка, Реюньйон, Майотта, Сен-Бартелемі, Сен-Мартін, Сен-П'єр і Мікелон, острови Уолліс і Футуна та Французька Полінезія мають статус, визначений у статті 73 відносно заморських департаментів і регіонів (departement et region d`outre-mer). Статус Нової Каледонії визначений в розділі XIII Конституції Франції, а правовий режим і особливості організації французьких володінь у районі Австралії і Антарктики, а також Кліппертона — визначаються окремим законом [27, с. 49–50].

У главі V Конституції Італії «Регіони, провінції, комуни» також поєднано регламентацію територіального устрою та засад управління та самоврядування адміністративно-територіальних одиниць. Згідно зі ст. 114 Конституції Італії територіальний устрій охоплює комуни, провінції, метрополітенські міста, які є містами з самоврядуванням, регіони і держава. При чому на підставі принципів, визначених Конституцією, комуни, провінції, метрополітенські міста і регіони є автономними утвореннями з власними статутами, повноваженнями і функціями. Також управління Римом, тобто столицею Республіки, здійснюється в окремому порядку, визначеному спеціальним законом [28, с. 48].

Італія, будучи унітарною державою, має у своєму складі декілька автономій, які є регіонами зі спеціальним статусом. Зокрема, ст. 116 Конституції Італії визначає, що Фріулі-Венеція Джулія, Сардинія, Сицилія, Трентіно-Альто Адідже (Південний Тіроль) і Валле д'Аоста мають особливу форму і умови автономії відповідно до спеціальних статутів, які затверджені конституційними законами. У свою чергу, регіон зі спеціальним статусом Трентіно-Альто Адідже складається з автономних провінцій Тренто і Больцано,

які мають низку управлінських особливостей [28, с. 49]. Загалом, відповідно до ст. 131 Конституції Італії, утворюються такі регіони: П'ємонт, Валле д'Аоста, Ломбардія, Трентіно-Альто Адідже, Венето, Фріулі-Венеція Джулія, Лігурія, Емілія-Романія, Тоскана, Умбрія, Марке, Лаціо, Абруцці, Молізе, Кампанія, Апулія, Базіліката, Калабрія, Сицилія, Сардинія [28, с. 55].

Отже, як вбачається з викладеного, у Конституціях різних держав мають місце відмінні між собою підходи до викладу норм про територіальний устрій унітарної держави: якщо у Конституції України та у Конституції Італії закріплений перелік адміністративно-територіальних одиниць, то у Конституції Францію перелічені виключно заморські території, а у Конституції Польщі це питання взагалі не регламентовано. Крім цього, у наведених Конституціях наведені різні форми унітарного устрою — держава без автономних утворень (Польща), держава з одним автономним утворенням (Україна), держава з багатьма автономними утвореннями (Італія) та держава з територіями зі спеціальним статусом, які не іменуються автономіями, хоча мають свої особливості управління.

У розділі XI Конституції України «Місцеве самоврядування» закріплені основні засади права територіальної громади — жителів села чи добровільного об'єднання у сільську громаду жителів кількох сіл, селища та міста — самостійно вирішувати питання місцевого значення в межах Конституції і законів України (ст. 140 Конституції України). Причому особливості здійснення місцевого самоврядування в містах Києві та Севастополі визначаються окремими законами України [2].

Розділ VII Конституції Польщі «Територіальне самоврядування» містить базові засади місцевого самоврядування. Зокрема, територіальне самоврядування, основною одиницею якого є гміна, виконує публічні завдання, не віднесені Конституцією або законами до компетенції органів інших публічних влад, а громада

виконує усі завдання територіального самоврядування, не віднесені до компетенції інших одиниць територіального самоврядування. Згідно зі ст. 166 Конституції Польщі публічні завдання, що слугують задоволенню потреб самоврядної спільноти, виконуються одиницями територіального самоврядування як власні завдання. Проте, якщо це зумовлено обґрунтованими потребами держави, згідно із законом може бути доручено одиницям територіального самоврядування виконувати інші публічні завдання. Законом визначаються порядок здійснення доручення і спосіб виконання доручених завдань [26, с. 57].

Так само згідно зі ст. 72 Конституції Франції «відповідно до передбачених законом умов територіальні колективи вільно управляються виборними радами, які наділені повноваженнями регламентарного характеру, тобто повноваженнями видавати місцеві акти. Територіальні колективи мають ресурси, якими вони вільно розпоряджаються відповідно до умов, встановлених законом.

Будь-яка передача повноважень держави територіальним колективам і між самими колективами супроводжується передачею ресурсів, необхідних для їх здійснення. Будь-яке надання або розширення повноважень, яке пов'язане із збільшенням витрат територіальних колективів, супроводжується виділенням ресурсів відповідно до закону (ст. 72-2 Конституції Франції) [27, с. 48].

У статтях 73–74-2 Конституції Франції регламентовано статус заморського регіону або департаменту. Як зазначено у ст. 73 Конституції Франції «у заморських департаментах і регіонах на загальних підставах застосовуються закони і регламенти. Вони можуть бути адаптовані з урахуванням особливостей цих територіальних колективів. Якщо на це уповноважує закон або регламент, адаптація з питань, віднесених до компетенції територіальних колективів, здійснюється самими колективами шляхом ухвалення відповідних рішень. Без урахування першої частини, територіальні колективи,

визначені у цій статті, можуть бути уповноважені згідно із законом або регламентом встановлювати правила з визначених питань законодавчого або регламентарного характеру, які будуть застосовуватися в межах їх території.» Проте з цих положень є винятки, оскільки такі акти не повинні охоплювати питання громадянства, громадянських прав, гарантій публічної свободи, статусу і правоздатності індивідів, судоустрою, кримінального права, кримінального процесу, зовнішньої політики, оборони, безпеки і публічного порядку, емісії грошей, кредитування і грошового ринку, а також виборчого права [27, с. 49].

Стаття 118 Конституції Італії передбачає, що здійснення адміністративних функцій є компетенцією комун, за винятком тих, здійснення яких для забезпечення єдиних підходів належить до відання провінцій, метрополітенських міст, регіонів і держави при дотриманні принципів субсидіарності, диференційованості і пропорційності.

Комуни, провінції і метрополітенські міста наділені власними адміністративними функціями, які визначені законом держави або законом регіону відповідно до компетенції [28, с. 51].

На відміну від Конституцій наведених вище держав, Конституція Італії передбачає широкий спектр повноважень територіальних громад, оскільки регіони, як і держава в цілому, здійснюють законодавчу владу, виходячи з вимог Конституції і враховуючи положення права ЄС та міжнародні зобов'язання. При чому, як визначає ст. 117 Конституції Італії, «Регіони здійснюють законодавчу владу у будь-якій сфері, спеціально не зарезервованій за державою. Регіони і автономні провінції Тренто і Больцано у сфері своєї компетенції беруть участь в ухваленні рішень, співвіднесених за змістом з положеннями права ЄС. Регіони і провінції забезпечують імплементацію та виконання міжнародних зобов'язань і актів Європейського Союзу при дотриманні процедури, встановленої законом

держави. Закон держави встановлює процедуру, відповідно до якої держава діє замість регіону кожного разу якщо регіон не виконує свої зобов'язання щодо співпраці» [28, с. 50]. Так само Законом регіону ратифікуються угоди регіону, укладені з іншими регіонами для кращого здійснення функцій, а також з метою утворення спільних органів. У сферах, віднесених до їх компетенції, регіони можуть укладати угоди з іноземними державами і з територіальними утвореннями у складі інших держав у передбачених випадках і у встановлених формах згідно із законом держави. Такий підхід до визначення повноважень регіонів дещо відрізняється від інших унітарних держав, для яких укладання міжнародних договорів є більш характерним для центрального рівня державної влади.

Отже, виклад конституційних засад унітаризму у Конституціях розглянутих держав відрізняється. У Конституції України засади унітаризму, крім розділу I «Загальні засади», чітко прослідковуються ще у декількох розділах, які регламентують різні складові частини конституційного ладу (розділ II «Права, свободи та обов'язки людини і громадянина», розділ IV «Верховна Рада України», розділ VI «Кабінет Міністрів України. Інші органи виконавчої влади», розділ IX «Територіальний устрій України», розділ X «Автономна Республіка Крим»). Фактично ці норми деталізують ідеї унітаризму. Натомість у Конституції Польщі, Конституції Франції та Конституції Італії такі норми здебільшого зосереджені у розділах, які регламентують загальні питання державного устрою та суверенітету і переважно полягають у констатації унітарного характеру територіального устрою (Конституція Польщі, Конституція Італії) або наведенні ознак, які характеризують державний устрій як унітарний (Конституція Франції). При цьому в Основних законах більшості наведених держав наголошується на децентралізації територіального устрою у різних контекстах (ст. 132 Конституції України: «поєднання централізації

і децентралізації у здійсненні державної влади»; ст. 15 Конституції Польщі: «Територіальний устрій Польської Республіки слугує децентралізації публічної влади»; ст. 5 Конституції Італії: «Єдина і неподільна Республіка визнає місцеві автономії і сприяє їх розвитку, здійснює найширшу адміністративну децентралізацію у службах, які залежать від Держави, узгоджує принципи і методи власного законотворення із завданнями автономії і децентралізації.»). У Конституції Франції немає згадки про децентралізацію, проте, як зазначає В. М. Шаповал, характеризуючи політико-правові процеси у Франції, «в країні вже протягом кількох десятиліть проводиться політика децентралізації і деконцентрації влади, яка набувала різних форм» [27, с. 14].

Отже, загалом у Конституції України положення про повноваження органів державної влади в тому числі ті, з характеру яких вбачаються засади унітаризму, виписані детальніше. Разом з тим у Конституції Польщі, Конституції Італії та Конституції Франції, висвітлення засад унітаризму переважають у положеннях про територіальний устрій, які, крім положень про адміністративно — територіальний поділ, також охоплюють порядок здійснення місцевого самоврядування, політико-правових відносин місцевих державних та центральних державних органів влади, а також зафіксована побудова співпраці місцевих державних органів влади та органів місцевого самоврядування.

3. Розвиток унітаризму в Україні та зарубіжних державах в сучасних умовах

Тривалий час у теорії конституційного права домінувала тенденція до того, що державний устрій характеризується такими формами: 1) унітарна держава; 2) федерація; 3) конфедерація; 4) імперія. Наразі конфедерація і імперія залишаються ретроспективною формою державного устрою з огляду на практично

відсутність прикладів цих форм державного устрою серед сучасних держав (крім Швейцарії як конфедерації). На думку А. В. Панова, на сучасному етапі «такий поділ держав на сьогодні вже не є достатньо ефективним, оскільки не відображає суті територіальної організації влади… статус італійського регіону та австрійської федеральної землі мало чим відрізняється по суті, однак першу країну традиційно відносять до унітарних, а другу — до федеративних». Виходячи з цього, на думку науковця, доцільніше розділяти держави на централізовані та децентралізовані [29, с. 6]. На нашу думку, такий підхід фактично змішує два різні поняття — державний устрій як національно-територіальну організацію держави, та метод управління, який може характеризуватись як централізаційними, так і децентралізаційними процесами. А тому усталений підхід поділу держав за критерієм форми державного устрою на унітарні та федеративні зберігає актуальність. Виходячи з цього, закріплення у Конституції України форми державного устрою залишається актуальним.

Доцільно звернути увагу на тенденцію регіоналізації, яка спостерігається в окремих європейських державах. За регіоналізації регіони позиціонуються як політико-географічні суб'єкти, що об'єднані низкою чинників: історичний, психологічно-ментальний, економічний, культурний та інші [29, с. 6]. Політико-правовою основою регіоналізації є «Декларація про регіоналізм у Європі», прийнята Асамблеєю Європейських регіонів — міждержавною організацією, метою якої є захист прав європейських регіонів 4 грудня 1996 року. Зазначена декларація визначає концепцію регіону, його інституційну організацію, регіональні повноваження, фінансування, засади міжрегіонального фінансового зрівняння, правові відносини між державою та регіонами, засади розподілу функцій та повноважень, у тому числі у сфері міжнародних відносин, прикордонного співробітництва та відносин з ЄС.

Прикладами регіоналізації на сучасному етапі розвитку унітарної держави є Франція та Італія. Так, адміністративно-територіальний устрій Франції охоплює поділ території держави на 27 регіонів, що поділяються на 101 департамент, з яких 22 регіони та 96 департаментів територіально знаходяться власне у Франції, тоді як інші 5 регіонів — Гвадалупа, Майотта, Мартиніка, Французька Гвіана, Реюньон — складаються з одного департаменту [29, с. 10].

У Італії регіони становлять територіальні одиниці з найвищим статусом, що характеризуються автономністю у здійсненні своїх повноважень при вирішенні питань регіонального значення. З 20 регіонів Італії 5 — мають більш широкі повноваження та окрему систему державного та місцевого урядування, ніж інші в силу регіональних особливостей: Трентіно-Альто-Адідже, Валле-д'Аоста та Фріулі-Венеція-Джулія є регіонами, у яких мешкають національні меншини — німецька, словенська та французька, а Сардинія та Сицилія — віддалені острови з автохтонною культурою [28, с. 61]. Окремі українські вчені обстоюють позицію про те, що використання французького та італійського досвіду було б корисним при адміністративно-територіальній реформі в Україні у «пошуку балансу між сферами компетенції держави та самоврядування» [29, с. 46]. Наприклад, О. Рафальський зазначає, що «...об'єктивний аналіз показує, що Україна є країною багатонаціональною, багатомовною, поліконфесійною, має різновекторні економічні інтереси регіональних еліт. Як справедливо підкреслюють окремі вчені і політики, історично територія України формувалася з різних частин, які протягом певного історичного часу перебували у складі, а отже, і під впливом таких держав, як Польща, Росія, Австро-Угорщина, Румунія, Чехословаччина. Саме ці обставини і зумовили соціально-економічні, ментальні, культурні, конфесійні, лінгвістичні і т.п. відмінності різних регіонів України. Державна політика має полягати не у невиправданому придушенні

цих об'єктивних реалій, а в їх перетворенні з чинника потенційної небезпеки на чинники, що зміцнює єдність держави» [30, с. 25].

Водночас, регіоналізація, яка передусім бере до уваги історичні та ментальні чинники, не є єдиним варіантом вдосконалення державного територіального устрою. Також, на нашу думку, існують три вагомих чинника, які потенційно ускладнюють регіоналізацію в Україні.

По-перше, регіоналізація базується на визнанні культурних та ментальних відмінностей між регіонами, що сформувались історично. Новітня історія України для усіх українських регіонів є спільною: це період тоталітарної радянської держави, політика якої була спрямована на русифікацію та подолання культурних та релігійних відмінностей, що, крім іншого, було виражено у державній політиці, у тому числі у сфері переміщень як окремих людей, так і цілих народів. Тому наразі спільною проблемою різних регіонів України є подолання тоталітарного минулого і формування єдиної української ідентичності, що потребує інтеграції регіонів. Без врахування цього регіоналізація несе ризик поглиблення розколу суспільства та держави.

Вивчаючи досвід зарубіжних держав стосовно чинників регіоналізації, потрібно звернути увагу на те, що одним з таких чинників є наявність компактного проживання національних меншин або національних етнічних особливостей. Зокрема, на прикладі Італії, це регіони Трентіно-Альто-Адідже, Валле-д'Аоста та Фріулі-Венеція-Джулія у яких мешкають німецька, словенська та французька національні меншини. Згідно за ст. 6 Конституції Італії «Республіка на основі відповідних норм охороняє мовні діалекти» [28, с. 20]. Крім цього, кожен історичний регіон має свій діалект (усього близька 200, які поділяються на 7 великих груп).

Також це приклад Франції, сучасний устрій якої частково враховує історично сформовані регіональні особливості, серед яких

і регіональні мови. Зокрема, це баскська, бретонська, ельзаська, каталанська, лотарінгзько-франконська мови, мови ойль, окситанська та інші. Причому у ст. 2 Конституції Франції визначено, що мова Республіки — французька [27, с. 18], а окремий розділ Конституції Франції — розділ XIV «Франкофонія та угоди про об'єднання» містить ст. 87, згідно з якою «Республіка бере участь у розвитку солідарності і співробітництва між державами і народами, спільною для яких є французька мова (франкофонія) [27, с. 52]. Натомість відповідно до ст. 75-1 Конституції Франції регіональні мови проголошені надбанням Республіки.

Проте і у Італії, і у Франції, офіційний статус мають відповідно італійська та французька мови, чий статус не оспорюється. Натомість в Україні, різні регіони якої протягом тривалого історичного проміжку зазнавали насильницької мадяризації, полонізації, румунізації та русифікації, мовне питання залишається більш гострим. З огляду на певний відсоток територій, мешканці яких навіть в умовах повномасштабного вторгнення російської федерації обстоюють доцільність виняткового статусу російської мови, а також питання регіоналізації з наданням широких повноважень регіонам, у тому числі в питаннях міжнародних відносин, може нести потенційну загрозу національній безпеці. Натомість однією з функцій державної мови є об'єднувальна функція, значення якої полягає у ставленні громадян до мови як до чинника, який об'єднує суспільство і є основою механізму інтеграції у суспільство, що є особливо важливим у тих державах, де населенням традиційно є багатомовним [31, с. 24]. В українському суспільстві такою основою механізму інтеграції має бути одна офіційна (державна) мова — українська.

По-друге, регіоналізація у державах Західної Європи відбулась умовах відсутності територіальних претензій на відповідні регіони зі сторони сусідніх держав. Зокрема, та обставина, що в межах території Італії є три регіони, у якому компактно проживає

німецьке, словенське та французьке населення, не ставала підставою для вимог про передачу територій відповідним державам, надання її мешканцям громадянств цих держав або іншого втручання у внутрішні справи Італії та на «специфічні» відносини цих (сусідніх з Італією держав) з відповідними регіонами Італії.

По-третє, з 2014 року триває збройна агресія проти України зі сторони Російської Федерації, що має наслідком окупацію Автономної Республіки Крим, частин Донецької, Запорізької, Луганської, Харківської і Херсонської областей. Крім окупаційного режиму російських збройних сил, частина вказаних територій перебуває під контролем терористичних організацій «ДНР» та «ЛНР». Після відновлення контролю України за цими територіями буде проведена їхня реінтеграція, але особливості досвіду цих регіонів у виді окупації та перебування під контролем військових та терористичних угрупувань унеможливить регіоналізацію з огляду потенційних ризиків для національної безпеки.

З огляду на викладене, вважаємо, що для України більш вдалим кроком було запозичення досвіду тих держав, які здійснили децентралізацію, що полягає у перенесенні низки владних повноважень від рівня державної влади до рівня органів місцевого самоврядування. Метою децентралізації є побудова сильної моделі місцевого самоврядування, яка, як зазначають Я. О. Бариська та Т. П. Попович, характеризується принаймні такими ознаками як: «а) достатні владні повноваження, які оптимально дають змогу забезпечити розвиток територіальної громади й спільні інтереси територіальних громад на рівні регіону; б) достатні фінансові механізми, які створюють спроможність громади та мотиваційне поле для її розвитку; в) інституційна завершеність системи органів місцевого самоврядування, в основі якої — обрані виборцями органи; г) забезпечення ефективним державним контролем, що здійснюється уповноваженими урядом структурами» [32, с. 71].

В цьому аспекті є цікавим досвід децентралізації у Польщі. У результаті реформи система місцевого самоврядування стала триступеневою: гміни і повіти вирішують колективні потреби місцевого населення; воєводства вирішують питання регіонального розвитку разом із центральним урядом. Усі три рівні незалежні фінансово та діють на принципах субсидіарності й гарантованих доходів і кожен з рівнів має визначені повноваження.

За гмінами визначено повноваження у сфері початкової освіти, комунальних послуг, охорони здоров'я, закладів культури та окремих питань дорожньо-транспортного господарства. Джерелом доходів є місцеві податки та збори, а також фіксований відсоток певних загальнодержавних податків. До сфери відповідальності повіту — територіального об'єднання, яке складається з кількох гмін, відносяться адміністративні послуги, громадські послуги на місцевому понадґмінному рівні, громадська безпека, школи, лікарні, заклади культури та музеї, дороги повітового значення. Також повіт здійснює контрольні функції стосовно інших служб, підпорядкованих адміністрації повіту: поліція, пожежна служба, санітарно-епідеміологічна інспекція, ветеринарна інспекція. Воєводство як найвища ланка місцевого самоврядування визначає політику регіону і, відповідно, займається питаннями розвитку регіону, бере участь у реалізації завдань, що стоять перед державою, укладає контракти регіонів з центральним урядом [33, с. 90–92].

У с. 132 Конституції України визначені основні засади територіального устрою, серед яких також поєднання централізації і децентралізації у здійсненні державної влади. Проте процес децентралізації в України розпочався лише після Революції Гідності 2013–2014 рр. Програмним документом децентралізації стала Концепція реформування місцевого самоврядування та територіальної організації влади в Україні, схвалена розпорядженням Кабінету Міністрів України 1 квітня 2014 р. № 333-р (далі — Концепція).

Метою Концепції є визначення напрямів, механізмів і строків формування ефективного місцевого самоврядування та територіальної організації влади для створення і підтримки повноцінного життєвого середовища для громадян, надання високоякісних та доступних публічних послуг, становлення інститутів прямого народовладдя, задоволення інтересів громадян в усіх сферах життєдіяльності на відповідній території, узгодження інтересів держави та територіальних громад. Серед основних проблем у Концепції було названо те, що «розвиток місцевого самоврядування фактично здійснювався лише на рівні територіальних громад міст обласного значення, оскільки переважна більшість територіальних громад через їх надмірну подрібненість та надзвичайно слабку матеріально-фінансову базу виявилися неспроможними виконувати всі повноваження органів місцевого самоврядування». Серед інших проблем також було названо те, що «система місцевого самоврядування на сьогодні не задовольняє потреб суспільства», а також «збереження диспропорційності адміністративно-територіального устрою як основи існування нераціональної територіальної організації влади». Така диспропорція полягала у відсутності цілісної території адміністративно-територіальної одиниці базового рівня (перебування територіальної громади села, селища, міста у складі іншої територіальної громади або на території іншої адміністративно-територіальної одиниці, територіальної громади району в місті) призводить до конфлікту компетенції як між органами місцевого самоврядування, так і між органами місцевого самоврядування та місцевими органами виконавчої влади [34].

Концепція передбачала такі шляхи вирішення проблем місцевого самоврядування: 1) визначення обґрунтованої територіальної основи для діяльності органів місцевого самоврядування та органів виконавчої влади, здатних забезпечити доступність та належну якість публічних послуг, що надаються такими органами, а також

необхідної для цього ресурсної бази; 2) створення належних матеріальних, фінансових та організаційних умов для забезпечення здійснення органами місцевого самоврядування власних і делегованих повноважень; 3) розмежування повноважень у системі органів місцевого самоврядування та органів виконавчої влади на різних рівнях адміністративно-територіального устрою за принципом субсидіарності; 4) розмежування повноважень між органами виконавчої влади та органами місцевого самоврядування на засадах децентралізації влади; 5) запровадження механізму державного контролю за відповідністю Конституції та законам України рішень органів місцевого самоврядування та якістю надання населенню публічних послуг; 6) максимального залучення населення до прийняття управлінських рішень, сприяння розвитку форм прямого народовладдя; 7) удосконалення механізму координації діяльності місцевих органів виконавчої влади [34].

Нормативно-правова база децентралізації охоплювала Закон України «Про співробітництво територіальних громад» від 17 червня 2014 року, Закон України «Про добровільне об'єднання територіальних громад» від 05 лютого 2015 року та Закони, якими було внесено зміни до Бюджетного і Податкового кодексів — в аспекті фінансової децентралізації. Передбачалось три етапи децентралізації:

1) створення найнижчого адміністративно-територіального рівня — об'єднаних територіальних громад (далі — ОТГ) та передача їм частини повноважень держави, реорганізація сільських рад в ОТГ та ліквідація районів;

2) формування середнього рівня адміністративно-територіального устрою країни — районів;

3) внесення змін до Конституції України з метою закріплення конституційного статусу органів місцевого самоврядування та виконавчої влади, побудови ефективної системи територіальної організації влади в Україні [35, с. 48].

Нині в Україні утворено 1070 ОТГ, у які добровільно об'єдналися 4882 громади, що охоплює майже 47 % від загальної площі України, що є територією проживання для більше ніж 70 % населення України [37, с. 6]. Проте в силу воєнного стану процес децентралізації є незавершеним, оскільки внесення змін до Конституції України під час воєнного стану заборонено. Крім цього, з огляду на воєнний стан виникла низка інших проблемних питань: розмежування повноважень органів місцевого самоврядування та місцевими органами виконавчої влади, взаємодія з військово-цивільними адміністраціями, фінансування виконання делегованих державою повноважень, на виконання яких не виділено кошти, оновлення державної стратегії розвитку регіонів та інше.

Отже, в подальшому продовження реформи децентралізації та розвиток унітаризму в Україні в цілому буде визначатись не лише політико-правовими чинниками, але й зазнаватиме впливу обставин, зумовлених воєнним станом.

4. Висновки

Підсумовуючи викладене, можна дійти висновку, що унітаризм є багатоаспектним поняттям, який охоплює різні елементи конституційного ладу: державний та адміністративно-територіальний устрій, принципи територіального управління та його взаємодії з органами місцевого самоврядування.

Основні засади унітаризму в Україні визначені у Конституції України, які з огляду на їх конституційний статус становлять підґрунтя для розвитку положень про унітаризм у інших нормативно-правових актах. При цьому виклад засад унітаризму в Конституції України відрізняється від регламентації відповідних положень у Основних законах зарубіжних країн. У Конституції України засади унітаризму висвітлені у різних розділах та контекстах, включаючи загальні засади конституційного ладу, організацію державної влади,

розподіл повноважень між гілками влади, адміністративно-територіальний устрій та місцеве самоврядування. У Конституції Польщі, Конституції Італії та Конституції Франції, висвітлення засад унітаризму переважають у положеннях про територіальний устрій, які, крім положень про адміністративно-територіальний поділ, також охоплюють порядок здійснення місцевого самоврядування, політико-правові відносини місцевих державних та центральних державних органів влади, а також побудову співпраці місцевих державних органів влади та органів місцевого самоврядування.

Зарубіжний досвід унітаризму, зокрема, у Франції та Італії, характеризується тенденцією до регіоналізації, що базується на стратегії розширення повноважень регіонів. Проте в Україні регіоналізація може набути потенційно небезпечних ознак з огляду на воєнний стан, необхідність подолання тоталітарного минулого і формування єдиної української ідентичності. З огляду на викладене, для України більш вдалішим кроком є продовження реформи децентралізації, що полягає у перенесенні низки владних повноважень від рівня державної влади до рівня органів місцевого самоврядування.

Список використаних джерел:

1. Погорілко В. Ф. Територіальний устрій. Юридична енциклопедія : в 6 т. / редкол.: Ю. С. Шемшученко та ін. Київ : Українська Енциклопедія, 1998. Т. 6 : Т–Я. С. 42

2. Конституція України в редакції від 28.06.1996. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/ed19960628/conv#o578

3. Кампо В. Федералізація: чому це небезпечно? Главком. URL: https://glavcom.ua/columns/kampo/123845-federalizatsija.-chomu-tse-nebezpechno.html

4. Словник української мови : в 11 тт. / АН УРСР. Інститут мовознавства ; за ред. І. К. Білодіда. К. Наукова думка, 1970–1980. Портал

української мови та культури. URL: https://slovnyk.ua/index.php?swrd=%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD

5. Стацюк Р. В. Основні підходи до визначення поняття «термін» у сучасній лінгвістичній науці. *Науковий вісник Дрогобицького державного педагогічного університету імені Івана Франка. Серія: Філологічні науки (мовознавство)*. 2016. № 5 (2). С. 112–116. URL: http://nbuv.gov.ua/UJRN/nvddpufm_2016_2_5_29

6. Артикуца Н. В. Основи вчення про юридичний термін і юридичну термінологію. [препринт]. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/3a35a1ce-87c6-41d2-8cb9-708795424cb0/content

7. Конверський А. Є. Логіка. Київ : ВПЦ «Київський університет», 2017. 391 с. URL: http://philosophy.univ.kiev.ua/uploads/editor/Files/LIBRARY/KONVERSKII/1.pdf

8. Батанов О. В. Унітаристика у системі наукових знань про унітаризм: проблеми концептуалізації та інституціоналізації. *Університетські наукові записки*. 2020. Т. 19. № 1 (73). С. 18–34. URL: https://unz.univer.km.ua/article/download/73_18-34/pdf/

9. Сучасний унітаризм: доктрина і практика : монографія / Ю. С. Шемшученко, О. В. Скрипнюк, О. В. Батанов та ін. Київ : Вид-во «Юридична думка», 2021. 516 с.

10. Батанов О. В. Муніципально-правовий вимір унітаризму в Україні: проблеми та виклики. *Муніципальна реформа в контексті євроінтеграції України: позиція влади, науковців, профспілок та громадськості* : зб. тез доповідей. Київ : АПСВТ. 2020. С. 28–38.

11. Батанов О. В. Концептуальні проблеми сучасного унітаризму. *Часопис Київського університету права*. 2020. (1). 87–92. URL: https://chasprava.com.ua/index.php/journal/article/view/262

12. Кушніренко О. Унітаризм як базова цінність конституційного ладу України. *Віче*. 2012. № 2. С. 17–20. URL: http://nbuv.gov.ua/UJRN/viche_2012_2_8

13. Шаповал В. М. Конституційний лад. Юридична енциклопедія : в 6 т. / редкол: Ю. С. Шемшученко та ін. Київ : Українська Енциклопедія, 2001. Т. 3 : К–М. С. 279

14. Ковальов Д. В., Пономаренко А. В. Політико-правові принципи конституційного ладу в Конституції Української Народної Республіки. *Політичне життя*. 2020. № 4. С. 11–16. URL: https://jpl.donnu.edu.ua/article/view/6234

15. Курцев О. Ю. Принцип унітаризму та система адміністративно-територіального устрою України. *Право та державне управління*. 2020. № 4. С. 141–147. URL: http://www.pdu-journal.kpu.zp.ua/archive/4_2020/13.pdf

16. Курцев О. Ю. Поняття та ознаки унітаризму як принципу конституційного ладу України. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2020. № 44. С. 107–112. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/1350595

17. Кушніренко О. Г. Поняття, природа і види конституційних цінностей. *Конституція як основа розвитку правової системи* : VIII Тодиківські читання : зб. тез наук. доп. і повідомл. міжнар. наук. конф. молодих учених, аспірантів і студентів (2–3 жовт. 2015 р.). Харків, 2015. С. 44–46. URL: https://dspace.nlu.edu.ua/handle/123456789/14434

18. Цінності конституційні. Мала енциклопедія конституційного права / за ред. проф. Ю. Л. Бошицького. Київський університет права НАН України. Київ : Кондор-Видавництво. 2012. 470 с.

19. Грищук О. Конституційні цінності та принципи: окремі аспекти застосування Конституційними Судами. *Конституціоналіст*. 2022. № 6. URL: https://constitutionalist.com.ua/oksana-hryshchuk-konstytutsijni-tsinnosti-ta-pryntsypy-okremi-aspekty-zastosuvannia-konstytutsijnymy-sudamy/

20. Савчин М. В. Конституційне право України. Київ : Правова єдність, 2009. 1008 с.

21. Міщук В. В. Унітарна форма територіального устрою України, Польщі та Італії (порівняльно-правовий аналіз) : автореф. дис. на здоб. наук. ступ. канд. юрид. наук. Київ. 2011. 24 с.

22. Батанов О. В. Унітаризм як політичний та правовий феномен: вітчизняний та зарубіжний досвід. *Вісник Донецького національного університету імені Василя Стуса. Серія: Політичні науки*. 2019. № 4. С. 20–25. URL: http://nbuv.gov.ua/UJRN/vdonnupn_2019_4_5

23. Сєрік М. В. Теоретичний аналіз сутності поняття «громадянськість». *Науковий вісник Донбасу*. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/nvd_2013_1_29

24. Явір В. В. Україна унітарна: аналіз цивілізаційного вибору форми державного устрою. *Політикус*. 2020. № 5. С. 166–171. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/10378/1/Yavir.pdf

25. Рішення Конституційного Суду України у справі за конституційним поданням виконуючого обов'язки Президента України, Голови Верховної Ради України щодо відповідності Конституції України (конституційності) Постанови Верховної Ради Автономної Республіки Крим «Про Декларацію про незалежність Автономної Республіки Крим і міста Севастополя»: судовий акт від 20 березня 2014 року № 3-рп/2014. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/v003p710-14#Text

26. Конституція Польської Республіки / ред. В. М. Шаповала. Київ : Москаленко О. М., 2018. 82 с.

27. Конституція Французької Республіки / ред. В. М. Шаповала. Київ : Москаленко О. М., 2018. 56 с.

28. Конституція Італійської Республіки / ред. В. М. Шаповала. Київ : Москаленко О. М., 2018. 62 с.

29. Панов А. В. Територіальний устрій Франції та Італії — уроки для України : монографія. Ужгород : ПП «АУТДОР-ШАРК», 2015. 126 с.

30. Рафальський О. Регіоналізм в Україні: проблеми і перспективи. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України*. 2010. Вип. 2. С. 22–29. URL: http://nbuv.gov.ua/UJRN/Nzipiend_2010_2_4

31. Янковська Г. В. Функції державної мови. *Юридичний науковий електронний журнал*. 2014. № 5. С. 23–27. URL: http://lsej.org.ua/5_2014/7.pdf

32. Бариська Я. О., Попович Т. П. Децентралізація публічної влади (досвід Польщі та Угорщини). *Науковий вісник Ужгородського Національного університету. Серія: Право*. Ужгород : Видавничий дім «Гельветика». 2017. Т. 1. Вип. 45. С. 69–73. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/34090

33. Гудзь Л. В. Польська та українська моделі децентралізації: порівняльний аналіз. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Право,* 2020. № 29. С. 91–96. DOI: https://doi.org/10.26565/2075-1834-2020-29-11.

34. Концепція реформування місцевого самоврядування та територіальної організації влади в Україні від 01.04.2014 р. № 333-р. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/333-2014-%D1%80#Text

35. Лелеченко А. П., Васильєва О. І., Куйбіда В. С., Ткачук А. Ф. Місцеве самоврядування в умовах децентралізації повноважень : навч. посібник. Київ, 2017. 110 с.

36. Захарченко О. Взаємозв'язок між децентралізацією та європейською інтеграцією. Центр «Нова Європа». 2020. 30 с. URL: http://neweurope.org.ua/wp-content/uploads/2020/02/Decentralization_ukr_web-2.pdf

References:

1. Pohorilko, V. F. Territorial system. Legal encyclopedia in 6 volumes / Ed.: Yu. s. Shemshuchenko et al. Kyiv: Ukrainian Encyclopedia, 1998. T. 6: T–Ya. P. 42

2. Constitution of Ukraine as amended on 28.06.1996. Legislation of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/ed19960628/conv#o578

3. Campo, V. Federalization: why is it dangerous? Commander-in-Chief. Retrieved from https://glavcom.ua/columns/kampo/123845-federalizatsija.-chomu-tse-nebezpechno.html

4. Dictionary of the Ukrainian language: in 11 vols. / Academy of Sciences of the Ukrainian SSR. Institute of Linguistics; ed. I. K. Bilodid. K.: Naukova dumka, 1970–1980. Portal of the Ukrainian language and culture. Retrieved from https://slovnyk.ua/index.php?swrd=%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD

5. Statsyuk, R. V. Main approaches to the definition of the concept of "term" in modern linguistic science. *Scientific Bulletin of the Ivan Franko Drohobych State Pedagogical University. Series: Philological Sciences (Linguistics)*. 2016. No. 5(2). P. 112–116. Retrieved from http://nbuv.gov.ua/UJRN/nvddpufm_2016_2_5_29

6. Artikutsa, N. V. Fundamentals of the doctrine of the legal term and legal terminology. [preprint]. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/3a35a1ce-87c6-41d2-8cb9-708795424cb0/content

7. Konverskyi, A. E. Logic. Kyiv: VPC "Kyiv University", 2017. 391 p. Retrieved from http://philosophy.univ.kiev.ua/uploads/editor/Files/LIBRARY/KONVERSKII/1.pdf

8. Batanov, O. V. Unitarianism in the system of scientific knowledge about Unitarianism: problems of conceptualization and institutionalization. *University Scientific Notes*. 2020. Vol. 19. No. 1 (73). P. 18–34. Retrieved from https://unz.univer.km.ua/article/download/73_18-34/pdf/

9. Modern Unitarianism: doctrine and practice: monograph / Yu. S. Shemshuchenko, O. V. Skrypnyuk, O. V. Batanov and others. Kyiv: Publishing house "Yurydychna Dumka". 2021. 516 p.

10. Batanov, O. V. Municipal and legal dimension of unitarism in Ukraine: problems and challenges. Municipal reform in the context of European integration of Ukraine: the position of the authorities, scientists, trade unions and the public: collection of abstracts. Kyiv: APSVT. 2020. P. 28–38.

11. Batanov, O. V. Conceptual problems of modern unitarism. *Journal of the Kyiv University of Law*. 2020. (1), 87–92. Retrieved from https://chasprava.com.ua/index.php/journal/article/view/262

12. Kushnirenko, O. Unitarism as a basic value of the constitutional order of Ukraine. *Viche*. 2012. No. 2. P. 17–20. Retrieved from http://nbuv.gov.ua/UJRN/viche_2012_2_8

13. Shapoval, V. M. Constitutional system. Legal encyclopedia in 6 volumes / Editorial staff: Yu. S. Shemshuchenko et al. Kyiv: Ukrainian Encyclopedia, 2001. Vol. 3: K–M. P. 279

14. Kovalev, D. V., Ponomarenko, A. V. Political and legal principles of the constitutional system in the Constitution of the Ukrainian People's Republic. *Political life*. 2020. No. 4. P. 11–16. Retrieved from https://jpl.donnu.edu.ua/article/view/6234

15. Kurtsev, O. Yu. The principle of unitarism and the system of administrative-territorial organization of Ukraine. *Law and public administration*. 2020. No. 4. P. 141–147. Retrieved from http://www.pdu-journal.kpu.zp.ua/archive/4_2020/13.pdf

16. Kurtsev, O. Yu. The concept and features of unitarism as a principle of the constitutional order of Ukraine. *Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence*. 2020. No. 44. P. 107–112. Retrieved from https://journals.indexcopernicus.com/api/file/viewByFileId/1350595

17. Kushnirenko, O. G. Concept, nature and types of constitutional values. *Constitution as a basis for the development of the legal system*. VIII Todykiv Readings: collection of theses of scientific. additional. and reports of the international scientific. conference of young scientists, postgraduates and students (October 2–3, 2015). Kharkiv, 2015. Pp. 44–46. Retrieved from https://dspace.nlu.edu.ua/handle/123456789/14434

18. Constitutional values. Small encyclopedia of constitutional law. Edited by prof. Yu. L. Boshytsky. Kyiv University of Law of the NAS of Ukraine. Kyiv: Condor-Publishing House. 2012. 470 p.

19. Hryshchuk, O. Constitutional values and principles: some aspects of application by the Constitutional Courts. Constitutionalist. 2022. No. 6. Retrieved from https://constitutionalist.com.ua/oksana-hryshchuk-konstytutsijni-tsinnosti-ta-pryntsypy-okremi-aspekty-zastosuvannia-konstytutsijnymy-sudamy/

20. Savchyn, M. V. Constitutional law of Ukraine. Kyiv: Legal unity, 2009. 1008 p.

21. Mishchuk, V. V. Unitary form of territorial organization of Ukraine, Poland and Italy (comparative legal analysis): author's abstract of dissertation for the degree of candidate of legal sciences. Kyiv, 2011. 24 p.

22. Batanov, O. V. Unitarianism as a political and legal phenomenon: domestic and foreign experience. *Bulletin of the Vasyl Stus Donetsk National University. Series: Political Sciences*. 2019. No. 4. P. 20–25. Retrieved from http://nbuv.gov.ua/UJRN/vdonnupn_2019_4_5.

23. Serik, M. V. Theoretical analysis of the essence the concept of "citizenship". Scientific Bulletin of Donbass. 2013. No. 1. Retrieved from http://nbuv.gov.ua/UJRN/nvd_2013_1_29

24. Yavir, V. V. Unitary Ukraine: Analysis of the Civilizational Choice of the Form of State System. *Politicus*. 2020. No. 5. Pp. 166–171. Retrieved from http://dspace.pdpu.edu.ua/bitstream/123456789/10378/1/Yavir.pdf

25. Decision of the Constitutional Court of Ukraine in the case on the constitutional submission of the Acting President of Ukraine, Chairman of the Verkhovna Rada of Ukraine on the compliance with the Constitution of Ukraine (constitutionality) of the Resolution of the Verkhovna Rada of the Autonomous Republic of Crimea "On the Declaration of Independence of the Autonomous Republic of Crimea and the City of Sevastopol": judicial act of March 20, 2014 No. 3-рп/2014. Legislation of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/v003p710-14#Text

26. Constitution of the Republic of Poland: edited by V. M. Shapoval. Kyiv: Moskalenko O. M. 2018. 82 p.

27. Constitution of the French Republic: edited by V. M. Shapoval. Kyiv: Moskalenko O. M. 2018. 56 p.

28. Constitution of the Italian Republic: edited by V. M. Shapoval. Kyiv: Moskalenko O. M. 2018. 62 p.

29. Panov, A. V. Territorial structure of France and Italy — lessons for Ukraine: Monograph. Uzhgorod: PP "OUTDOOR-SHARK". 2015. 126 p.

30. Rafalsky, O. Regionalism in Ukraine: problems and prospects. *Scientific notes of the Institute of Political and Ethnonational Studies named after I. F. Kuras of the NAS of Ukraine*. 2010. Issue 2. P. 22–29. Retrieved from http://nbuv.gov.ua/UJRN/Nzipiend_2010_2_4

31. Yankovska, G. V. Functions of the state language. *Legal scientific electronic journal*. 2014. No. 5. P. 23–27. Retrieved from http://lsej.org.ua/5_2014/7.pdf

32. Baryska, Ya. O., Popovych T.P. Decentralization of public power (the experience of Poland and Hungary). *Scientific Bulletin of the Uzhhorod National University. Series: Law*. Uzhhorod: Publishing House "Helvetica". 2017. T. 1. Issue. 45. P. 69–73. Retrieved from https://dspace.uzhnu.edu.ua/jspui/handle/lib/34090

33. Gudz, L. V. Polish and Ukrainian models of decentralization: comparative analysis. *Bulletin of the V. N. Karazin Kharkiv National University. Series: Law*. 2020. No. 29. P. 91–96. https://doi.org/10.26565/2075-1834-2020-29-11.

34. Concept of reforming local self-government and territorial organization of power in Ukraine dated 01.04.2014 No. 333-r. Legislation of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/333-2014-%D1%80#Text

35. Lelechenko, A. P., Vasilyeva, O. I., Kuybida, V. S., Tkachuk, A. F. Local self-government in the context of decentralization of powers: a textbook. Kyiv, 2017. 110 p.

36. Zakharchenko, O. The relationship between decentralization and European integration. New Europe Center. 2020. 30 p. URL: http://neweurope.org.ua/wp-content/uploads/2020/02/Decentralization_ukr_web-2.pdf

ТЕОРЕТИКО-ІДЕОЛОГІЧНІ ЗАСАДИ ПОЛІТИЧНОЇ ЛЕГІТИМАЦІЇ РОСІЙСЬКОГО ОКУПАЦІЙНОГО РЕЖИМУ

THEORETICAL AND IDEOLOGICAL FOUNDATIONS OF THE POLITICAL LEGITIMIZATION OF THE RUSSIAN OCCUPATION REGIME

Iastrebova V. A.,
Doctor of Philosophy in Political Science,
Director of the NGO&quot, Eastern Human Rights Group&quot,
PhD student at the I. F. Kuras Institute of Political
and Ethno-National Studies,
NAS of Ukraine,
Odesa, Ukraine

Abstract. The chapter of the monograph is devoted to a comprehensive conceptualization of the theoretical and ideological foundations of the political legitimation of the Russian occupation regime as a phenomenon shaped by the combination of geopolitical ambitions, imperial historical tradition, information and propaganda technologies, and the instrumentalization of law. The main idea of the study is to demonstrate that the legitimation of the occupation authority is not a situational political process, but constitutes a systemic ideological construction aimed at creating an illusion of legality of control over occupied territories and substituting the principles of international law with political and propaganda narratives.

The subject of the research includes ideological doctrines, political and legal arguments, and communicative mechanisms used to justify

occupation and to construct the appearance of legitimacy of power. Particular attention is paid to the transformation of the concepts of sovereignty, self-determination of peoples, security, and historical justice within propaganda discourse, as well as to the role of pseudo-referendums, normative acts of occupation administrations, and information campaigns in constructing the illusion of legal legitimacy.

The aim of the monograph chapter is to provide a comprehensive analysis of theoretical ideologemes and political-legal mechanisms of legitimizing the Russian occupation regime, taking into account the norms of international law, the practice of international organizations, and the experience of countering occupation regimes. The study is aimed at substantiating the necessity of developing effective legal and informational strategies for delegitimizing occupation authorities and restoring internationally recognized legal order.

The research methodology is based on a combination of general scientific and special legal approaches. The dialectical method is used to analyze the evolution of imperial ideologemes in contemporary political discourse; the system approach is applied to examine the legitimation of occupation authority as a complex interaction of political, legal, and informational instruments; the comparative legal method is used to study international standards regarding occupation and annexation of territories; formal-legal and hermeneutic methods are applied to analyze normative acts, decisions of international institutions, and propaganda texts. The conceptual foundation is formed by theories of political legitimacy, hybrid warfare, and informational influence.

The conclusions substantiate that the legitimation of the Russian occupation regime has a multidimensional character, combining ideological, legal, informational, and symbolic elements. Its implementation occurs through two complementary pathways: through manipulative interpretation of international legal principles

and through the creation of pseudo-legal mechanisms designed to imitate democratic procedures. The effectiveness of countering such legitimation depends on a comprehensive system of legal, diplomatic, informational, and educational measures. The study demonstrates that the delegitimization of occupation regimes is a continuous process aimed at restoring the principles of sovereignty, territorial integrity, and the rule of international law. It is precisely the combination of legal instruments and strategic communications that creates the prerequisites for protecting democratic values and ensuring a just international order.

Keywords: Political legitimation, Occupation regime, Ideological foundations, Russian aggression, Propaganda, "Russian world" (Russkiy mir), Geopolitical doctrine, Historical revisionism.

1. Вступ

Трансформація сучасного геополітичного порядку та зростання ролі гібридних форм ведення війни зумовлюють появу нових механізмів встановлення та утримання контролю над територіями без формального визнання суверенітету. У цьому контексті російська агресія проти України супроводжується не лише воєнною окупацією, а й системною політико-ідеологічною діяльністю, спрямованою на створення видимості правомірності встановленої влади. Легітимація окупаційного режиму здійснюється через поєднання історичних наративів, ідеологічних доктрин, інформаційно-пропагандистських стратегій та псевдоправових механізмів, що покликані сформувати уявлення про законність зміни політико-правового статусу територій. За таких умов легітимація окупаційної влади постає як самостійний об'єкт політико-правового аналізу.

Актуальність дослідження зумовлена необхідністю теоретичного осмислення механізмів політичної легітимації російського окупаційного режиму та вироблення ефективних інструментів

його делегітимації у міжнародно-правовому та інформаційному просторі. Окупаційна влада прагне створити ілюзію правомірності через маніпулятивне тлумачення принципів самовизначення народів, безпеки, історичної справедливості та захисту населення. Водночас відбувається системне порушення норм міжнародного гуманітарного права, принципів суверенітету і територіальної цілісності держав. Це потребує формування сучасних наукових підходів до аналізу ідеологічних і правових інструментів легітимації окупації та розроблення стратегій протидії таким практикам. Особливої ваги набуває дослідження цієї проблематики в умовах європейської інтеграції України та посилення ролі міжнародних інституцій у відновленні правопорядку.

Наукова новизна дослідження полягає у комплексному розгляді політичної легітимації окупаційного режиму як багатовимірного явища, що формується на перетині політичних, правових, ідеологічних та інформаційних процесів. У роботі обґрунтовується підхід до легітимації не лише як до правової чи політичної процедури, а як до цілеспрямованої ідеологічної конструкції, що спрямована на формування уявної законності окупаційної влади. Запропоновано системне бачення механізмів легітимації через поєднання пропагандистських наративів, псевдодемократичних процедур і нормативної імітації правового порядку, а також розкрито роль інформаційного впливу у формуванні суспільного сприйняття окупації.

Метою дослідження є з'ясування за результатами комплексного аналізу теоретико-ідеологічних засад політичної легітимації російського окупаційного режиму та обґрунтування підходів до його делегітимації в умовах сучасного міжнародного правопорядку.

Для досягнення поставленої мети визначено такі науково-дослідницькі завдання: дослідити воєнний догматизм як системоутворювальний елемент ідеологічної доктрини окупаційної політики агресора та з'ясувати його роль у виправданні війни

й територіальної експансії; проаналізувати засади мілітаризації суспільної свідомості та механізми політичної соціалізації населення в умовах окупаційного режиму; розкрити ідеологічні основи та пропагандистські дискурси легітимації окупаційної влади як інструменти символічного домінування; визначити взаємозв'язок воєнної ідеології, мілітаризованих наративів і інформаційного впливу у формуванні видимості правомірності окупаційного порядку.

Методологія дослідження базується на поєднанні загальнонаукових і спеціально-правових методів. Діалектичний метод дозволив простежити еволюцію імперських ідеологем та їх трансформацію у сучасному політичному дискурсі. Системний підхід застосовано для аналізу легітимації окупаційного режиму як складної взаємодії політичних, правових та інформаційних інструментів. Порівняльно-правовий метод використано для дослідження міжнародних стандартів щодо окупації та анексії територій і практики їх застосування. Формально-юридичний та інтерпретаційний методи забезпечили аналіз нормативних актів окупаційної влади, рішень міжнародних організацій та пропагандистських текстів. Концептуальною основою дослідження виступають теорії політичної легітимності, гібридної війни та стратегічних комунікацій.

Логіка подання матеріалу зумовлена метою та завданнями дослідження. У першому параграфі аналізується воєнний догматизм як системоутворювальний елемент ідеологічної доктрини окупаційної політики агресора та його роль у виправданні війни й експансії. Другий параграф присвячений дослідженню мілітаризації суспільної свідомості та механізмів політичної соціалізації населення в умовах окупаційного режиму. У третьому параграфі розкриваються ідеологічні засади та пропагандистські дискурси легітимації окупаційної влади як інструменти символічного домінування і формування уявної правомірності політичного контролю. Така

структура забезпечує послідовний перехід від аналізу ідеологічних основ окупаційної політики до дослідження механізмів впливу на суспільну свідомість і засобів символічної легітимації влади.

1. Специфіка воєнного догматизму як системоутворювального елементу ідеологічної доктрини окупаційної політики агресора

У зовнішній політиці на рішення часто впливає певна політична ідеологія, прийнята політичними елітами, яка може формувати їхнє сприйняття світу та керувати їхніми діями. Однак, коли ідеологія стає догматичною, це може призвести до хибних сприйняттів та непорозумінь, які можуть мати серйозні наслідки для міжнародних відносин. Будь-яка ідеологія використовує спрощений та більшменш упереджений образ реальності, але А. Гат зазначає, що що «всі ідеологічні фактичні твердження є недійсними, однаково оманливими або однаково міфічними» [1, с. 38].

Так, з моменту розпаду Радянського Союзу Росія намагається визначити свою роль у міжнародній системі. Багато російських політиків та аналітиків вважають, що Захід, зокрема Сполучені Штати, вороже налаштований до Росії та прагне підірвати її інтереси. Цей світогляд дедалі більше формується догматичною ідеологією, яка розглядає Росію як жертву безжального експансіонізму Заходу та виправдовує її агресивні дії як оборонні, провокативні відповіді на уявні загрози [1, с. 37].

Ця догматична ідеологія, що діє як когнітивний фільтр та директивне керівництво, сприяла хибним уявленням та непорозумінням у зовнішній політиці Росії щодо України. Коли проросійський президент України Віктор Янукович був усунений у результаті народного повстання у 2014 році (Євромайдан), Росія розцінила це як доказ західної змови та загрозу своїм інтересам. Російський уряд відповів анексією Криму та підтримкою сепаратистів-повстанців на сході України. Залежність від обраного шляху, що базується

на цьому хибному сприйнятті, призвела російське керівництво до ще більш дороговартісних помилок, особливо до повномасштабного вторгнення, яке розпочалося 24 лютого 2022 року [2].

З самого початку дії Росії ґрунтувалися на хибному сприйнятті. Росія розглядала повстання в Україні як підтримуваний Заходом державний переворот, хоча насправді це був масовий рух проти корумпованого та авторитарного уряду. Підтримуючи сепаратистів-повстанців на сході України, Росія також неправильно сприйняла ситуацію на місцях.

Такі уявлення, створені догматичною ідеологією, мали серйозні наслідки для міжнародних відносин. Дії Росії в Україні призвели до економічних санкцій та дипломатичної ізоляції, різко погіршивши її відносини із Заходом та його союзниками. Конфлікт на сході України також призвів до тисяч смертей, мільйонів переміщених осіб та відновлення давно прихованих побоювань щодо військового конфлікту між НАТО та Росією в Європі та навіть ядерної ескалації. Безумовно, що хибні уявлення у зовнішній політиці агресора частково є побічним продуктом надзвичайно догматичної ідеології, яка може радикально спотворювати образ реальності, засліплюючи політиків щодо альтернативних точок зору та доказів.

Роберт Джервіс визначає хибне сприйняття як «різницю між тим, як актор сприймає міжнародну ситуацію, і тим, якою ця ситуація є насправді» [3]. Іншими словами, хибне сприйняття виникає, коли особи, які приймають рішення, неправильно розуміють або неправильно інтерпретують інформацію про ситуацію, що призводить до помилкових політичних рішень. Джервіс стверджує, що хибне сприйняття є поширеним явищем у міжнародній політиці через низку факторів, включаючи неповну інформацію, когнітивні упередження та складність точного прогнозування поведінки інших акторів. Він визначає три категорії хибного сприйняття: хибне

сприйняття намірів інших, хибне сприйняття можливостей інших та хибне сприйняття наслідків власних дій [3].

Неправильне сприйняття намірів інших стосується ситуацій, коли особи, що приймають рішення, помилково вважають, що інші суб'єкти мають ворожі наміри, хоча насправді це не так (і навпаки). Це може призвести до спіралі недовіри та конфлікту, оскільки кожна сторона вважає, що інша діє агресивно. Неправильне сприйняття можливостей інших виникає, коли особи, що приймають рішення, переоцінюють або недооцінюють військову, економічну чи політичну силу інших суб'єктів. Це може призвести до неправильних розрахунків щодо потенційного успіху чи невдачі військових втручань чи дипломатичних переговорів. Неправильне сприйняття наслідків власних дій виникає, коли особи, що приймають рішення, не можуть точно передбачити реакцію інших суб'єктів на власні дії. Це може призвести до непередбачуваних наслідків, таких як ескалація конфліктів або непередбачувані союзи, або, як у цьому випадку, виконання декларацій союзу (НАТО).

Загалом, Джервіс стверджує, що неправильне сприйняття є поширеним і небезпечним явищем у міжнародній політиці, яке може призвести до катастрофічних політичних рішень та ескалації конфліктів. Щоб запобігти хибному сприйняттю, особи, що приймають рішення, повинні усвідомлювати власні когнітивні упередження та обмеження, збирати точну інформацію та враховувати різні точки зору на ситуацію [3].

Так, Я. Верцбергер пропонує типологічну основу для аналізу хибного сприйняття в міжнародній політиці. Автор визначає чотири типи хибного сприйняття: перцептивне спрощення, перцептивне викривлення, когнітивна жорсткість та ідеологічно викликане хибне сприйняття. Перцептивне спрощення виникає, коли особи, які приймають рішення, спрощують складну ситуацію, надмірно спрощуючи її до бінарних термінів. Перцептивне

викривлення виникає, коли особи, які приймають рішення, розглядають ситуацію на основі власного досвіду та упереджень [1, с. 39].

Когнітивна жорсткість стосується нездатності осіб, які приймають рішення, коригувати своє сприйняття у відповідь на нову інформацію. Нарешті, ідеологічно викликане хибне сприйняття виникає, коли дотримання ідеології особами, які приймають рішення, призводить до хибного сприйняття ситуації. З часом розрив між реальністю та сприйняттям може або збільшуватися (дезадаптація), залишатися незмінним (неадаптація), або зменшуватися (адаптація).

У свою чергу, догматична ідеологія стосується жорсткого та безкомпромісного набору переконань та цінностей, які стійкі до змін та альтернативних перспектив, часто характеризуючись непохитною відданістю певній доктрині чи світогляду. Догматична ідеологія може негативно впливати на прийняття рішень та сприйняття, оскільки окремі особи та колективи можуть категорично відкидати або ігнорувати інформацію, яка суперечить їхнім попереднім переконанням, і можуть чинити опір зміні своїх позицій навіть перед обличчям нових доказів. Це може призвести до неправильного сприйняття та поляризації в політичному дискурсі, оскільки окремі особи стають більш закріпленими у своїх переконаннях та менш охочими до конструктивного діалогу [3].

Зв'язок між догматизмом та неправильними сприйняттями добре вивчається у літературі з соціальної психології та політології. Дослідження показали, що догматична ідеологія може призвести до неправильних сприйняттів у різних сферах, включаючи політику, релігію та науку. Наприклад, у політичному контексті догматичні особистості можуть бути більш схильні до неправильного сприйняття мотивів та намірів протилежних політичних груп, що призводить до посилення поляризації та конфліктів. У науці догматичні особистості можуть бути більш схильні до прийняття нових доказів, які суперечать їхнім попереднім переконанням, що призводить

до відсутності прогресу та інновацій. Крім того, догматичні особистості також можуть бути більш схильні до дезінформації та пропаганди, оскільки вони менш схильні критично оцінювати точність та достовірність інформації. Це може призвести до неправильних сприйняттів щодо важливих питань та подій, таких як теорії змови або хибні переконання щодо наукових явищ [1, с. 40].

Протягом останніх приблизно дванадцяти років спостерігаються дедалі чіткіші ознаки трансформації Росії з досить безідеологічної, авторитарної, клептократичної політичної системи, що базується на соціально-політичній масовій демобілізації та обіцянці відносної матеріальної стабільності, на типовий радикальний інструмент управління терором.

Однією з ранніх ознак цього процесу була сек'юритизація так званих духовно-моральних цінностей протягом приблизно десятиліття, особливо як реакція на масові протести після виборів до Державної Думи у грудні 2011 року. Як зазначав Ярдар Остбе, у Стратегії національної безпеки Росії 2015 року «збереження традиційних цінностей» «визначено як найважливішу стратегічну мету, термін «духовний» зустрічається 15 разів у документі, а духовна сфера виділяється як один із секторів (поряд з економічним, політичним та військовим), де Російська Федерація повинна розвивати свій потенціал» [4].

Естбе справедливо зазначив, що в російському гегемоністському дискурсі духовно-моральні цінності «трактуються як щось самоочевидне, вічне, абсолютне та незмінне, але також як щось, що перебуває під атакою та має бути захищене» [4]. Як ми стверджували вище, ідея ідеологічного «безпечного простору», що вимагає «знезараження» та захисту від зовнішніх та внутрішніх ворогів, є одним з елементів радикального механізму управління тероризмом. Він неодноразово характеризується набором специфічних параметрів, що виникають в результаті функцій, що виконуються цим типом системи.

Сучасна Росія чудово відповідає критеріям еволюції від клептократичного режиму до радикального механізму управління тероризмом. Вторгнення в Україну було одночасно наслідком і паливом для цього механізму. Як таке, воно відображає взаємно-оберальні стосунки. Немає сумнівів, що путінізм наразі є сильно догматичною ідеологією, яка вимірюється жорсткістю переконань, замкнутістю, нетерпимістю до інакомислення та абсолютистським мисленням. У процесі прийняття рішень у Росії вони чітко бачать сильні ознаки перцептивного спотворення, когнітивної ригідності та ідеологічно спричиненого хибного сприйняття, що робить цю систему дуже вразливою до дезадаптації [4].

З часом найнепохитніші догматичні системи руйнуються або радикально трансформуються через кумулятивний вплив хибного сприйняття. Чим товстіший і непроникніший захисний «броня проти реальності», тим складніше завдання підтримувати мобільність та гнучкість. Стає важче встигати за змінами в середовищі та забезпечити достатню вільність сприйняття від небезпечних спотворень. Відсікання сигналів від середовища, які породжують психологічний дискомфорт і соціальну тривогу, створює розрив між реальністю та сприйняттям, створюючи інформаційний вакуум, заповнений переконливими, але потенційно смертельними індивідуальними та колективними фантазіями.

Зрештою, проблеми, пов'язані з фактичним середовищем безпеки та реальною діяльністю конкурентів і ворогів, роблять стратегічний, політичний та ідеологічний ескапізм дуже ризикованим і дорогим вибором. Це одна з причин, чому Росія, через серйозні хибні уявлення про навколишню реальність, вирішила вторгнутися в Україну. Вона відмовилася від високоефективної стратегії гібридної війни заради відкритого конфлікту, який приніс приниження російським збройним силам та знецінення на міжнародному рівні [4].

Тому, актуальною залишається позиція Завгородньої Ю. В., яка стверджує, що для української державної політики «повномасштабна війна прискорила ряд політичних рішень, які не визначались першочерговими, проте повномасштабна війна сприяла актуалізації безпекових питань в усіх сферах та площинах» [5]. Звичайно, збройна агресія проти України виступила каталізатором трансформації державної політики, спричинивши прискорену інституціоналізацію рішень, що раніше не належали до пріоритетних, та зумовивши сек'юритизацію публічної політики, у межах якої безпековий вимір набув системоутворювального характеру в усіх сферах суспільного розвитку. В свою чергу і ворог розпочав активніше розвиватись і формувати свої ідеологічні переконання з більшою силою не лише на окупованих територіях України, а й на переважній більшості розвинутої території Росії.

Повномасштабне російське вторгнення в Україну стало одним із найбільших конфліктів у Європі з часів Другої світової війни за масштабами агресії, геополітичними наслідками для відносин між міжнародними «великими державами», геополітичними трансформаціями у сфері міжнародної безпеки, найочевиднішою з яких є вступ Фінляндії до НАТО та готовність Швеції приєднатися до цієї організації, і, звичайно ж, масштабами кризи біженців.

Порівняно з іншими нещодавніми війнами, російське вторгнення вплинуло на глобальні погляди на міжнародну продовольчу безпеку, ланцюги поставок, відносини між основними міжнародними суб'єктами та інші глобальні проблеми. Це складне питання, яке включає не лише територіальні суперечки, а й конфлікти між цивілізаційними та геополітичними одиницями з дуже різними національними підходами.

Російська агресія проти України розпочалася таким чином у 2014 році з міжнародно невизнаної анексії Кримського півострова, яка була проведена гібридним способом шляхом проведення

незаконного референдуму на півострові, а також спонсорування та надання зброї сепаратистам на Донбасі, тим самим розпочавши інформаційну та ідеологічну війну проти України з різними способами впливу на соціальний та цивільний порядок. Таким чином, ми можемо спостерігати еволюцію та новизну російського підходу до війни, а війна в Україні є прикладом того, як гібридний підхід може стати домінуючим.

Так, поведінка Росії відповідає частині національної ідеології, де правлячі еліти з «старомодним» радянським способом мислення до початку війни в Україні як способу покращення позицій Російської Федерації на світовій арені та демонстрації російської могутності на міжнародному рівні.

На основі аналізу встановлено, що сучасна ідеологія агресора трансформувалася з відносно прагматичної клептократії в радикальний механізм управління терором. Фундаментом цієї трансформації є воєнний догматизм — жорстка, безкомпромісна система переконань, що базується на військовому мисленні радянського зразка.

Ідеологія агресора виконує роль «когнітивного фільтра», який радикально спотворює сприйняття реальності. Центральним елементом є міфологізація Росії як «жертви західного експансіонізму», що дозволяє інтерпретувати будь-яку зовнішню агресію як «вимушену оборону».

Особливістю російського догматизму є переведення «духовно-моральних цінностей» у площину національної безпеки. Використання терміну «духовний» як стратегічної категорії свідчить про створення ідеологічного «безпечного простору». Це вимагає постійного пошуку внутрішніх та зовнішніх ворогів для виправдання існування режиму, перетворюючи ідеологію на інструмент мобілізації через страх.

Вторгнення 24 лютого 2022 року стало найвищою точкою дезадаптації російської системи. Прагнення «старомодних» еліт

продемонструвати могутність призвело до зворотних результатів: економічна та дипломатична ізоляція РФ; глобальна зміна архітектури безпеки (вступ Фінляндії та Швеції до НАТО); сек'юритизація всіх сфер публічної політики в Україні як вимушена відповідь на екзистенційну загрозу.

Воєнний догматизм агресора створив «броні проти реальності», яка на початкових етапах забезпечувала внутрішню консолідацію, але в довгостроковій перспективі призвела до стратегічної сліпоти. Розрив між ідеологічними фантомами («державний переворот», «штучність України») та реальним станом справ став причиною військового приниження та системної кризи російської державності. Для України це означає необхідність подальшої інституціоналізації безпекових рішень, оскільки ідеологічна інерція агресора виключає можливість швидкого повернення до раціонального діалогу.

2. Засади мілітаризації суспільної свідомості в контексті політичної соціалізації російського окупаційного режиму

Дослідження засад мілітаризації суспільної свідомості в контексті політичної соціалізації російського окупаційного режиму зумовлена радикальною трансформацією політичної та ідеологічної політики Російської Федерації після початку повномасштабної війни проти України у 2022 році. Російська держава системно використовує механізми політичної соціалізації для формування мілітаризованої ідентичності громадян, зокрема через систему освіти, молодіжні військово-патріотичні організації та державну пропаганду.

В освітньому просторі активно впроваджуються програми військово-патріотичного виховання, обов'язкові ідеологічні заняття та елементи початкової військової підготовки, що спрямовані на формування лояльності до держави та готовності до участі у військових конфліктах. Аналітичні дослідження відзначають, що російська влада послідовно розширює мережу військово-патріотичних

організацій і програм, спрямованих на формування у молоді позитивного ставлення до військової служби та легітимацію агресивної зовнішньої політики держави.

Особливої актуальності ця проблематика набуває у контексті окупованих територій України, де механізми мілітаризації суспільної свідомості використовуються як інструмент політичної інтеграції та ідеологічної трансформації місцевого населення. Через освітні програми, військово-спортивні табори, діяльність молодіжних організацій та пропагандистські практики окупаційна адміністрація намагається сформувати нову політичну ідентичність, засновану на російському державному наративі та культі війни.

Такі процеси супроводжуються системною інституціоналізацією мілітаристських цінностей, що спрямована на легітимацію тривалого воєнного протистояння та мобілізацію суспільства навколо ідеології «оборони держави». Відтак дослідження засад мілітаризації суспільної свідомості дозволяє глибше зрозуміти механізми політичної соціалізації, які використовує російський режим для конструювання лояльності, підтримки війни та відтворення авторитарної політичної системи.

Так, на думку авторського колективу Еллісон Едвардс та Дженніфер Г. Мазерс «Росія приділяє велику увагу патріотичному вихованню своїх дітей та молоді, що включає заохочення їх до прославляння війни та безумовну підтримку збройних сил Росії. Зусилля держави щодо мілітаризації російської молоді прискорилися з початку повномасштабного вторгнення в Україну в лютому 2022 року та все більше спираються на привабливість героїзму та героїв як взірців для наслідування, щоб залучати та надихати молодих людей. Героїчна поведінка, пов'язана з війною, представлена як досяжний ідеал для молоді, який можна розвивати, беручи участь у низці захопливих заходів» [6].

Така позиція відображає критичний підхід до аналізу державної політики Російської Федерації щодо формування мілітаризованої

моделі політичної соціалізації молоді. Адже, практика свідчить про цілеспрямовану діяльність державних інституцій щодо конструювання специфічної системи цінностей, у якій війна та військова служба подаються як ключові елементи громадянської ідентичності. У цьому контексті мілітаризація молоді виступає інструментом політичного контролю, що сприяє легітимації агресивної зовнішньої політики держави та зниженню критичного сприйняття воєнних дій.

Водночас подібна державна політика має суперечливий і потенційно деструктивний вплив на розвиток суспільної свідомості. Надмірна героїзація війни та формування культури військового подвигу як головного соціального ідеалу обмежують розвиток критичного мислення, плюралізму поглядів і демократичних цінностей серед молоді.

Через освітні програми, молодіжні організації та інформаційні кампанії влада фактично формує одновимірну модель політичної соціалізації, у якій пріоритет надається ідеям державної сили, жертви заради держави та підтримки військових дій. У довгостроковій перспективі така практика сприяє нормалізації війни як інструменту політики та створює передумови для відтворення мілітаризованого типу політичної культури, що суперечить принципам демократичного розвитку суспільства та підриває гуманістичні засади формування громадянської свідомості. Аналітичні дослідження українських правників, журналістів, науковців та політологів проведені у 2025 році стали якісною базою підтвердження негативного окрасу сучасних мілітариських процесів, особливо відносно дітей, підлітків та молоді [7].

Встановлено, що російська держава використовує концепцію героїзму у своїх зусиллях щодо мілітаризації російських дітей: героїзм та перспектива стати героями використовуються для спонукання молоді прийняти прославляння війни та надавати безумовну підтримку російській армії. Героїчна поведінка, пов'язана

з війною, зокрема, що проявляється через минулі дії ветеранів війни, представлена як захопливі та досяжні ідеали для молоді, які можна розвивати, беручи участь в інтерактивних та емоційно сповнених заходах. Акцент на участі молоді розкриває важливість практики, і особливо ролі, яку втілення та емоції відіграють у цих практиках, як ключових механізмів повсякденної мілітаризації [6].

Так, Міністр оборони Сергій Шойгу створив Юнармію у 2016 році в рамках проекту 2016–2020 років «Патріотичне виховання громадян Росії». Вона нагадує патріотичні військові групи радянської епохи, такі як Добровільне товариство сприяння армії, ВПС та ВМС (ДОСААФ). Станом на лютий 2025 року Юнармія налічувала 1,7 мільйона членів та 89 регіональних штабів. Група зосереджується на розвитку цінностей та здібностей молоді у чотирьох сферах: духовно-моральній; соціальній; фізичній; та інтелектуальній. Це лише одна з низки ініціатив з патріотичного виховання, розпочатих російською державою з 2001 року для сприяння соціальній згуртованості та культивування самобутньої російської національної ідентичності. Як і ДОСААФ, Юнармія робить акцент на підготовці молоді до військової служби [6].

Окрім того, ті, хто досліджує мілітаризацію в західних демократичних суспільствах, наголошують, що ця практика часто є непомітною, процеси мілітаризації в Росії є набагато більш відвертими та явно керованими державою або здійснюваними окремими особами та організаціями, які користуються державною підтримкою. Ще до лютого 2022 року військові широко фігурували в повсякденному житті росіян: у екстравагантних пам'ятних заходах, присвячених минулим війнам, а також у поширених наративах, які зображують велику та потужну армію як рішення уявної вразливості Росії у ворожому світі. Жорсткий контроль держави над ландшафтом пам'яті країни, який підтримує цей світогляд, означає, що російська молодь стикається з ним через широке середовище, що охоплює

мілітаризовану масову культуру та позакласні заходи, призначені для дітей, а також у школі [6].

Тому, «Військові розваги» — це важлива концептуальна лінза для розуміння мілітаризації як процесу підготовки суспільства до прийняття ідеї війни та прийняття військових цінностей. Роджер Шталь концептуалізував військові розваги як захопливі форми розваг, які пропонують цивільному населенню «реалістичний», але безпечний досвід війни і таким чином перетворюють аудиторію з глядача війни на віртуального учасника.

Хоча російська держава передає власні наративи про героїзм воєнного часу через офіційні канали, зустрічі між ветеранами та молоддю, організовані Молодіжною армією та Волонтерами Перемоги, є ключовими місцями для інформування та натхнення молоді про героїчні вчинки воєнного часу. Акцент на особистих зустрічах між ветеранами та молоддю свідчить про те, що групи намагаються подолати деякі обмеження розуміння війни без безпосереднього особистого досвіду. Зустрічі також можуть досягати інших державних цілей, включаючи сприяння патріотизму та інтересу до російської історії серед молоді, а також надання молодим людям живих взірців для наслідування звичайних героїв. У прес-релізах груп зустрічі з ветеранами та прослуховування їхніх історій представлені як такі, що справляють сильне враження на молодих людей [10].

У розповідях підкреслюються героїчні риси ветеранів, такі як мужність, самопожертва та відданість країні й обов'язку. Існує чітка тема зображення певних героїчних якостей як притаманних російським: «російський солдат — це благородний воїн… втілення особливої сили духу: мужності, хоробрості, безкорисливості, безстрашності та доблесті» [11].

Ці чесноти слугують ознакою того, що справжній і добрий російський патріот природно діятиме, щоб «захищати» свою країну, коли це буде потрібно, а мілітаризаційний дискурс, який пропагує ідею

про те, що війна неминуча та є нормальною обставиною для російського народу, робить важливість цих тверджень про російський характер ще більш переконливою, оскільки це натякає на те, що молодь одного дня матиме можливість продемонструвати їх. Нормальність війни також передається в переказі історій ветеранів молодим людям шляхом вбудовування їхнього воєнного досвіду в їхнє звичайне цивільне життя до та після війни. Дорослі лідери «Молодіжної армії» та «Добровольців Перемоги» могли б зосередитися лише на героїчних вчинках воєнного часу. Натомість акцент — іноді значний — робиться на довоєнному та післявоєнному житті [10].

Будь-хто може бути героєм. Ця оманливо проста ідея лежить в основі важливого та амбітного напрямку патріотичного виховання в путінській Росії. Завдяки заходам, організованим популярними державними молодіжними групами, такими як «Молодіжна армія» та «Волонтери перемоги», дітям та молоді в Росії надається можливість не лише уявити себе героями, а й пережити дуже схожий досвід на досвід героїв воєнного часу, особливо героїв найвідомішої історичної події останнього часу в Росії: Великої Вітчизняної війни [6].

Завдяки особистим зустрічам з ветеранами війни, а також за допомогою захопливих та інтерактивних методів, молоді люди можуть не лише чути та бачити, але й торкатися та відчувати аспекти життя у військових та воєнних умовах, включаючи переживання деяких емоцій, викликаних таким досвідом. На нашу думку, акцент на втіленому досвіді має на меті зробити ці заходи більш змістовними та незабутніми для молодих учасників та встановити зв'язок з попередніми поколіннями [10].

А представляючи героїзм воєнного часу як ідеал, до якого може прагнути молодь, сам героїзм поміщається у виразно мілітаризоване середовище. Героєм може бути кожен, але молоді люди, які брали участь у заходах, організованих однією з цих молодіжних груп, заохочуються до висновку, що внесок у воєнні зусилля своєї

країни, в будь-якій якості, дає їм найкращі шанси реалізувати прихований у них героїчний потенціал [11].

Звичайно, російський режим спирається на різні заходи для реалізації своєї політики військово-патріотичної освіти. Вони відрізняються за характером (обов'язкові чи добровільні), змістовною спрямованістю та цільовою групою (віком та/або статтю).

Деякі заходи є обов'язковими для всіх школярів та студентів університетів. Вони базуються на єдиній навчальній програмі. Водночас пропонується цілий спектр позакласних заходів. Хоча формально вони є необов'язковими, неявний тиск з боку системи та певні практичні міркування, такі як відсутність альтернативного догляду за дітьми, обмежують свободу вибору особистості. Позакласні заходи дозволяють зосередити увагу на низці тем, а це означає, що діти та молодь нібито можуть вибирати з-поміж вузько визначених ідеологічних варіантів, і тому охоплення може бути максимально широким. Водночас молоді росіяни постійно стикаються з подібним контентом через інші канали, такі як поп-культура та ігрова сфера [12].

До повномасштабного вторгнення в Україну військово-патріотичне виховання в Росії було спрямоване переважно на школярів, підлітків та молодь. Однак у жовтні 2024 року Путін наполягав на проведенні аналогічних заходів у дитячих садках, включаючи візити ветеранів, участь у парадах та ознайомлення з офіційною пропагандою. Загалом, ідеологічна складова щодо гендерних відносин очевидна. У той час як воєнізовані заходи більше орієнтовані на хлопчиків, програмні сегменти, що стосуються «цивільних» навичок, призначені, перш за все, для дівчаток. Останніх навчають, що, в принципі, вони можуть займатися будь-якою професією, але бути матір'ю — відповідно до традиційної моделі наслідування — є найбажанішим покликанням для жінки [12].

Велика кількість державних та пов'язаних з державою організацій залучена до планування та реалізації заходів. Серед

них — Міністерство освіти та Федеральне агентство у справах молоді (Росмолодь) до Міністерства оборони, козацьких груп, ветеранських організацій та формально приватних «військових компаній». Наприклад, група найманців «Вагнер» заснувала молодіжний клуб «Вагнеренок» та проводила вербувальні бесіди в школах, тоді як інші відповідні компанії, такі як «ЕНОТ», організували воєнізовані молодіжні табори [12].

Так, ключовими елементами військово-патріотичного виховання в Росії є інтерпретація історії країни як постійної, славної оборонної боротьби проти зовнішніх загроз (насамперед із Заходу), її самосприйняття як обложеної фортеці та прославляння її військових сил. Водночас постулюється існування незалежної російської «цивілізації», яка чітко контрастує із західними ліберальними цінностями. Крім того, російський канон включає традиційні ідеї сім'ї, жертовності, героїзму та вірності керівництву, згідно з якими інтереси окремої людини мають бути підпорядковані інтересам громади.

Той факт, що багато учасників залучені до військово-патріотичного виховання молодого покоління, відображає типову для Кремля систему управління та контролю. Ця система не лише гарантує, що багато хто несе витрати на ці заходи, але й запобігає доступу будь-якого із залучених учасників до надмірних фінансових ресурсів чи впливу. Ґрунтуючись на принципі «розділяй і володарюй», контроль Кремля забезпечується шляхом перекриття, дублювання та конкуренції. Таким чином, хоча нові освітні заходи спрямовані на мілітаризацію суспільства, Міністерство оборони є лише одним із кількох важливих учасників. Мілітаризм, що розвинувся в Росії, формується Кремлем; він не перетворюється на більшу автономію для військових.

Отже, описані практики свідчать про цілеспрямовану політику формування мілітаризованого світогляду серед молоді, що реалізується через емоційно насичені та символічно значущі форми

взаємодії з воєнним досвідом. Акцент на «втіленому досвіді» та героїзації війни сприяє не лише романтизації воєнної дійсності, але й формує у молодих людей уявлення про війну як про природний та соціально схвалюваний спосіб самореалізації. У цьому контексті героїзм подається як досяжний і бажаний ідеал, реалізація якого безпосередньо пов'язується з участю у воєнних зусиллях держави. Такий підхід свідчить про інструменталізацію історичної пам'яті та ветеранів війни з боку російської федерації з метою політичної соціалізації молодого покоління у дусі лояльності до мілітаристської ідеології та готовності підтримувати агресивну зовнішню політику держави. У результаті подібні практики виступають важливим елементом системної мілітаризації суспільної свідомості, спрямованої на легітимацію війни та відтворення культури насильства в російському суспільстві.

На думку Маргарет Кляйн та Сьюзен Стюарт російське керівництво стурбоване тим, що молодь більш критично ставиться до режиму, ніж інші вікові групи. Таким чином, описані вище заходи та програми можна розуміти як спробу завоювати прихильність молодого покоління за допомогою різних методів. Вони мають дедалі ширший вплив, поширюючись не лише на школи, а й на університети, а останнім часом і на дитячі садки. Крім того, відповідні програми також впроваджуються на окупованих Росією територіях України. Це особливо підступний підхід, оскільки українських дітей перевиховують відповідно до російської пропаганди та налаштовують проти України як фізично, так і психологічно [12].

Серед спостерігачів існують різні думки щодо того, чого досягне ця політика. Одні очікують, що значну частину російського населення буде успішно приведено до контролю. Інші вважають, що ці заходи викличуть протести в середньостроковій перспективі, оскільки деякі представники цільової групи почуваються зневаженими. Ще інші вказують на зростаючу поляризацію суспільства,

яка посилюється мобілізаційними кампаніями та пропагандою. Якщо паралелі, проведені з радянською епохою, сприймати серйозно, то, ймовірно, знадобиться деякий час, щоб опір цим заходам поширився за межі невеликої маргіналізованої меншини — якщо це взагалі станеться. Навіть попри те, що світ кардинально змінився з часів радянського часу, Москва успішно забезпечує, щоб значна частина російського населення не мала доступу до достовірної інформації, та вселяє недовіру до західних ЗМІ. Це пов'язано не лише зі здатністю режиму контролювати потік інформації, але й з тим, що багатьом громадянам було б важко або навіть боляче змінити свої погляди.

Отже, не можна припускати, що наступне покоління в Росії буде прихильником значно позитивних відносин із Заходом, ніж сьогодні. Це особливо стосується тих, хто на шляху до того, щоб стати частиною політичної еліти країни. Швидше за все, цінності, які зараз пропагує Кремль, відображатимуться в діях цих людей, не в останню чергу тому, що ці цінності підкріплюються відчутними стимулами. Ті, хто вважає війну нормальною частиною повсякденного життя, ймовірно, охочіше підтримають конфлікт в Україні та приймуть жертви. Ті, хто шанує героїв, ймовірно, прагнутимуть наслідувати їх. Оскільки багато згаданих вище організацій не лише індоктринують своїх членів, а й прагнуть охопити ширше населення, їхній вплив виходить за межі вікової групи дітей та підлітків. Мілітаризоване суспільство буде більш схильне підтримувати войовничий підхід Кремля та його ризиковану зовнішню політику.

Важливо розуміти, що ідеологічні елементи йдуть пліч-о-пліч із практичною користю для молоді, яка бере участь у програмах. Якщо вони розглядають свою участь як попередній крок до вступу до бажаного університету або отримання привабливої професії, їм буде легше сприйняти зміст програм, не виникаючи жодних питань. Цей ефект посилюється формуванням та зміцненням мереж

з часом. Учасники зустрічаються знову в інших контекстах та підтримують одне одного професійно та/або приватно. Вони приймають ідеологію або більш охоче підтримують її через почуття приналежності та соціального просування, які є результатом цього.

Своєю діяльністю у сфері військово-патріотичного виховання дітей та молоді Кремль намагається забезпечити довгострокову підтримку населення своєї нинішньої зовнішньої політики. Звичайно, в майбутньому будуть громадяни Росії, які виступатимуть проти цієї політики. Однак, найімовірніше, вони залишатимуться в меншості та належатимуть до соціально-економічних верств, які мають незначний вплив на політичні події в країні. Ті, хто формуватиме російську політику в майбутньому, — або з переконань, або (що більш ймовірно) з опортунізму — приймуть ідеологію, яка неофіційно утвердилася завдяки військово-патріотичним виховним заходам останніх років. Ця ідеологія очорнює Захід і прославляє війну. Таким чином, знадобляться покоління, а не роки, щоб з'явилася інша Росія.

3. Ідеологічні основи та пропагандистські дискурси легітимації, як інструменти символічної влади

Дослідження ідеологічних основ та пропагандистських дискурсів легітимації як інструментів символічної влади зумовлена зростанням ролі інформаційного та смислового виміру політики в сучасних конфліктах і процесах трансформації міжнародного порядку. У XXI столітті боротьба за владу дедалі частіше відбувається не лише у військовій чи економічній площині, а й у сфері формування уявлень, цінностей та інтерпретацій політичної реальності. Через ідеологічні наративи, політичну міфологію та системно сконструйовані пропагандистські дискурси владні режими прагнуть легітимізувати власні політичні практики, мобілізувати населення та формувати лояльність до державної політики. У цьому контексті символічна влада виступає важливим механізмом впливу

на суспільну свідомість, оскільки вона дозволяє закріплювати певні інтерпретації подій як домінантні та соціально прийнятні.

Ідеологія виступає ключовим культурно-ідеологічним чинником легітимації влади, діючи поруч із релігійними та міфологічними конструктами. Політичні актори використовують систему ідей як інструментарій для обґрунтування своїх претензій на владу та формування програми майбутньої діяльності. Ефективність ідеології як засобу легітимації проявляється у двох аспектах: через раціоналізацію та виправдання очікувань індивідів (обіцянка реалізації їхніх інтересів) та через консолідацію суспільства навколо боротьби зі спільним ворогом, що забезпечує суб'єкту необхідний рівень підтримки [28].

Особливої актуальності зазначена проблематика набуває в умовах посилення авторитарних тенденцій, гібридних конфліктів та інформаційних війн, де пропагандистські дискурси активно використовуються для виправдання агресивної політики, мілітаризації суспільства та конструювання образу зовнішнього ворога. У таких умовах ідеологічні наративи виконують функцію інструменту легітимації політичних рішень та засобу формування колективної ідентичності, що підтримує існування відповідного політичного режиму. Аналіз цих процесів дозволяє глибше зрозуміти механізми відтворення символічної влади країни агресора, а також виявити способи маніпуляції суспільною свідомістю через контроль над дискурсами, смислами та інтерпретаціями політичної дійсності.

Згідно з М. Вебером, ідеологія є не лише доповненням до волі до влади, а й базовим елементом, що формує політичні інтереси та перетворює політичний процес на динамічну взаємодію цих інтересів. Розвиваючи марксистську тезу про ідеї як інструментарій впливу, П. Бергер та Т. Лукман пов'язують дефініцію ідеології безпосередньо з механізмами легітимації влади. На їхню думку, ідеологія виникає тоді, коли суб'єктивне трактування реальності починає

обслуговувати конкретний владний інтерес. Як тільки певна група апропріює доктрину, остання трансформується під її потреби, стаючи інструментом виправдання (легітимації) її дій. Таким чином, будь-яка концепція реальності набуває ідеологічного статусу, якщо вона надає групі можливість ефективно управляти соціальним простором та успішно реалізовувати свої прагнення [28].

На думку П. Смирнової та М. Махортих російські ультраправі спільноти в Telegram формують сприйняття політичних діячів за допомогою мемів та візуальних наративів. Ці актори, далеко не пасивні глядачі, спільно продукують пропаганду, поєднуючи державні меседжі з власними екстремістськими фреймінгами. У Росії такі групи є центральними, оскільки вони висловлюють ідеологічні основи війни проти України та відображають поступовий схил режиму до ультранаціоналістичної риторики [13].

Спираючись на набір даних із 200 000 зображень з відібраних експертами ультраправих Telegram-каналів, автори використали комп'ютерний зір та неконтрольовану кластеризацію для виявлення мемів із зображенням російських (Путін, Шойгу) та іноземних політиків (Зеленський, Байден, Трамп) та виявлення повторюваних візуальних патернів у їхньому представленні. Використовуючи масштабну та часову глибину цього набору даних, автори змогли виявити різні патерни легітимації та делегітимації у різних акторів та з плином часу [13].

Так, попередні результати показали, що ультраправі меми функціонують як інструменти спільного виробництва пропаганди. Ці спільноти не просто повторюють офіційні повідомлення, а й генерують наративи легітимації та делегітимації знизу вгору, що узгоджуються з державною ідеологією. Представляючи лідерів як героїв, а опонентів як корумпованих або слабких, ультраправі актори виступають неформальними співтворцями авторитарної легітимності в рамках інформаційної автократії Росії.

Загалом, російсько-українська війна — один із найважливіших конфліктів XXI століття. Вторгнення Росії у 2022 році було провалом як у військовому сенсі, так і в пропагандистському плані. Незважаючи на величезний запас ідеологічних та історичних референтів, з яких можна було черпати, ні Росія, ні керівництво «народних республік» Донбасу не дуже дбали про ідеологію. Усі спроби побудувати колективну ідентичність («внутрішню групу») були короткочасними, рідко та непослідовно озвучувалися на сторінках місцевих газет та вебсайтів [14].

Тим часом, зовнішня група, або «вони», що протистоять «ми», була об'єктом дуже детальної та багатої дискурсивної конструкції. Внутрішньо (звертаючись до місцевого населення) цей дискурс, зосереджений на зовнішній групі, повертався до минулих конфліктів, насамперед Другої світової війни, та проектував почуття провини з боку України щодо Донбасу. Зовні (звертаючись до аудиторії за межами ДНР та ЛНР, насамперед російськомовних українців), цей дискурс повністю ігнорував історію, а натомість проектував почуття сорому, а не провини, прагнучи дискредитувати український уряд без посилання на втрачений спільний зв'язок.

Звичайно, кремлівська пропаганда має величезне історичне підґрунтя для формування поглядів людей. Відбулася війна, яка вже відома як війна в соціальних мережах або перша війна в TikTok; терміни дезінформація, пропаганда та неправдива інформація в соціальних мережах обговорюються повсюдно, і обидві сторони здійснювали величезні маніпуляції інформацією в соціальних мережах.

На думку П. Лисянського та В. Ястребової «критичне мислення у сучасному світі — це здатність індивіда свідомо, системно й рефлексивно аналізувати інформацію, відрізняти факти від маніпуляцій, перевіряти достовірність джерел та ухвалювати обґрунтовані рішення в умовах надлишку даних і постійного інформаційного тиску. У глобалізованому інформаційному середовищі

критичне мислення виконує функцію «інтелектуального імунітету», що захищає людину від впливу дезінформації, пропаганди, алгоритмічно підсилених ехо-камер і синтетичного контенту, створеного за допомогою штучного інтелекту» [29].

Звичайно, критичне мислення сьогодні кваліфікується як фундаментальна компетенція XXI століття, що посідає чільне місце в ієрархії софт-скілів поруч із цифровою грамотністю та комунікативною адаптивністю. У контексті сучасної геополітики воно постає базовим інструментом збереження суб'єктності особистості та запорукою інституційної стійкості демократій. Особливої ваги цей ресурс набуває в умовах гібридних загроз, де когнітивна стійкість є головним валом оборони проти інформаційно-психологічних операцій, які інтегровані в загальну стратегію збройної агресії.

Держава-агресор сформувала розгалужену інституційну екосистему, що функціонує як координована матриця інформаційного домінування. У цій системі спостерігається чітка детермінація ролей [29]:

Стратегічний рівень: Державні інституції, фонди та афілійовані структури розробляють ідеологічні канони та домінантні наративи.

Операційний рівень: Офіційні медіа та інформагенції забезпечують первинну легітимацію змістів, тоді як мережа проксі-акторів — від троль-ферм та «воєнкорів» до PR-агентств — здійснює їхню тактичну імплементацію.

Культурно-символічний рівень: Кінематограф та масова культура інтегрують задані смисли у повсякденний дискурс, забезпечуючи їхню довгострокову фіксацію у суспільній свідомості.

Центральну роль у забезпеченні функціональної цілісності цієї машини відіграють спецслужби. Вони здійснюють оперативне керівництво, визначають пріоритети цілепокладання, курують агентурні мережі впливу та контролюють дистрибуцію ресурсів через легальні й латентні канали.

Технологічний інструментарій системи охоплює широкий спектр цифрових рішень: від мікротаргетингу та алгоритмічної маніпуляції трендами до застосування генеративного штучного інтелекту й дипфейків. Це створює адаптивну оперативну «оболонку», яка дозволяє масштабувати операції впливу та підвищувати їхню вірулентність.

Фінансова архітектура системи базується на диверсифікації потоків: прямі бюджетні асигнування поєднуються з грантовою підтримкою через мережу фондів-прокладок, що дозволяє маскувати деструктивний контент під просвітницькі чи культурні ініціативи. Така стратегія сприяє проникненню в локальні медіаекосистеми європейських країн та колаборації з діаспорними організаціями [29].

Синергія інституційного, технологічного та культурного рівнів призводить до ефекту «дискурсивної окупації». Кінцевою метою є не просто дисемінація фейків, а системна деструкція механізмів критичної верифікації інформації, що спричиняє ерозію колективного інформаційного імунітету та ускладнює відновлення соціальної стійкості.

Однією з важливих ідеологічний основ діяльності окупаційної влади варто відзначити підготовка, оголошення та проведення псевдо референдумів на окупованих Росією українських територіях. У межах аналізу ідеологічних основ та пропагандистських дискурсів легітимації, ці псевдореферендуми можна розглядати як інструмент символічної влади, спрямований на створення видимості демократичної процедури. Російська влада намагалася сформувати наратив про нібито «вільне волевиявлення населення» окупованих територій, що мало слугувати підґрунтям для подальших політичних рішень, включно з їхньою анексією.

З позиції теорії символічної влади, запропонованої Pierre Bourdieu, подібні практики виконують функцію легітимації політичного домінування через символічні та дискурсивні механізми.

Формально використовуючи демократичні інститути — такі як референдум, — авторитарна влада прагне надати власним діям вигляду легітимності, навіть якщо ці процедури не відповідають міжнародним стандартам. Таким чином, референдум перетворюється не на механізм народного волевиявлення, а на інструмент політичної маніпуляції.

Окрім того, на міжнародному рівні проведення псевдореферендумів було частиною ширшої інформаційно-політичної стратегії Росії. Їх використовували для просування наративу про «самовизначення народів» і спробу перекласти відповідальність за зміну статусу територій на їхніх мешканців. Проте, більшість демократичних держав та міжнародних організацій, засудили ці дії та підтвердили підтримку територіальної цілісності України.

Окрім того, сама Україна Постановою «Про нікчемність псевдореферендумів на тимчасово окупованих територіях України» від 27 вересня 2022 року № 101, ухваленою Верховною Радою України, визначає офіційну позицію держави щодо так званих референдумів, організованих Росією на окупованих територіях України. Та стверджує, що ці голосування були спрямовані на створення формального приводу для подальшої анексії територій [33].

У документі зазначається, що організовані Росією голосування на тимчасово окупованих територіях Донецької, Луганської, Запорізької та Херсонської областей не мають жодної юридичної сили. Верховна Рада України підкреслює, що ці так звані референдуми проводилися з грубим порушенням Конституції України, міжнародного права та принципів суверенітету і територіальної цілісності держав [33].

Постанова також наголошує, що результати цих голосувань є нікчемними, а будь-які спроби використати їх для зміни міжнародно визнаних кордонів України не можуть бути визнані міжнародною спільнотою. Документ закликає іноземні держави та міжнародні організації не визнавати результати псевдореферендумів

і посилювати політичний, дипломатичний та санкційний тиск на державу-агресора [33].

Отже, постанова українського парламенту стала важливим елементом політико-правової протидії російській інформаційній та ідеологічній стратегії. Вона не лише закріпила офіційну позицію України щодо незаконності псевдореферендумів, але й підкреслила їхню роль як інструменту пропагандистської легітимації та символічного конструювання влади у межах російської політики окупації.

Загалом, аналіз ідеологічних основ та пропагандистських дискурсів легітимації засвідчує, що у сучасних конфліктах символічна влада стає одним із ключових інструментів політичного домінування. Через використання ідеологічних наративів, політичної міфології, інформаційних кампаній і контроль над медійними дискурсами владні режими прагнуть сформувати вигідну інтерпретацію політичної реальності, мобілізувати суспільство та виправдати власні дії на внутрішньому й міжнародному рівнях. У контексті російсько-української війни ці механізми проявляються у конструюванні образу ворога, використанні історичних символів, залученні цифрових платформ та мережевих спільнот до поширення пропаганди, а також у спробах надати агресивним політичним рішенням формальної легітимності через такі інструменти, як псевдореферендуми на окупованих територіях. Водночас міжнародна реакція та офіційна позиція України щодо їхньої нікчемності демонструють обмеженість подібних стратегій легітимації, підкреслюючи їхній пропагандистський характер і спрямованість на маніпуляцію суспільною свідомістю.

4. Висновки

У сучасних авторитарних режимах механізми легітимації дедалі частіше набувають символічного характеру. Концепція символічної влади, пояснює, що домінування може здійснюватися не лише через примус або економічні ресурси, але й через контроль над

символічними структурами суспільства — мовою, знанням, культурними кодами та інформаційними потоками. Символічна влада проявляється у здатності визначати значення політичних подій, формувати домінантні інтерпретації реальності та нав'язувати їх як природні й безальтернативні.

У цьому контексті пропагандистські дискурси виконують функцію інструменту конструювання політичної реальності. Через систематичне відтворення певних наративів — таких як історична місія держави, образ «зовнішнього ворога», ідея цивілізаційного протистояння або необхідність «захисту населення» — влада прагне сформувати у суспільстві певну систему уявлень, що виправдовує політичні рішення та легітимує існуючий політичний порядок.

У випадку Російської Федерації ідеологічні наративи активно використовуються для виправдання агресивної зовнішньої політики та конструювання образу війни як історично необхідного та неминучого явища. Центральними елементами цього дискурсу виступають концепти «захисту російськомовного населення», «історичної єдності народів», «боротьби з нацизмом» та протистояння із Заходом. Через системну медійну репрезентацію ці наративи трансформуються у домінантні інтерпретації політичної реальності, які покликані сформувати суспільну підтримку війни та нейтралізувати критичні погляди.

Особливу роль у процесі легітимації відіграють псевдодемократичні процедури, зокрема організація так званих референдумів на тимчасово окупованих територіях України. Проведення таких заходів має на меті створення імітації народного волевиявлення та формування у міжнародному інформаційному просторі видимості правомірності зміни політико-правового статусу територій. Водночас міжнародна спільнота та Україна однозначно визнають подібні дії порушенням норм міжнародного права та принципів територіальної цілісності держав.

Таким чином, ідеологічні наративи та пропагандистські дискурси виступають важливим інструментом символічної влади, що дозволяє авторитарним режимам конструювати уявну легітимність своїх дій. Контроль над інформаційним простором, маніпуляція історичною пам'яттю та використання псевдоправових механізмів формують систему символічного домінування, спрямовану на виправдання політичної агресії та підтримку існування відповідного політичного режиму.

Список використаних джерел:

1. Bolechów B., Szulc K. Błędna percepcja w polityce zagranicznej jako produkt uboczny dogmatycznej ideologii. Przypadek wojny Rosji z Ukrainą. *Eastern Review*. 2024. 12(2). 37–56. DOI: https://doi.org/10.18778/1427-9657.12.09.

2. Barbashin, A., Thoburn, H. 2014. Putin's Brain: Alexander Dugin and the Philosophy Behind Putin's Invasion of Crimea. *Foreign Affairs*. URL: https://www.foreignaffairs.com/articles/russia-fsu/2014-03-31/putins-brain

3. Berger J. M. Extremist construction of identity: how escalating demands for legitimacy shape and define in-group and out-group dynamics. ICCT Research Paper. 2017. URL: https://icct.nl/wp-content/uploads/2017/04/ICCT-Berger-Extremist-Construction-of-Identity-April-2017-2.pdf https://doi.org/10.19165/2017.1.07.

4. Østbø J. Securitizing "spiritual-moral values" in Russia. Post Soviet Affairs. 2016. DOI: http://dx.doi.org/10.1080/1060586X.2016.1251023.

5. Завгородня Ю. В. 2024. Державна політика в сфері кібербезпеки в умовах повномасштабної війни. *Актульні проблеми політики*. № 74. С. 62–66 URL: http://app.nuoua.od.ua/archive/74_2024/10.pdf

6. Allyson Edwards, Jennifer G Mathers, Anyone can be a hero: the militarization of children in Putin's Russia, *International Affairs*. 2025. Vol. 101. Issue 2. P. 399–417. DOI: https://doi.org/10.1093/ia/iiae329.

7. Eastern Human Rights Group & Institute for Strategic Studies and Security. Militarization of industry in the temporarily occupied

territoris of Ukraine: Infrastructural remnants, repressive practices, and military-industrial vectors of the RF [Analytical report]. Konrad-Adenauer-Stiftung Ukraine. 2025. URL: https://isrs.group/

8. Eastern Human Rights Group & Institute for Strategic Studies and Security. Education in the temporarily occupied territories of Ukraine: The political dimension [Analytical report]. Konrad-Adenauer-Stiftung Ukraine. 2025. URL: https://isrs.group/

9. Ana Caballero-Mengibar, Critical discourse analysis in the study of representation, identity politics and power relations: a multi-method approach. *Communication and Society* 28: 2, 2015. Pp. 39–54 at p. 41, DOI: https://doi.org/10.15581/003.28.35957.

10. See, for example, Kiril Avramov, Yunarmia: meet the young Russian "guardians of order", GlobePost, 5 Feb. 2021. URL: https://theglobepost.com/2019/02/05/yunarmia-russia-youth-army

11. Anton Troianovski, Ivan Nechepurenko and Valerie Hopkins, 'How the Kremlin is militarizing Russian society', *New York Times*, 21 Dec. 2021. URL: https://www.nytimes.com/2021/12/21/world/europe/russia-military-putin-kremlin.html

12. Klein M., Stewart S. Military-Patriotic Education in Russia: How the Next Generation Is Being Brought Into Line with the Regime. *SWP Comment*, No. 46. 2025. URL: https://www.swp-berlin.org/en/publication/military-patriotic-education-in-russia

13. Smirnova P., Makhortykh M. Analyzing Far-Right Telegram Channels as Constituents of Information Autocracy in Russia [Electronic resource]. Computer Science. Computers and Society. 2026. URL: https://arxiv.org/abs/2601.14190

14. Rosenbeck J. Introduction. Propaganda and Ideology in the Russian–Ukrainian War. Cambridge : Cambridge University Press, 2024. P. 1–6. (Contemporary Social Issues). DOI: https://doi.org/10.1017/9781009244039.002.

15. Hasan M. Russian-Ukrainian Propaganda on Social Media: A Bibliometric Analysis. *Journal. Media*. 2024. 5. 980–992. DOI: https://doi.org/10.3390/journalmedia5030062.

16. Jamieson, Kathleen Hall. Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know. Oxford: Oxford University Press, 2021. 375 p.

17. Завгородня Ю. В. Фейки як сучасна форма політичного протиборства у кіберпросторі. *Регіональні студії*. № 28. 2022. URL: http://regionalstudies.uzhnu.uz.ua/archive/28/12.pdf

18. Mejias, Ulises A. and Nikolai E. Vokuev. Disinformation and the Media: The Case of Russia and Ukraine. *Media, Culture & Society*. 2017. № 39. 1027–1042.

19. Roozenbeek J. Propaganda and Ideology in the Russian–Ukrainian War. Cambridge : Cambridge University Press, 2024. 238 p. DOI: https://doi.org/10.1017/9781009244039.

20. McGlynn J. Russia's War. Cambridge : Polity Press, 2023. 264 p. URL: https://books.google.com/books/about/Russia_s_War.html?id=oIeqEAAAQBAJ

21. McGlynn J. Russian Propaganda Tactics in Ukraine's Newly Occupied Territories. *Russian Analytical Digest*. 2024. No. 313. P. 2–6. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Russian_Analytical_Digest_313.pdf

22. Goble P. Russian Propaganda from V to Z: Projecting Banal and Everyday Nationalism in Unsettled Times. *Nationalities Papers*. 2025. Vol. 53, Iss. 1. P. 15–32. DOI: https://doi.org/10.1017/nps.2024.12

23. Hasan M. Russian-Ukrainian Propaganda on Social Media: A Bibliometric Analysis. *Journal. Media*. 2024. Vol. 5. Iss. 3. P. 980–992. DOI: https://doi.org/10.3390/journalmedia5030062.

24. Laruelle M. Imperialist ideology or depoliticization? Why Russian citizens support the invasion of Ukraine. *Post-Soviet Affairs*. 2022. Vol. 38. Iss. 4. P. 301–318. DOI: https://doi.org/10.1080/1060586X.2022.2101832.

25. Центр протидії дезінформації : офіційний вебсайт. Київ : РНБО України. URL: https://cpd.gov.ua/

26. EUvsDisinfo : official website. Brussels : European External Action Service. URL: https://euvsdisinfo.eu/

27. Детектор Медіа : онлайн-видання. Київ : ГО «Детектор медіа». URL: https://detector.media/

28. Вонсович Г. Дискурс ідеології як засобу легітимації влади. *Гілея* : науковий вісник. 2014. Вип. 83. С. 367–370. URL: http://nbuv.gov.ua/UJRN/gileya_2014_83_93

29. Лисянський П. Л., Ястребова В. А. Руйнування критичного мислення як інструмент когнітивної війни агресора. Політична культура та ідеологія : зб. наук. пр. / чи журнал. 2024. DOI: https://doi.org/10.5281/zenodo.17404382.

30. Лисянський П. Л., Ястребова В. А. Ідеологічні диверсії в умовах гібридної війни: виклики для національної безпеки та політичної стабільності. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право* : зб. наук. пр. 2023. № 1 (57). С. 97–102.

31. Culver N. Russian Influence Operations: Hybrid Warfare or Modern Statecraft, and its Impact to the West. *Canadian Forces College Research Series*. 2019. № JCSP-46. С. 1–28.

32. Minzarari D. The next war: How Russian hybrid aggression could threaten Moldova. *European Council of Foreign Relations Research Series*. 2022. № ECFR/460. С. 1–21.

33. Про нікчемність псевдореферендумів на тимчасово окупованих територіях України : Постанова Верховної Ради України від 27 вересня 2022 р. № 101. URL: https://www.rada.gov.ua

References:

1. Belov, D. M., Peresh, I. Ye., & Pokorba, I. (2024). Tsyfrovi prava liudyny: Doktrynalni zasady. *Analitychno-porivnialne pravoznavstvo*, (2), 110–115. https://doi.org/10.24144/2788-6018.2024.02.17.

2. Bolechów, B., & Szulc, K. (2024). Błędna percepcja w polityce zagranicznej jako produkt uboczny dogmatycznej ideologii: Przypadek wojny Rosji z Ukrainą. *Eastern Review*, 12(2), 37–56. https://doi.org/10.18778/1427-9657.12.09.

3. Barbashin, A., & Thoburn, H. (2014). Putin's brain: Alexander Dugin and the philosophy behind Putin's invasion of Crimea. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/russia-fsu/2014-03-31/putins-brain

4. Berger, J. M. (2017). Extremist construction of identity: How escalating demands for legitimacy shape and define in-group and out-group dynamics. ICCT Research Paper. https://doi.org/10.19165/2017.1.07.

5. Østbø, J. (2016). Securitizing "spiritual-moral values" in Russia. *Post-Soviet Affairs*. https://doi.org/10.1080/1060586X.2016.1251023.

6. Zavhorodnia, Yu. V. (2024). Derzhavna polityka v sferi kiberbezpeky v umovakh povnomasshtabnoi viiny. *Aktualni problemy polityky*, 74, 62–66. Retrieved from http://app.nuoua.od.ua/archive/74_2024/10.pdf

7. Edwards, A., & Mathers, J. G. (2025). Anyone can be a hero: The militarization of children in Putin's Russia. *International Affairs*, 101(2), 399–417. https://doi.org/10.1093/ia/iiae329.

8. Eastern Human Rights Group, & Institute for Strategic Studies and Security. (2025). Militarization of industry in the temporarily occupied territories of Ukraine: Infrastructural remnants, repressive practices, and military-industrial vectors of the Russian Federation (Analytical report). Retrieved from https://isrs.group/

9. Eastern Human Rights Group, & Institute for Strategic Studies and Security. (2025). Education in the temporarily occupied territories of Ukraine: The political dimension (Analytical report). Retrieved from https://isrs.group/

10. Caballero-Mengibar, A. (2015). Critical discourse analysis in the study of representation, identity politics and power relations: A multi-method approach. *Communication and Society*, 28(2), 39–54. https://doi.org/10.15581/003.28.35957.

11. Avramov, K. (2019). Yunarmia: Meet the young Russian "guardians of order". The Globe Post. Retrieved from https://theglobepost.com/2019/02/05/yunarmia-russia-youth-army

12. Troianovski, A., Nechepurenko, I., & Hopkins, V. (2021). How the Kremlin is militarizing Russian society. *The New York Times*. Retrieved from https://www.nytimes.com/2021/12/21/world/europe/russia-military-putin-kremlin.html

13. Klein, M., & Stewart, S. (2025). Military-patriotic education in Russia: How the next generation is being brought into line with the regime. SWP Comment, 46. Retrieved from https://www.swp-berlin.org/en/publication/military-patriotic-education-in-russia

14. Smirnova, P., & Makhortykh, M. (2026). Analyzing far-right Telegram channels as constituents of information autocracy in Russia. Computer Science. Computers and Society. Retrieved from https://arxiv.org/abs/2601.14190

15. Rosenbeck, J. (2024). Introduction. In J. Roozenbeek (Ed.), Propaganda and ideology in the Russian–Ukrainian war (pp. 1–6). Cambridge University Press. https://doi.org/10.1017/9781009244039.002.

16. Hasan, M. (2024). Russian-Ukrainian propaganda on social media: A bibliometric analysis. *Journal. Media*, 5, 980–992. https://doi.org/10.3390/journalmedia5030062.

17. Jamieson, K. H. (2021). Cyberwar: How Russian hackers and trolls helped elect a president. Oxford University Press.

18. Zavhorodnia, Yu. V. (2022). Feiky yak suchasna forma politychnoho protyborstva u kiberprostori. Rehionalni studii, 28. Retrieved from http://regionalstudies.uzhnu.uz.ua/archive/28/12.pdf

19. Mejias, U. A., & Vokuev, N. E. (2017). Disinformation and the media: The case of Russia and Ukraine. *Media, Culture & Society*, 39, 1027–1042.

20. Roozenbeek, J. (2024). Propaganda and ideology in the Russian–Ukrainian war. Cambridge University Press. https://doi.org/10.1017/9781009244039.

21. McGlynn, J. (2023). Russia's war. Polity Press.

22. McGlynn, J. (2024). Russian propaganda tactics in Ukraine's newly occupied territories. *Russian Analytical Digest*, 313, 2–6.

23. Goble, P. (2025). Russian propaganda from V to Z: Projecting banal and everyday nationalism in unsettled times. *Nationalities Papers*, 53(1), 15–32. https://doi.org/10.1017/nps.2024.12.

24. Laruelle, M. (2022). Imperialist ideology or depoliticization? Why Russian citizens support the invasion of Ukraine. *Post-Soviet Affairs*, 38(4), 301–318. https://doi.org/10.1080/1060586X.2022.2101832.

25. Center for Countering Disinformation. (n.d.). Official website. Retrieved from https://cpd.gov.ua/

26. EUvsDisinfo. (n.d.). Official website. Retrieved from https://euvsdisinfo.eu/

27. Detector Media. (n.d.). Official website. Retrieved from https://detector.media/

28. Vonsovych, H. (2014). Dyskurs ideolohii yak zasobu lehitymatsii vlady. *Hileia*, 83, 367–370.

29. Lysianskyi, P. L., & Yastrebova, V. A. (2024). Ruinuvannia krytychnoho myslennia yak instrument kohnityvnoi viiny ahresora. https://doi.org/10.5281/zenodo.17404382.

30. Lysianskyi, P. L., & Yastrebova, V. A. (2023). Ideolohichni dyversii v umovakh hibrydnoi viiny: Vyklyky dlia natsionalnoi bezpeky ta politychnoi stabilnosti. *Visnyk NTUU KPI. Politolohiia. Sotsiolohiia. Pravo*, 1(57), 97–102.

31. Culver, N. (2019). Russian influence operations: Hybrid warfare or modern statecraft and its impact to the West. Canadian Forces College Research Series, JCSP-46, 1–28.

32. Minzarari, D. (2022). The next war: How Russian hybrid aggression could threaten Moldova. European Council on Foreign Relations.

33. Verkhovna Rada of Ukraine. (2022). Resolution on the illegitimacy of pseudo-referendums in the temporarily occupied territories of Ukraine (27 September 2022 No. 101). Retrieved from https://zakon.rada.gov.ua

ESSENCE AND ELEMENTS OF THE MECHANISM OF ADMINISTRATIVE AND LEGAL REGULATION OF THE CREATION OF LEGAL ENTITIES

Ilnytska N. F.,
Candidate of Law Sciences, Associate Professor,
Associate Professor of the Department of Private Law
Kyiv National Economic University named after Vadym Hetman,
Kyiv, Ukraine

Abstract. Creation of legal entities is a key component of the functioning of a modern legal and economic system, as it leads to the emergence of new subjects of law and participants in economic circulation. The effectiveness of this process depends on the proper functioning of the mechanism of administrative and legal regulation, which ensures the orderly development of social relations in the field of establishment of legal entities, the implementation of administrative procedures, and the official recognition of newly created entities by the state. Strengthening legal regulation of this process is crucial for ensuring legality, transparency, and stability in the business environment. **Purpose** of the research is to determine the essence, structure, and specific features of the mechanism of administrative and legal regulation of the establishment of legal entities, and to clarify its role in ensuring the legality of administrative procedures and forming a stable legal environment for entrepreneurial and other activities. Achieving this objective guided the logic of the research, which includes: the analysis of the concept and characteristics of the mechanism of administrative and legal regulation of the establishment of legal entities; determination of its structure; and characterization

of its main elements. **Methodology** of the research combines general scientific and legal methods. The dialectical method was used to study the development and interrelation of legal phenomena in establishing legal entities; the system-structural method helped define the structure of administrative and legal regulation; the comparative-legal method analyzed approaches to understanding legal and administrative-legal mechanisms; and analysis and synthesis were applied to generalize scientific approaches for improving legal regulation of the establishment of legal entities. **Results** indicate that the establishment of legal entities is an interdisciplinary legal institution regulated by civil, commercial, and administrative law. A significant part of the procedures related to the legitimation of legal entities has an administrative and legal nature, as they involve public administration bodies performing state registration, licensing, and permitting functions. The research demonstrates that the mechanism of administrative and legal regulation is a system of interconnected legal means, forms, and methods that ensure the implementation of administrative procedures, guarantee legality, and provide legal certainty and stability in economic circulation. **Practical implications** lie in the possibility of applying the research results to improve administrative procedures for the establishment of legal entities, enhance the effectiveness of public administration bodies, and optimize legal regulation. **Value and originality** of the research consist in a comprehensive analysis of the mechanism of administrative and legal regulation as an integrated system of interrelated elements that ensure the functioning of administrative procedures for the legitimation of legal entities and support a stable legal environment for entrepreneurial activity.

Keywords: Administrative and legal regulation, Mechanism of regulation, Legal entity, Creation of a legal entity, State registration, Legal status, Subjects of public administration, Administrative procedure.

1. Introduction

Relevance and novelty of the research topic. The legal regulation of the creation of legal entities is of a complex nature and is implemented through norms of various branches of law, in particular civil, commercial, and administrative law. At the same time, a significant part of the procedures related to the emergence of legal entities has a public-law nature, as it involves the participation of authorities in the process of official recognition of legal entities by the state. Such procedures include, in particular, state registration of legal entities, licensing of certain types of their activities, as well as obtaining permit-based documents.

In this regard, the creation of legal entities is largely implemented through mechanisms of administrative-legal regulation, which ensure the practical implementation of relevant legal norms and the ordering of social relations in the indicated sphere. The administrative-legal regulation mechanism serves as an instrument for transforming normative prescriptions into specific administrative procedures and management decisions of public administration bodies. Studying such a mechanism allows us to determine the system of administrative-legal tools through which the emergence and functioning of legal entities are ensured, as well as to identify problems in law enforcement practice and directions for improving normative regulation.

Certain issues of the administrative-legal regulation mechanism have been reflected in the scientific works of V. B. Averyanov, S. I. Bevz, Yu. P. Bityak, N. V. Halitsina, V. V. Halunko, T. O. Kolomoiets, L. P. Kotyash, P. S. Lyutikov, S. H. Stetsenko, S. O. Mosiondz, V. M. Harashchuk, A. V. Omelchenko, Kh. P. Yarmak, and other scholars.

At the same time, issues of a comprehensive study of the administrative-legal regulation mechanism for the creation of legal entities, its structure, elements, and functional purpose remain

insufficiently developed in modern legal science. Most scientific works are dedicated either to the civil-law aspects of the legal status of legal entities or to general issues of administrative-legal regulation of economic activity, which necessitates an in-depth scientific analysis of this problem.

Considering the above, the study of the administrative-legal regulation mechanism for the creation of legal entities has significant theoretical and practical value, as it contributes to forming a holistic scientific approach to understanding the administrative-legal means of regulating relevant procedures, as well as determining directions for improving the legal support of public administration bodies in this sphere.

Methodological basis of the study is a combination of general scientific and specialized legal methods of cognition. In particular, the dialectical method was used to study the development and interconnection of legal phenomena in the sphere of legal entity creation; the formal-legal method — for analyzing the content of legislative norms regulating relevant administrative procedures; the system-structural method — for determining the structure of the administrative-legal regulation mechanism; the comparative-legal method — for analyzing scientific approaches to understanding the mechanism of legal and administrative-legal regulation; as well as methods of analysis and synthesis, which allowed summarizing scientific approaches and formulating theoretical conclusions regarding the improvement of legal regulation of the creation of legal entities.

Purpose of the study is to determine the essence, structure, and features of the administrative-legal regulation mechanism for the creation of legal entities, as well as to clarify its role in ensuring the legality of administrative procedures and forming a stable legal environment for entrepreneurial and other activities.

Achieving the stated purpose determines *the logic of presenting the material*, which involves: analyzing the concept and features

of the administrative-legal regulation mechanism for the creation of legal entities; determining the structure of the administrative-legal regulation mechanism for the creation of legal entities; and characterizing the elements of the administrative-legal regulation mechanism for the creation of legal entities.

2. The concept and features of the administrative-legal regulation mechanism for the creation of legal entities

The creation of legal entities is a subject of complex legal regulation by various branches of law, and in particular, a subject of administrative-legal regulation, since most procedures within the creation of legal entities that have legal significance involve the participation of state authorities and local self-government bodies, i.e., they contain a state-law, public-law component.

It should be noted that the content of administrative-legal regulation is revealed through its mechanism, which is a concept derived from the mechanism of legal regulation, implemented based on norms enshrined in laws or subordinate administrative-legal acts.

A distinctive feature of legal regulation, as noted by O. F. Skakun, is that it has a specific mechanism. The category of the legal regulation mechanism is used in legal theory to reveal the interaction of elements of the legal system through which a regulatory influence on social relations is exercised to order them. Thus, according to the scholar, the mechanism of legal regulation is "a system of legal means, methods, and forms taken in unity, through which the normativity of law is transformed into the orderliness of social relations, the interests of legal subjects are satisfied, and law and order are established and ensured" [1, p. 498].

Scholars Yu. A. Vedernikov and A. V. Papirna understand the legal regulation mechanism as a system of legal means, taken as a whole, through which legal regulation of social relations is carried

out [2]. O. H. Murashin and M. S. Kelman reveal the legal regulation mechanism similarly, namely as a system of legal means through which the legal ordering of social relations and overcoming obstacles to satisfying the interests of legal subjects are carried out [3, p. 372].

Since the legal regulation mechanism, on the one hand, functions within one system — society, and on the other hand, is itself a system of elements, O. M. Kurakin proves the existence of two levels of its functions: external (general social in nature, determining the content of general regulatory influence on society) and internal (influence on specific social relations) [4, p. 16].

S. Bobrovnik and N. Onishchenko consider that the legal regulation mechanism is a unified set of legal means, methods, and forms through which the ordering of social relations corresponding to the interests of legal subjects is ensured, aimed at resolving conflicts and achieving social compromise in the legal sphere. Thus, the scholars propose abandoning the understanding of this mechanism only as the activity of a legislator who formulates a legal norm, gives it empowering, obligating, or prohibitive character, and only as the implementation of a legal prescription [5, p. 15].

Among the features of the legal regulation mechanism, T. I. Tarakhonych identifies that it: 1) is a component of social regulation; 2) is a system of interconnected elements, including legal means (legal norms, subjective rights, and legal obligations), methods (permissions, prohibitions, and obligations), and forms (observance, execution, and use); 3) ensures the regulation of social relations, being a dynamic part of the legal system; 4) has a result-oriented and purposeful character [6, p. 305].

A similar approach is adopted by V. S. Grekula and Yu. A. Vedernikov, who highlight the following features of the legal regulation mechanism: 1) it is a component of the social regulation mechanism; 2) it unites all phenomena of legal reality (means,

methods, forms); 3) it is an interconnected and interacting system; 4) it is a dynamic part of the legal system—necessary for bringing elements of the legal system into action; 5) the result of its action in society is the establishment of law and order [7, p. 91].

Thus, the legal regulation mechanism ensures the implementation of legal regulation in society, the ordering of legal phenomena, the provision of their unity, interconnection, and interaction, and the process of transforming legal prescriptions into the real behavior of legal subjects.

Considering the doctrinal positions regarding the concept of the legal regulation mechanism and its characteristic features, it can be argued that at the current stage of legal development and democratization of social relations, the legal regulation mechanism can be defined as a set of legal means, methods, and forms through which the ordering of social relations is carried out, taking into account the interests of legal subjects.

Characterizing the legal regulation mechanism allows establishing its components, ensuring their unity and mutual consistency. The need for various legal means is caused by the ambiguity of satisfying the interests of different legal subjects. It should be noted that these means, being instruments of legal influence, must be diverse and interconnected, form a certain system, and, in their entirety, be aimed at achieving the effectiveness of legal regulation.

Traditionally, the main elements of the legal regulation mechanism in legal theory include: legal norm; legal relations; acts of implementation of subjective rights and obligations; acts of application of legal norms [8, p. 262; 1, p. 499].

A broader approach also exists, according to which the elements of the legal regulation mechanism include: legal norm; normative-legal act; legal facts; legal relations; interpretation of legal norms; implementation of law; legality; legal consciousness; legal culture; lawful behavior; unlawful behavior; legal liability.

As noted above, a derivative of the concept of the legal regulation mechanism is the concept of the administrative-legal regulation mechanism, which has its specific features and characteristics. It should be noted that administrative law plays a special role in the legal regulation mechanism, as it serves as an important instrument for managing social processes.

S. H. Stetsenko notes that the administrative-legal regulation mechanism of social relations is a category that expresses the transformation of legal normativity into the orderliness of social relations regulated by administrative law norms; that is, through the administrative-legal regulation mechanism, legal norms, which are static in themselves, are set in motion. According to the scholar, the administrative-legal regulation mechanism can be defined as a set of legal means through which legal regulation of social relations in the field of administrative law is carried out [9, pp. 63–64].

O. I. Ostapenko understands the administrative-legal regulation mechanism as part of the legal regulation mechanism, the essence of which lies in the existence of specific legal tools (administrative-legal norms, administrative-legal relations, acts of application of administrative law), through which the implementation and protection of social relations are carried out [10, p. 45].

I. P. Holosnichenko, M. F. Stakhursky, and N. I. Zolotaryova define the administrative-legal regulation mechanism of social relations as a set of administrative-legal means through which influence on relations is exercised in the process of performing executive authority [11, p. 20].

According to S. T. Honcharuk, the administrative-legal regulation mechanism is a system of administrative-legal means through which legal regulation (ordering) of social relations in the sphere of public administration is carried out [12].

According to V. V. Halunko, the administrative-legal regulation mechanism consists of the means of functioning of the administrative-legal

regulation system to ensure the rights, freedoms, and public interests of legal and natural persons, civil society, and the state [13].

S. I. Bevz proposes defining the administrative-legal regulation mechanism of state governance in the field of economic activity as "a system of administrative-legal means used by authorized subjects to exert purposeful (aimed at achieving the goals of state governance in the sphere of economic activity) legal influence on social relations arising in the process of implementing state governance functions concerning the sphere of economic activity" [14, p. 184].

T. O. Kolomoiets and P. S. Lyutikov consider the administrative-legal regulation mechanism to be a set of legal means through which legal regulation of social relations in the field of administrative law is carried out [15, p. 13].

There is also a tendency to perceive the administrative-legal regulation mechanism as a dynamic phenomenon. In particular, O. I. Shkuropatsky notes that one should not focus solely on the system of elements as the main feature of the administrative-legal regulation mechanism, since the essence of the legal regulation mechanism is determined precisely through the sequence of certain processes (mechanism elements) to ensure the efficiency and effectiveness of legal regulation in the respective sphere. Thus, the mechanism is not only a set of elements but also the sequence of their actions, forming processes that order relevant legal relations to ensure the effective, complete, and comprehensive exercise of human rights and freedoms in the respective sphere [16, p. 111].

Scholars also provide their own definitions of the administrative-legal regulation mechanism within the subject of their research.

Thus, K. P. Zhydchenko, under the concept of the administrative-legal regulation mechanism for the implementation by military personnel of the right to receive a one-time monetary allowance, understands the set of administrative-legal means that influence

the behavior of subjects and objects of social relations arising in the process of implementing administrative obligations of state authorities to ensure the effectiveness of their execution [17, p. 69].

O. V. Kuzmenko and V. H. Chorna, who studied the problem of the public administration mechanism of extracurricular education in Ukraine, propose considering the administrative-legal regulation mechanism of extracurricular education as "a set of administrative-legal means through which social relations in the field of extracurricular education are regulated by subjects endowed with authority for the purpose of satisfying public needs, Europeanization, and raising the level of societal education" [18, p. 101].

L. P. Kotyash concluded that the administrative-legal regulation mechanism of state registration of legal entities in Ukraine is a set of administrative-legal means through which special subjects of public administration authorized for state registration actions influence the relations arising in the process of legalizing or terminating a legal entity, changing the information contained in the Unified State Register of Legal Entities, as well as performing other registration actions provided by law to implement the rights of persons to entrepreneurial (business), political, cultural, sports, professional, and other activities for the benefit of society [18, p. 71].

O. H. Rozhon defined the administrative-legal regulation mechanism of small privatization as "a system of administrative-legal means in the process of their use by authorized persons for regulating, on the principles of legality, openness, transparency, control, and responsibility, administrative-legal relations in the sphere of small privatization to ensure its efficiency, accelerate economic growth, attract foreign and domestic investment, and reduce the share of state or communal property in the economy" [20, p. 113].

Thus, in defining the administrative-legal regulation mechanism, most scientific positions converge on the fact that this mechanism

represents a set of certain administrative-legal means, and its essence lies precisely in the application of these means.

It should be noted that administrative-legal regulation of the creation of legal entities is assigned to the system of public administration bodies and delegated authorities, which ensure the conduct of necessary pre-registration, registration, licensing, and permit procedures: the Ministry of Justice of Ukraine and its territorial offices, the State Regulatory Service of Ukraine, local state administrations, executive bodies of village, settlement, and city councils, notaries, as well as other public authorities (the National Bank of Ukraine, the National Securities and Stock Market Commission of Ukraine, the Antimonopoly Committee of Ukraine, the State Property Fund of Ukraine, licensing authorities, etc.).

Thus, the *administrative-legal regulation mechanism for the creation of legal entities* is a set of administrative-legal means applied by public administration bodies and delegated authorities to order social relations in the process of creating legal entities and aimed at ensuring the rights and legitimate interests of legal entities, their founders, and participants during the creation process.

Based on the analysis of doctrinal positions on this issue, we can identify the *substantive features of the administrative-legal mechanism for creating legal entities*, which imply defining the objectives of such regulation, realized through the application of administrative-legal means, and consist of the following:

1. the duty of public administration bodies and authorized non-state subjects to prevent unlawful encroachments on the rights and legitimate public interests of legal entities, their founders, and participants during the creation process;

2. preventing violations of the rights and legitimate interests of legal entities, their founders, and participants during the creation process by third parties;

3. terminating violations of the rights and legitimate interests of legal entities, their founders, and participants during the creation process;

4. applying all measures provided by law and the powers of public administration subjects to restore the rights and legitimate interests of legal entities, their founders, and participants during the creation process;

5. bringing guilty persons to legal responsibility.

The goal of administrative-legal regulation of the creation of legal entities can be achieved through the application of specific means through which legal influence on the behavior of subjects and objects of public administration in the indicated sphere is exercised. These means differ in nature and functional purpose, but their combination constitutes a formal feature of the administrative-legal regulation mechanism for the creation of legal entities.

The mechanism allows covering the entire process of administrative-legal regulation, "presenting it in a system-dynamic form, revealing its structure, interconnections, and interaction of all elements" [13, pp. 87–97]. The administrative-legal regulation mechanism, like the legal regulation mechanism as a whole, reveals its essence through its structure and constituent elements.

3. The structure of the mechanism of administrative and legal regulation of the creation of legal entities

Similarly to the approaches used in determining the structure of the mechanism of legal regulation in general, two approaches can also be identified with regard to determining the elements of the mechanism of administrative and legal regulation: a broad and a narrow one. The broad approach is characterized by the multiplicity of elements and according to it the mechanism consists of legal norms, legal facts, legal relations, interpretation of legal norms, their implementation, legality, legal culture, legal consciousness, lawful and unlawful behaviour, and legal liability. The narrow approach includes only some of the above-mentioned

elements, for example legal norms, individual acts, legal relations, the implementation of law, and legality [6, p. 308; 21, p. 212].

S. H. Stetsenko, as well as T. O. Kolomoiets and P. S. Liutikov, propose distinguishing organic and functional components of the mechanism of administrative and legal regulation. According to the scholars, the organic components include those without which the mechanism cannot exist: legal norms, acts of implementation of legal norms, and legal relations. Functional components include those elements that significantly influence the mechanism of administrative and legal regulation but are nevertheless not its mandatory elements: legal facts, legal consciousness, legality, acts of interpretation, and acts of application of legal norms [9, pp. 65–66; 15, pp. 13–14].

From the standpoint of S. O. Mosondz, the mechanism of administrative and legal regulation contains the following elements: administrative legal norms, acts of interpretation of administrative legal norms, acts of implementation of administrative legal norms, and administrative legal relations [22, p. 34].

According to Kh. P. Yarmaki, the structural elements of the mechanism of administrative and legal regulation include: norms of administrative law, administrative legal relations, acts of interpretation of administrative law norms, and acts of implementation of administrative legal norms [23].

S. I. Bevz believes that the mechanism of administrative and legal regulation of public administration in the sphere of economic activity combines norms of administrative law, acts of interpretation of administrative legal norms, and acts of implementation of administrative law norms, which are manifested in administrative legal relations involving authorized subjects. Thus, the scholar adheres to the view that administrative legal relations may be only a functional but not a mandatory component of the mechanism of administrative and legal regulation [14, pp. 183–184].

Some scholars propose an expanded system of elements of the mechanism of administrative and legal regulation, including: norms of administrative law and sources of law as their external form of expression; public authorities and the principles of their activity; individual acts of public administration; forms and methods of administrative and legal regulation; administrative legal relations; interpretation of administrative law norms; administrative legal regimes; and administrative procedures [21, p. 214]. It is also noted that in order to achieve the greatest effectiveness the system of the mechanism may be supplemented with additional elements.

Summarizing the above, it should be stated that most scholars identify the following mandatory elements of the mechanism of administrative and legal regulation:

— administrative legal norms;
— administrative legal relations;
— acts of implementation of subjective rights and obligations.

Taking into account the specific features of the object of our research, we consider it appropriate to include the following components among the elements of the mechanism of administrative and legal regulation of the establishment of legal entities:

— administrative legal norms;
— administrative legal relations in the sphere of establishment of legal entities, including the subjects of administrative and legal regulation;
— acts of implementation of subjective rights and obligations of participants in the establishment process, in particular individual acts of subjects of public administration;
— forms and methods of administrative and legal regulation;
— the procedure for legitimation of legal entities [24, p. 99].

Let us briefly characterize the specified elements of the mechanism of administrative and legal regulation of the establishment of legal entities.

4. Characteristics of the elements of the mechanism of administrative and legal regulation of the creation of legal entities

An administrative legal norm is the basic element and the normative foundation of the mechanism of administrative and legal regulation. It represents a general model and a binding rule of conduct for all, which defines for the subject both a possible variant of behaviour (a subjective right) and a necessary variant (a subjective obligation). If such variants of behaviour are not defined and there is no regulatory basis, it is impossible to "launch" the mechanism of administrative and legal regulation and realize the regulatory potential of administrative law. This approach is relevant for any sphere of legal regulation.

An administrative legal norm can be defined as a generally binding formally defined rule of conduct established or sanctioned by the state for the purpose of regulating social relations in the sphere of public administration and ensuring public rights and freedoms of individuals and citizens.

S. H. Stetsenko accurately identified the specific features of administrative legal norms, noting that:

1. They express and consolidate the state interest and ensure the functioning of public administration, and consequently the state as such.
2. They have predominantly an imperative character and are ensured by the possibility of the application of state coercion.
3. They regulate relations in many spheres of social life (economy, construction, transport, internal affairs, healthcare, etc.) and in terms of complexity have no equivalents among other legal norms.
4. The structural elements of an administrative legal norm (hypothesis, disposition, sanction) are often contained in different normative legal acts.
5. They contribute to the protection of human rights against violations by representatives of public authority [9, pp. 70–71].

Administrative legal norms find their external expression in normative legal acts (laws and subordinate legislation).

Administrative legal norms regulating the procedure for the establishment of legal entities may traditionally be divided into empowering, binding, and prohibitive norms. The essence of empowering administrative legal norms regulating the procedure for the establishment of legal entities lies in granting the founders of legal entities a discretionary right to decide on the implementation of the behavioural options provided for by legal norms. Binding and prohibitive administrative legal norms, respectively, are manifested in imposing subjective legal obligations of an active or passive nature on participants in the establishment procedure. In particular, binding administrative legal norms impose on a person the obligation of active behaviour. Prohibitive administrative legal norms provide for the obligation of a person to refrain from committing certain types of actions [25, p. 196].

The next element of the mechanism of administrative and legal regulation of the establishment of legal entities is the *acts of implementation of subjective rights and obligations of participants in the establishment procedure*. In general, the implementation of legal norms is understood as the lawful behaviour of participants in social relations determined by legal prescriptions; as the embodiment of the provisions of legal norms in the actual behaviour (activity) of legal subjects; and as the realization of their prescriptions in the practical actions (or inaction) of subjects.

The following methods of implementation of administrative legal norms are distinguished:

— *compliance* — passive behaviour of a subject that prevents violation of administrative legal norms (for example, when founders comply with the requirements for the preparation of documents submitted for state registration of the establishment of a legal entity);

— *execution* — active behaviour of subjects aimed at fulfilling legal obligations established in administrative legal norms. For example, when the state registrar accepts documents for state registration of the establishment of legal entities in paper form according to an inventory and produces copies of these documents in electronic form (para. 2, 3 part 2 art. 25 of the Law of Ukraine "On State Registration of Legal Entities, Individual Entrepreneurs and Public Formations" [26]);

— *use* — active behaviour of subjects of administrative law in which they independently decide whether to carry out certain actions or refrain from them. For example, founders decide independently whether to submit documents for state registration of the establishment of a legal entity in paper or electronic form (part 2 art. 4 of the Law on State Registration [26]);

— *application* — the practical resolution of specific issues through the adoption by an authorized subject (as a rule, public authorities) of binding individual legally authoritative decisions [9, pp. 78–79; 27, pp. 162–165]. Application is the prerogative only of bodies vested with public authority, and its result is the adoption of individual legal acts, which will be discussed in the following subsections of this research.

However, the operation of administrative legal norms and the implementation of administrative legal regulation in general are impossible outside administrative legal relations, within which the relevant norms are individualized and the subjective rights and obligations of specific subjects, their powers and legal liability acquire concrete features [1, p. 542].

Administrative legal relations in the sphere of establishment of legal entities may be defined as social relations regulated by norms of administrative law, the parties of which (founders, participants, and bodies of the legal entity on the one hand, and public authorities and subjects exercising delegated powers on the other) are mutually connected and interact through the exercise of subjective rights

and obligations established by relevant administrative legal norms. The structure of these administrative legal relations is traditionally characterized by the interconnection of all their constituent elements, namely subjects, objects, the content of legal relations, and legal facts.

A specific feature of administrative legal relations in general is that they are formed within the sphere of public administration and one of the parties is always a bearer of authoritative powers; therefore, such relations have a public-authoritative character.

In the process of establishing legal entities, civil-law, commercial-law, and other types of relations also arise. However, within the framework of legitimation procedures, when founders apply to state bodies or local self-government bodies for the purpose of state registration of a legal entity, or when the head (representative) of a legal entity applies in order to obtain a licence or permits, that is, when "contact" with a subject of public administration occurs and a bearer of authoritative powers becomes involved in the establishment procedure (for example, a notary within the framework of the state registration procedure, performing the functions of a state registrar and thus exercising delegated public functions, is also a bearer of authoritative powers), we may speak about *administrative legal relations*.

It should be noted that administrative legal relations may arise on the initiative of any of the parties, and the consent or desire of the other party is not a necessary condition for their emergence, that is, they may arise even against the will of the other party.

In the process of establishing legal entities, most administrative legal relations arise on the initiative of founders, participants, or bodies of legal entities. The consent of the relevant subjects of public administration is not required. However, without such initiative voluntary establishment procedures usually cannot take place.

Administrative legal relations arise upon the occurrence of specific circumstances that cause their emergence, change, or termination.

These circumstances are referred to as legal facts. Only with the occurrence of relevant facts specified in the hypothesis of a legal norm do the grounds arise for the realization of subjective rights and legal obligations [27, p. 173]. Thus, para. 4 part 1 art. 4 of the Law on State Registration [26] establishes the declarative principle of state registration of legal entities. That is, without an application by interested subjects to state registration authorities such registration cannot take place. For this reason, some scholars identify legal facts as a separate element of the mechanism of administrative and legal regulation [28, p. 10; 29, p. 18].

The main forms of administrative and legal regulation of the establishment of legal entities include:

1) adoption of subordinate normative legal acts;
2) issuance of individual administrative acts;
3) conclusion of administrative contracts;
4) implementation of procedures of legitimation of legal entities, in particular state registration, licensing, and permitting procedures [24, p. 141].

At the same time, individual administrative acts, including those adopted in the sphere of establishment of legal entities, depending on the sphere of their application may be divided into: service acts, managerial acts, and delict acts.

A characteristic feature of the legal regulation of the establishment of legal entities is the combination of private-law and public-law principles, which determines a specific dualism of legal regulation. Accordingly, the method of legal influence in this sphere has an imperative–dispositive character, combining the necessity of strict compliance with legally established procedures and the requirement to act within legal prescriptions with the possibility for founders to independently determine certain aspects of the establishment of a legal entity at their own discretion.

Among the *methods of administrative and legal regulation of the establishment of legal entities* the following may be distinguished:

1. depending on the degree of use of authoritative powers: a) encouragement; b) persuasion; c) coercion;

2. depending on the nature of regulatory influence: a) administrative (direct); b) economic (indirect).

Within the procedures for the establishment of legal entities, the administrative method of legal regulation prevails, as it ensures strict compliance with legally established procedures, which guarantees the security and stability of the functioning of economic circulation. By their legal nature, procedures of state registration, licensing, and permitting procedures represent manifestations of the administrative method of regulation through which the regulatory influence of authorized subjects of public administration on the establishment of legal entities is implemented.

It should be emphasized that practically the entire process of establishing legal entities within the framework of administrative and legal regulation, that is, in its public-law component, consists of *procedures of legitimation* — state registration, licensing, and permitting procedures — which by their nature are administrative.

An administrative procedure is understood as a legislatively established procedure for consideration and resolution by public administration bodies of individual administrative cases with the aim of ensuring the rights, freedoms, and legitimate interests of individuals and legal entities, as well as the normal functioning of civil society and the state [21, p. 224]; or as legislatively established rules, order, and conditions for performing procedural actions regarding the consideration and resolution of a specific administrative case in the sphere of public administration [30].

N. V. Halitsyna identifies the following features of administrative procedures:

1) application in the public sphere;

2) regulation of the procedure for the implementation of law-enforcement activity;

3) coverage of managerial activity of a positive orientation;

4) establishment of a defined order for carrying out certain actions;

5) a specific subject composition (one of the parties is always a state body or an official endowed with state-authoritative powers);

6) consolidation in administrative procedural norms which regulate the application of substantive norms of administrative and other branches of law (financial, commercial, labour, etc.) and at the same time regulate the activities of authorized bodies and officials [31, p. 9].

Acquiring the status of a legal entity and obtaining the right to engage in the necessary types of activity requires the completion of mandatory legislatively regulated procedures: state registration — obligatory for all legal entities — as well as licensing and permitting procedures in cases directly provided for by law. These procedures are aimed at the legalization of both the legal entity itself and its activities and together constitute the procedure of legitimation of a legal entity [32].

In turn, the procedure of legitimation of a legal entity is administrative and legal in nature, as are the individual procedures of which it consists. All legitimation procedures are normatively regulated, their implementation is accompanied by imperative requirements at all stages; therefore, legitimation procedures constitute the public-law part of the process of establishing legal entities and are the subject of administrative and legal regulation.

From our point of view, procedures of legitimation of legal entities may be divided into:

1) *registration procedures*, within which the state registration of the establishment of a legal entity takes place and it acquires the relevant status;

2) *licensing procedures*, which provide for obtaining licences for engaging in certain types of economic activity;

3) *permitting procedures*, in cases where it is necessary to obtain permitting documents for carrying out certain actions in the course of economic activity or certain types of economic activity for which the law directly requires obtaining such permits.

Thus, the procedure of legitimation is an important element of the mechanism of administrative and legal regulation of the establishment of legal entities, reflects the specific subject of our research and emphasizes the public-law and administrative-procedural character of the legalization of legal entities.

Thus, the legitimation procedure constitutes an important element of the mechanism of administrative-legal regulation of the creation of legal entities. It reflects the specific subject matter of this study and emphasizes the public-law and administrative-procedural nature of the legalization of legal entities.

The procedure of legitimation of legal entities may be defined as a certain sequence of actions of an administrative and legal nature determined by law and aimed at the legalization of legal entities and their activities, and includes the procedure of state registration of the establishment of legal entities as well as licensing and permitting procedures in cases defined by law [24, pp. 146–147].

5. Conclusions

Based on the results of the conducted study of the essence and elements of the administrative-legal regulation mechanism for the creation of legal entities, the following conclusions can be formulated.

First, it has been established that the legal regulation of the creation of legal entities has a complex, interbranch character, as it is carried out through the norms of civil, commercial, and administrative law. At the same time, a significant part of the procedures related

to the emergence of legal entities has a public-law nature, since it involves the participation of public administration bodies in the process of official recognition of legal entities by the state. For this reason, administrative law plays a key role in ensuring procedural orderliness in the creation of legal entities.

Second, it has been clarified that the administrative-legal regulation mechanism for the creation of legal entities is derived from the general legal regulation mechanism and constitutes a system of interrelated administrative-legal means through which regulatory influence is exerted on social relations in the sphere of legal entity creation. Its functional purpose is the transformation of normative prescriptions of administrative law into specific administrative procedures and management decisions of public administration bodies aimed at ensuring legitimacy, legal certainty, and stability of legal entities' participation in civil and commercial turnover.

Third, it has been determined that the *administrative-legal regulation mechanism for the creation of legal entities* should be considered as a set of administrative-legal means applied by public administration bodies and delegated authorities in order to order social relations in the process of creating legal entities and to ensure the realization of the rights and legitimate interests of their founders and participants. Such subjects include, in particular, the Ministry of Justice of Ukraine and its territorial bodies, local self-government authorities, state registrars, notaries, as well as other public authorities authorized to carry out registration, licensing, and permit procedures.

Fourth, it has been substantiated that the structure of the administrative-legal regulation mechanism for the creation of legal entities includes interrelated elements, among which are:

— administrative-legal norms;

— administrative-legal relations, including subjects of administrative-legal regulation;

— acts of implementation of subjective rights and obligations of participants in the creation process, in particular, individual acts of public administration bodies;

— forms and methods of administrative-legal regulation;

— the procedure of legal entity legitimation.

It is precisely the interaction of these elements that ensures the effective functioning of the administrative-legal regulation mechanism in the respective sphere.

Fifth, it has been established that an important element of the studied mechanism is the procedure of legal entity legitimation, which includes:

— state registration;

— licensing;

— permit procedures.

The legitimation procedure has an administrative-legal nature and ensures the official recognition of legal entities by the state, as well as creates the legal preconditions for their engagement in commercial and other activities.

Sixth, it has been proven that a characteristic feature of administrative-legal regulation of the creation of legal entities is the combination of public-law and private-law principles, which determines the imperative-dispositive nature of legal influence. On the one hand, legislation establishes mandatory administrative procedures for creating legal entities, while on the other hand, it provides founders with the opportunity to independently determine certain aspects of their organizational and legal structure.

At the same time, the results of the conducted study indicate that certain aspects of the administrative-legal regulation mechanism for the creation of legal entities require further scientific consideration. Promising directions for further research in this sphere include: improving administrative procedures for state registration of legal

entities; optimizing the interaction of public administration bodies in the process of carrying out registration, licensing, and permit procedures; further implementation of modern digital tools of public administration in the field of legal entity legitimation; as well as harmonization of national legislation with European standards of administrative procedures and public governance.

The implementation of these directions will contribute to increasing the efficiency of administrative-legal regulation of the creation of legal entities, strengthening guarantees for the realization of the rights of business activity subjects, and forming a transparent and stable legal environment for the functioning of economic relations.

References:

1. Skakun, O. F. (2001). Theory of state and law. Kharkiv: Konsum. (in Ukrainian).

2. Vediernikov, Yu. A., Papirna, A. V. (2008). Theory of state and law. Kyiv: Znannia. (in Ukrainian).

3. Kelman, M. S., Murashyn, O. H. (2006). General theory of state and law. Kyiv: Kondor. (in Ukrainian).

4. Kurakin, O. M. (2016). Mechanism of legal regulation: theoretical-legal model. Extended abstract of Doctor's thesis. Kharkiv (in Ukrainian).

5. Bobrovnyk, S. V., Onishchenko, N. M. (1995). Social and legal effectiveness of legislation. In: Legislation: problems of effectiveness. Kyiv: Naukova dumka. (in Ukrainian).

6. Zaichuk, O. V., Onishchenko, N. M. (Eds.). (2008). [Theory of state and law. Academic course. Kyiv: Yurinkom Inter. (in Ukrainian).

7. Vediernikov, Yu. A., Hrekul, V. S. (2005). Theory of state and law. Kyiv. (in Ukrainian).

8. Bilozorov, Ye. V. et al.; Husariev, S. D., Tykhomyrov O. D. (Eds.). (2017). Theory of state and law. Kyiv: Osvita Ukrainy. (in Ukrainian).

9. Stetsenko, S. H. (2007). Administrative law of Ukraine. Kyiv: Atika (in Ukrainian).

10. Ostapenko, O. I., Ostapenko, L. O. (2007). Administrative and legal protection of property rights in Ukraine. Lviv (in Ukrainian).

11. Holosnichenko, I. P. (Ed.). (2005). Administrative law of Ukraine: basic concepts. Kyiv: HAN. (in Ukrainian).

12. Honcharuk, S. T. (2000). Administrative law of Ukraine. Kyiv (in Ukrainian).

13. Halunko, V. V. (Ed.). (2010). Administrative law of Ukraine in modern conditions. Kherson: Khersonska miska drukarnia (in Ukrainian).

14. Bevz, S. I. (2020). Administrative and legal regulation of public administration in the field of economic activity in Ukraine. Doctor's thesis. Kyiv. (in Ukrainian).

15. Kolomoiets, T. O. (Ed.). (2008). Administrative law of Ukraine. Kyiv: Istyna. (in Ukrainian).

16. Shkuropatskyi, O. I. (2017). On the definition of the concept of the mechanism of administrative and legal regulation of social protection of officers of the Armed Forces of Ukraine. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia "Pravo"*, no. 23, pp. 109–112. (in Ukrainian).

17. Zhydchenko, K. P. (2016). The essence of the mechanism of administrative-legal regulation of the realization by servicemen of the right to a one-time monetary assistance. *Yurydychnyi visnyk*, no. 3(40), pp. 67–72. (in Ukrainian).

18. Kuzmenko, O. V., Chorna, O. H. (2011). Public administration of extracurricular education in Ukraine. Kharkiv: Nika-Nova (in Ukrainian).

19. Kotiash, L. P. Administrative and legal regulation of state registration of legal entities in Ukraine. Candidate thesis. (in Ukrainian).

20. Rozhon, O. H. (2019). Administratyvno-pravove rehuliuvannia maloi pryvatyzatsii v Ukraini [Administrative and legal regulation of small privatization in Ukraine]. Candidate thesis. (in Ukrainian).

21. Halunko, V. V. (Ed.). (2015). Administrative law of Ukraine. Vol. 1: General administrative law. Kherson: Hrin D. S. (in Ukrainian).

22. Mosondz, S. O. (2006). Administrative law of Ukraine in definitions and schemes. Kyiv: Pretsedent. (in Ukrainian).

23. Yarmaki, Kh. P. (2006). Administrative supervisory activity of the police in Ukraine. Doctor's thesis. Kharkiv. (in Ukrainian).

24. Ilnytska, N. F. (2021). Administrative and legal regulation of the creation of legal entities. Candidate thesis. Kyiv. (in Ukrainian). Retrieved from https://ir.kneu.edu.ua/items/c06a89f2-3048-492f-bb5a-3cd846f242f6

25. Mosondz, S. O. (2008). Administrative law of Ukraine. Kyiv: Atika (in Ukrainian).

26. Verkhovna Rada Ukrainy. (2003). On state registration of legal entities, individual entrepreneurs and public associations. Retrieved from https://zakon.rada.gov.ua/go/755-15 (accessed 10 March 2026) (in Ukrainian).

27. Averianov, V. B. (Ed.). (2007). Administrative law of Ukraine. Academic course. Vol. 1. Kyiv. (in Ukrainian).

28. Hladun, Z. S. (2008). Administrative law of Ukraine. Ternopil: TNEU. (in Ukrainian).

29. Koval, L. V. (1998). Administrative law. Kyiv: Venturi (in Ukrainian).

30. Halitsyna, N. V. (2010). Administratyvna protsedura yak instytut administratyvnoho protsesu [Administrative procedure as an institution of administrative process]. *Forum prava*, no. 4, pp. 163–177. (in Ukrainian).

31. Halitsyna, N. V. (2010). Administrative-legal principles of the procedure for creation and functioning of limited liability companies in Ukraine. Extended abstract of Candidate's thesis. Zaporizhzhia (in Ukrainian).

32. Ilnytska, N. F., Kulaha, E. V. (2024). Sutnist ta zmist lehitymatsii yurydychnykh osib za zakonodavstvom Ukrainy [The essence and content of legitimation of legal entities under Ukrainian legislation]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia "Pravo"*, iss. 86, part 5, pp. 380–386. https://doi.org/10.24144/2307-3322.2024.86.5.55 (in Ukrainian).

ARCHITECTONICS OF COMPETENCE RELATIONS IN PUBLIC SERVICE

Karpa M.,
Doctor of Science in Public Administration, Professor,
Professor of the Department of Public Administration
and Management,
Hryhorii Skovoroda University,
Pereiaslav, Ukraine

Kitsak T.,
PhD in Public Administration, Associate Professor,
Deputy Director for Scientific and Pedagogical Work of Institute
of Public Administration, Governance and Professional Development,
Associate Professor at the Department of Public Governance,
Lviv Polytechnic National University,
Lviv, Ukraine

Abstract. The article examines the theoretical and methodological foundations of the architectonics of competence relations in public service. The study focuses on defining the essence of public service subjects, their functions, and the role of competence in structuring the system of public service. Public service is considered as a complex institutional system aimed at satisfying public interests through the provision of public services and the implementation of public authority functions. The research emphasizes that the competence of public service subjects determines the scope and content of their activities, distributes functions among different institutions and establishes the organizational framework of public administration. Special

attention is paid to the competency-based approach as an important methodological tool for improving the functioning of public service institutions and ensuring effective governance. **The purpose** of the article is to substantiate the theoretical principles of the architectonics of competence relations in public service and to determine the role of competencies in organizing the activities and interaction of public service subjects. **Methodology.** The research is based on a complex of general scientific and special methods. The system approach was used to analyze public service as an integrated institutional system. Structural and functional analysis helped to identify the relationship between functions and competencies of public service subjects. Comparative and logical methods were applied to clarify the conceptual and categorical apparatus and to generalize theoretical approaches to the formation of competencies in public service. **Results.** The study determines that a subject of public service is any public institution or official endowed with public service functions within the existing legal framework. The main features of public service functions include the service orientation, the implementation of public authority, and the focus on satisfying the interests of society. It is established that competence represents a set of legally defined powers, rights, duties and spheres of responsibility that determine the activities of public service subjects. The competency-based approach is substantiated as a conceptual framework for improving the organization, classification, and interaction of public service institutions. **Practical implications.** The results of the research can be used in the development of public administration reforms, improvement of the legal regulation of public service and formation of clear mechanisms for the distribution of functions and competencies among public service subjects. **Value / originality.** The originality of the study lies in the conceptualization of the architectonics of competence

relations in public service and the development of a competency-based approach that integrates institutional, functional and legal aspects of public service organization.

Keywords: Architectonics of relations, Public service, Competence relations, Allocation of powers (Distribution of competences), Public administration, Legal status of a public servant, Managerial interaction, Institutionalization.

1. Introduction

A relevant issue in the context of determining the relationship between competence and functional workload in the activities of public authorities is the study of public service functions. They define the directions of public service, as well as the essence and development processes of public service and its objectives. By studying their characteristics, it is possible to gain a deeper understanding of the nature of the public service system and its entities, as well as to classify public service entities and delineate their powers. The analysis of competence as one of the limiting criteria for establishing public service functions remains relevant. Since the public service is a system of entities performing public functions, the competence of the public service must generalize the competencies of all entities. Competence is one of the criteria defining the boundaries of public service functions and is restrictive in nature. The functions of public service are determined by the competence of the entity performing the service.

The institutional and functional approaches are commonly used as methodological prerequisites for defining the boundaries of public service. Institutionally, public service in a broad sense can be performed by employees of all public sector organizations: government institutions (i.e., not only the executive, but also the legislative and judicial branches), state-owned enterprises and institutions, local government institutions, and public utilities and institutions.

Researchers in this approach see the fulfillment of public tasks as fundamental to the definition of public service. In a narrower sense, institutionally, public service is considered to be service in government institutions and local government institutions.

Today, there are numerous approaches, arguments and trends in the study of the development of public service, its components, functions, etc. Among the main unresolved issues in the architecture and development of public service are: a lack of a clear understanding of the functions of public service and its components; duplication of functions between different types of services; the absence of a theoretical and methodological basis for constructing a clear public service structure; the conceptual and categorical apparatus for servicing an organization and performing public service has not been defined; and the lack of legal regulation of the concept of service. One of the important issues requiring more in-depth scientific research is the question of defining the main functions of the public service.

2. A Functional Approach to the Competencies of Public Service Entities

Architectonic laws play a key role in the study of complex systems, as they define their fundamental structure and harmonious patterns of development. They not only reflect the essence of holistic management mechanisms but also ensure sustainability, efficiency, and adaptability in the context of societal transformations. In the context of local government, the application of architectonic laws allows us to view this system not as static, but as dynamic, evolving in response to changes in the external environment and internal socioeconomic factors.

Such research is particularly relevant in the context of decentralization processes, when local authorities face the challenge of effectively managing resources, optimizing administrative structures and ensuring a balance between centralized and decentralized approaches.

The widespread functional approach to understanding public service in recent decades has focused on understanding public service not only as an activity of public sector institutions and organizations, but also as a tool for fulfilling public functions and objectives. Researchers even see the boundaries of public service defined through the implementation of public tasks and, accordingly, the expansion of the range of entities performing public functions. They cite examples of international experience involving not only the public (state and municipal) sector in the performance of public functions, but also delegating their implementation to public organizations and even private entities. There are numerous approaches to the issue of distribution of powers in general, among which the most prominent are the French state theory (the essence of which is that the distribution of powers is considered from the perspective of the problem of distributing the functions of state power), the German theory (through defining the powers of various government bodies), and the American theory (through cooperation, not only in legal but also political matters).

The study of the functions of public service primarily presupposes the systematization of scientific approaches to the study of the functions of civil service and local self-government as the main components of public service. In this part of the analysis of these functions, sufficient attention has been paid by domestic scholars; they are defined in the practice of state formation, enshrined in legislation and their implementation is constantly monitored and controlled. Since other participants in the public service also perform public functions, their activities remain poorly understood and unregulated in the context of the development of the public service. The research at this stage faces the following objectives:

— define public service actors as the actors performing functions;
— disclose the content of public service functions;
— define the main features of public service functions;

— identify criteria and classify the main functions of the public service according to them;

— analyze the competence of a public service actor as one of the limiting criteria for public service functions;

— explain the concept of "subject" and "object" functions in the context of establishing the competence of public service actors;

— schematically depict the competence of public service actors and its main components.

— show the relationship between the main components of competence (authority, scope of authority, jurisdiction, responsibility) and the functional content of public service actors.

Proponents of the second approach believed that the elements of a governing institutions competence are not the functions themselves, but rather the general right (in relation to the governed entity) and duty (to the state) to perform certain functions assigned to it, and, secondly, the set of specific rights and obligations (powers) necessary to implement these functions. Further analysis of this issue confirmed the conclusion that the competence of a governing institution is a legal reflection (mediation) of the functions assigned to the relevant institution in special, so-called competence (status) regulatory legal acts by establishing goals, objectives and the set of rights and obligations necessary for their implementation, i.e.

There is an approach that considers any institution, regardless of its form of ownership and subordination, endowed with public functions to belong to public administration institutions. It's worth noting that public functions are characteristic not only of public administration entities but also of other entities, namely, state and municipal organizations, institutions and enterprises. The specifics of operating procedures, tasks, financing, and other elements of activity differ significantly between the private and public sectors. Therefore, according to some researchers, the concept of public service may expand depending on

the scope of public functions. Considerable attention should be paid to the denationalization of certain public functions, which, accordingly, requires assigning a specific legal status to these entities, defining their powers, financing, distribution of tasks, etc. For example, public service in Germany is the activity of a public-law legal entity in the service of a legal entity. In addition to civil servants, the category of employees includes judges, professional military personnel, contract military personnel and employees and workers employed by a public-law legal entity. Since police officers and teachers are also civil servants in Germany, the proportion of civil servants is significantly higher than that of employees and workers employed in the civil service. There is a definition according to which public service in Germany is a professional activity consisting of the performance by certain entities of public-law functions in federal government bodies, state authorities, communities, and other entities of public law. Therefore, in the context of organizing the public service today, a clear definition of the essence of public functions is necessary, followed by their distribution among the entities of the public administration process.

According to the Constitution, the people are the bearer of sovereignty and the sole source of power in Ukraine. The people exercise power directly through state authorities and local governments (Article 5 of the Constitution of Ukraine). Article 140 of the Constitution defines local self-government as the right of a territorial community — residents of a village or a voluntary association of residents of several villages, a town, or a city into a rural community — to independently resolve local issues within the bounds of the Constitution and laws of Ukraine. Thus, the primary entity for establishing competence is the territorial community. Scholars emphasize that the Constitution of Ukraine limits the influence of acts of the President of Ukraine on expanding the scope of the Cabinet of Ministers' competence to the «functions» of the government only [1, p. 23]. Part two of Article 120

of the Constitution of Ukraine preserves the exclusive right to vest other powers in the Cabinet of Ministers only by law. This assertion is also noted in a more general constitutional provision: "State authorities... are obligated to act only... within the limits of their powers... stipulated by the Constitution and laws of Ukraine" (Constitution of Ukraine, Article 19, Part 2). Researchers also argue that "from the perspective of legal techniques for regulating the competence of any executive institution, the actual line between the definition of its functions, on the one hand, and its powers, on the other, is highly relative, although generally recognized in theory."

The implementation of public service functions by local governments and their substantive workload depend on the following circumstances:

— functions are largely determined by the territorial level of local government;

— the availability of resource potential and the ability to utilize it. The pressing issue pertains specifically to the economic component, the state of territorial development, and the source of local budget;

— the dependence, interdependence or autonomy of local government on state government.

In a state governed by the rule of law, each government institution and its officials have competence defined in regulatory legal acts and are obligated to act within their scope. Thus, the competence of the head of state and the highest authorities and administrative institutions is defined by the constitution, while that of other government institutions is determined by laws and regulations governing these institutions.

The competence of government institutions is specialized and not equal for all government institutions. The procedure for establishing and the scope of competence depend on the level of government in which the government institution belongs — legislative, executive, judicial, prosecutorial, etc. Unlike individual entities, the legal status of

collective entities — state institutions — as subjects of legal relations is limited by the goals and objectives for which they are created. The specific nature of the exercise of powers by state institutions lies in their operation within a subsystem of public law (constitutional and administrative law), which is characterized by the imperative method of legal subordination and subordination. On the one hand, these are issues of the competence of state institutions and officials who have the authority to unilaterally issue individual orders defining the rights and obligations of subordinates and accountable persons; on the other hand, these are issues of the passive legal personality of subordinates and accountable persons, their dutie, and responsibilities. The will of subordinates is not decisive for the individual act issued.

If state and local government authorities are considered components of public service, then the functions of state and local government authorities should also be considered as components of the functions of public service. Consequently, the functions of public authorities are the main areas of their activity, which reveal their essence and purpose within the state mechanism. Each institution, in accordance with its competence, performs its inherent functions.

There is also a tendency to distinguish the functions of public authorities. In the scientific literature, the concepts of "subject" and "object" functions are often equated. However, they are mostly compared as general (object) and partial (subject). From a legal perspective, in the context of analyzing the components of competence, it is more appropriate to use the concept of "subject functions" since it correlates with the concept of "subject matter." However, "subject" is categorically narrower, with a specific, concrete content, than "object." Therefore, we often encounter object functions both in the regulatory framework and in management practice. Today, it's traditional to consider the following functions of the state and its agencies to be objective: economic, social, cultural, environmental, defense, political, humanitarian and so on. Can

these functions be considered subject-matter functions? Object-matter functions reveal the main focus, primarily by sector. Therefore, it seems logical to base the competence of public service entities on the subject-matter functions of the state.

So, the main feature (goal) of public service functions is to satisfy the public interest by providing public services; performance of public authority functions; performance of functions and tasks of public institutions. It is appropriate to note that the practice of state administration in a substantive sense distinguishes the objects of the implementation of public service functions according to the following criteria: by purpose or spheres of influence — economic, social, spiritual, political, cultural, humanitarian; functionally — types of activities and social roles; on the organizational and structural basis — organizational forms acquired by objects and within which they function (administrative units such as local social systems, enterprises and organizations, branches of the economy and inter-industry complexes, public institutions, spheres of society, etc.). The complexity of object management is determined by their content characteristics, abundance, changes in the social environment, the influence of external factors and the constant dynamics of the development of the sphere of management processes in society.

3. Formation of the content of the competences of subjects of public service

In contrast to the functions outlined in a sufficiently general way, the competence of the subject of public service is determined by clear formulations, the exact direction of public administration and specific tasks determined by the subject's goals. The competence of public service subjects is always more clearly established in the legal field than the functions partially determined by legal norms. Competence determines the scope and content of the subject's activity; demarcates

functions with other entities; establishes a certain distribution of functions implemented by the public service as a whole. Competence is established above by the subject of public service by subjects according to the hierarchical principle or by the will of the people according to the electoral principle.

The most significant and key element of competence is determined by powers. Powers in legal literature are interpreted as "legal obligations", that is, it refers to the simultaneous availability of rights and the obligation to apply them. Article 3 of the Constitution establishes the normative basis of this statement. Human rights and freedoms and their guarantees determine the content and direction of state activity. The government is accountable to the people for its activities. Affirming and ensuring human rights and freedoms is the main responsibility of the state.

The central place and the dominant part among the powers of the executive institution are state-authorized powers, that is, the powers to make mandatory decisions and ensure their implementation of the subject to whom they are addressed.

Delegated functions, powers — functions, powers (rights and obligations) acquired by a certain subject (organ or official) by transfer to him for execution by another subject at the latter's own decision or on the basis of a law. "Delegation" means, as a rule, the transfer of functions, the power of attorney for the time being, while the delegating entity has the right to return it to its own performance. At the same time, the delegating entity acquires the right to control the state and consequences of the performance of delegated functions, the proxy; he can also finance their implementation from his own funds, transfer the necessary property objects for use. This question concerns the development of mechanisms for the implementation of powers.

There are known situations in which subjects have identical powers, which do not need to be matched with the same competence. In

each case, the competence is formed as an individual one for each subject of service implementation, that is, the principle "the same authority — different competence" applies. The second principle of competence delineation should be considered the scheme "the subject of management is the same — the powers are different." This is a more common practice of public service implementation, because the subjects of management today are not formed into a single database, which creates often adjacent competences of many subjects. For example, such identical subjects may be related to ensuring the defense capability and national security of Ukraine, but their implementation will be different in accordance with the acquired statuses of different institutes.

The practice of matching generalized functions to subjects of knowledge looks debatable, because it has more object characteristics than functional ones. According to the definition of the subject functions with an extended approach to the subject of the competence of a separate subject of the implementation of public service, it is expedient to distinguish the competences of different subjects within the performance of one function.

The criteria for determining the list of positions for government agency employees performing service functions are the content and nature of the work they perform, which in the vast majority of cases does not include the exercise of powers directly related to the performance of the tasks and functions defined in Part One of Article 1 of the Law of Ukraine "On Civil Service," nor work related to ensuring appropriate conditions:

— comprehensive maintenance and repair of buildings, restoration and construction and installation work;

— document management and record keeping (except for employees processing restricted documents);

— computer support and the implementation of information technology (except for employees whose responsibilities include the

administration of national registries and databases, as well as ensuring information security);

— secretarial and stenographer functions, computer typesetting, working with copying and duplicating equipment, recording and processing digital data;

— archive management and library services;

— logistical and economic support. Positions of employees performing service functions, as well as those of managers and deputy managers of independent structural divisions of government agencies, are not considered positions.

A common approach is to view competence as a combination of powers and areas of jurisdiction. Including areas of jurisdiction within competence significantly simplifies the relationship between government agencies and local governments. Analysis of this approach points to the practice of simplifying processes in an attempt to delineate competencies both in public administration practice in general and in the sphere of public administration [2, p. 195]. Defining the competence of each governing institution will allow for the immediate delineation of powers, creating a legal, organizational, structural and institutional environment with corresponding spheres of influence and the ability to perform functions. The problem arises from the fact that a generalized principle of establishing competence, often sectoral, is typically used. The primary area of jurisdiction for public service entities can also be considered the provision of public services. Their listing and the identification of providers of public services are a primary objective for delineating the powers of public service entities. The Concept for Reforming Local Self-Government and Territorial Organization of Authority in Ukraine notes that the second stage of the Concept's implementation (2015–2017) envisages unifying and standardizing public services provided to the population by local governments and executive authorities, taking into account the

principles of maximum accessibility to consumers and defining these principles in legislation.

The object of public administration by the state is those social relations, activities and social roles directly related to the production of material and spiritual products and the reproduction of the social conditions of human life. This indicates that the state does not manage everything, but only those manifestations of social relations, various activities, social roles, parties and relationships that are significant for the entire society and relate to the realization of common needs, interests and goals. The reproduction of material and spiritual products and social conditions receives primacy and significance for human life. Article 140 of the Constitution of Ukraine states that local self-government is the right of a territorial community to independently resolve local issues within the bounds of the Constitution and laws of Ukraine. Currently, there is no unified doctrinal understanding of the essence of local issues. The current paradigm is "only what is provided by law is permitted." Since local issues are not constitutionally defined, we turn to the Law of Ukraine "On Local Self-Government," which, according to experts, is "a kind of catalog of the functions and powers of local government institutions and officials."

The difficulty arises primarily from the lack of a legislative definition of "matters of local importance." The existence of a constitutional and declaratory definition of this concept creates significant problems both in the practice of public administration and in its theoretical and organizational support. Consequently, problems arise in the redistribution of functions among public service entities, and various balances of competence arise due to the ambiguity of this component of competence. There are proposals, in accordance with the European Charter of Local Self-Government, to explicitly stipulate that, with regard to the assignment of matters of local importance, local government institution and officials, as well as territorial

communities are granted all functions and powers, except those assigned to state authorities by the Constitution and laws of Ukraine.

The competencies of public service entities are defined according to a traditional, rather sectoral, scheme that has developed over many decades of traditionally planned economies and national economic development planning. State and municipal authorities have traditionally focused on the development of spheres of the state and local economy. Modern trends will orient the authorities toward defining issues of state and local importance. Defining specific areas of jurisdiction (in a narrower sense, based on the object and territorial principle) for public service entities at the local level will facilitate the expansion of local autonomy, enhance decentralization processes and delineate the functions and powers of the executive branch and local government, as well as the specific characteristics of the local territory.

Considering local specificities, cultural and historical traditions, social, economic, geographic, infrastructural, and other characteristics is of great importance when determining the scope of activities of local government entities.

The lack of a legislative definition of local issues as the primary focus of municipal government activity has led to the functions and powers of local government in Ukraine being defined according to the traditional sectoral principle. This approach is not focused on the territorial community, that is, not on the residents, as required by the Constitution of Ukraine, but on the areas of local life in which the institutions of these territorial communities are competent and their powers: exclusive, proprietary (self-governing) and delegated. A wealthy territorial community is a territorial community of villages (towns, cities) that, through voluntary association, is capable, independently or through the relevant local government institutions, of providing an adequate level of services, particularly in the areas of education, culture, healthcare, social

protection, housing and utilities, taking into account human resources, financial support and financial security.

Typically, the issue of determining public interest is advisory and consultative in nature. To ensure that the interests of territorial communities are taken into account when developing a draft long-term plan, officials authorized by the Council of Ministers of the Autonomous Republic of Crimea and the regional state administration consult with authorized representatives of local government institutions and their associations, as well as business entities and their public associations.

Regarding responsibility as a component of competence, two fundamentally different approaches to the concept of responsibility must be considered. According to the first approach, responsibility is considered as part of competence, which serves as a tool for monitoring the implementation of that competence. Responsibility (other than political) of executive institutions is a specific state (regime) of organizational relations between executive institutions, according to which a specific institution(official) has the right to apply disciplinary (official) liability measures to other institutions (officials).

The fundamental connection between competence and competency, systemically linked to results, is essential to the concept of "responsibility" and the basis for the new development of the concept of public service. The structure of responsibility includes competence, competence (the exercise of competence) and its result. To establish responsibility, it is necessary to establish its correspondence with the desired result.

Structurally, all elements of the competence of public service entities are interconnected, allowing us to assert a holistic and indivisible system. Exclusion or the presence of gaps in their formation creates an imbalance in the concept of competence, which in practice contributes to negative consequences in matters of determining

competence, delineating powers, duplication and the emergence of competence disputes.

The study identifies the main types of competence — sectoral, territorial and functional — which serve as the source for the formation of other types of competence, their classifications, divisions, etc. For example, intersectoral public administration functions were assigned to state committees. Currently, intersectoral competence is vested in the following executive branches:

— ministries;
— services;
— agencies;
— inspectorates;
— central executive institutions with special status;
— other central executive institutions;
— national commissions.

According to the researchers, the territoriality criterion is the primary distribution of powers and authority among government institutions and, consequently, their overall competence. Based on the territoriality criterion in public administration, it is appropriate to distinguish:

— national competence;
— territorial competence;
— local competence;
— local competence.

In the context of this issue, it is appropriate to consider other, particularly contractual, fundamental principles for defining and implementing competence. Examples of contractual positions in terms of defining competence include:

— at the national level — social dialogue, social partnership;

— at the international level — international agreements and treaties in various spheres of public life;

— non-legal positions — personal agreements, services, etc. outside the legal framework, including criminal offenses such as corruption, abuse, negligence, various types of misconduct, etc.

The Law of Ukraine "On Social Dialogue in Ukraine" [3] defines social dialogue as the process of identifying and harmonizing positions, reaching common agreements and making coordinated decisions by the parties to social dialogue, representing the interests of employees, employers, executive authorities and local governments, on issues of the formation and implementation of state social and economic policy. The treaties and legislation of the European Union define the term «social dialogue» as a procedure for joint consultations of social partners at the European level. Today, social dialogue in public administration functions as an effective tool for establishing a specific type of social relations between actors characterized by the presence of not only common interests, but also opposing social, economic and political beliefs. All social groups, as well as the state, have an interest in the establishment and development of such dialogue, as social dialogue further creates the preconditions for political and social stability in society and its progressive socio-economic development. Social dialogue, as an institution of public administration, occupies a key place in ensuring the participation of employers and employees in the development and implementation of social, labor and socio-economic policies and serves as a unique tool for balancing the interests of employees, entrepreneurs and government for the benefit of society as a whole.

Social dialogue is an effective tool for reconciling the conflicting interests of participants, a forum that enables constructive interaction to achieve common socially significant goals. Participants in broad-based dialogue include, for example, the state, employees and employers, local governments, scientists and business representatives, united in institutions as parties to social dialogue. Treaty-based

competence in the international context and its application translates into a transfer of powers between countries participating in the relevant agreements. This transfer of powers to supranational structures involves a corresponding transfer of authority, resources, responsibilities and jurisdiction—in other words, all components of these competencies, with the potential for their influence within the defined scope of their competence.

Consequently, having systematized the competencies of all public service entities, taking into account various approaches, it can be stated that the competence of the public service, by institutional definition, is the competence of public service entities; the competence of civil service institutions; the competence of local government institutions; the competence of state-owned enterprises, institutions, and organizations; and the competence of other persons engaged in labor relations with public legal entities. With this approach, a common situation is where a large number of entities have virtually identical powers, but the competence of each is defined individually, characterized by differences in jurisdiction. Consequently, the competence of the public service, by functional definition, can be considered the totality of tasks established by regulatory legal acts, the functions of public service entities and the rights and obligations of officials in public service. The competence of a public service entity determines the precise scope of its activities and coordinates them with the activities of other entities. Having received broad powers, the executive branch must ensure a mechanism for fulfilling its functions and influential means of supporting its own activities. To achieve this, a broad range of measures must be implemented, including: optimizing the public administration structure at all levels of the executive branch, beginning with the network of ministries and agencies; rationally delineating powers, rights, and responsibilities across the entire executive chain; establishing a clear system of accountability

for assigned tasks among managers at all ranks; reducing wasteful expenditures associated with the functioning of executive institutions and the structures supporting their activities; and other urgently needed reforms [4].

There are numerous studies aimed at examining the relationships between the functions and competencies of government entities, state institutions, local governments and other public service entities. These relationships are examined both between entities and at the level of each individual entity. Having analyzed the main elements of competence, it can be argued that functions are the areas for implementing the competence of a public service entity. The content of competence, compared to functions, is more dynamic and subject to change more frequently. The main areas of activity of public service entities are derived from the primary functions of the public service; in other words, the functions of the public service are distributed among all entities depending on their place in the public service system [5].

4. Conclusions

To summarize, we highlight the following points. In this study, a public service entity is defined as any institution, official or service provider vested with public service functions, regardless of ownership or subordination. The key characteristics of public service functions are: satisfying the public interest through the provision of public services; performing public authority functions; defining them through the areas of activity of public institutions (state institutions implement state functions; local governments ensure the fulfillment of community functions; enterprises, institutions and organizations operate within the scope of their assigned public service functions); service-oriented nature; aimed at satisfying the public interest, that is, the interests of the social community; determined by societal needs and the competence of the institution performing a given function,

among others. Competence determines the scope and content of the entity's activities; delineates functions between different entities; and establishes a specific distribution of functions performed by the public service as a whole. Consequently, the competence of the public service from the standpoint of the connection between the functions and competencies of public service entities can be considered a set of tasks established by regulatory legal acts, functions of public entities, rights and obligations of officials who are in the public service to perform the established functions.

Revealing the theoretical aspects of developing public services as warehouse systems is of great importance both at the legislative level and for the practical implementation of state-building and mass business development. A more detailed discussion of the challenges associated with creating methodological security for the development of public services is needed to define the categorical apparatus for servicing new service systems, creating a check-based transition to public services and so on. The functions of these systems should be distributed among public service entities. Supplementing the functions of public services with the core activities of public service units in additional scientific research makes it possible to create a structure and classification of public service units, define competencies for each and facilitate their better implementation.

The conceptual aspects of a competent approach to public service development define the core principles, method, object, and subject. A competency-based approach label for public services is indicated, which is used in subsequent research and practical work on attracting, recording, and implementing the competencies of public service entities. It is stated and substantiated that the objects of a mandatory competent approach in public services and public service entities are: The competence of public service entities is essential to a competent approach in public services. For storage, hardware is provided and

the provision of a competent approach in public services is formed in two areas: in the context of strengthening practical warehousing and scientific research. The conceptual basis for a competent approach in public services is formulated based on the fundamental principles of a legal framework, mutual modalities, control and awareness. Therefore, specific principles, primarily among them, are important: securing the constitutional and legal status of public service entities; linking public service entities with the establishment, development, and implementation of competencies; standardizing the integrity of public service entities (publications); the functioning of public service entities in areas of territorial and institutional delimitation and remoteness.

This work updates the provision for each institution, identifying public service entities, conducting pre-assessment studies to develop their competence in partially acquiring the status of a public institution. Furthermore, the institutional significance of public authorities in the processes of forming and implementing their competencies should be realized within the framework of the significance of public service entities and their competencies. The monograph emphasizes that public service entities are state institutions and public services that are local public services, endowed with status within the interstate legal framework for these institutions and conduct public affairs. The competencies of public service entities include the availability of benefits and legally established guarantees (rights and privileges), the scope of activity (whether travel is provided for), the obligation to sign a contract, the entity's reliability, etc., and the creation of a state institution aimed at implementing public functions and performing public functions. It is noted that the competencies of public service entities indicate the commonality and closeness of the entity; this delimits the functions between different entities; one of the sections of functions implemented by the public service is established.

References:

1. Oliushko, I. B. (2002). Vykonavcha vlada ta problemy administratyvnoi reformy v Ukraini [Executive power and problems of administrative reform in Ukraine]. Kyiv: Fakt, 260 p., pp. 40–43. (in Ukrainian).

2. Tkachenko, A. O. (2009). Poniattia kompetentsii derzhavnoho orhanu [The concept of competence of a state authority]. *Chasopys Kyivskoho universytetu prava*, no. 4, pp. 192–197, p. 194. (in Ukrainian).

3. Verkhovna Rada Ukrainy (2010). Pro sotsialnyi dialoh v Ukraini: Zakon Ukrainy vid 23.12.2010 № 2862-VI [On social dialogue in Ukraine: Law of Ukraine of December 23, 2010 No. 2862-VI]. Available at: http://zakon4.rada.gov.ua/laws/show/2862-17 (in Ukrainian).

4. Karpa, M., Zbarovskyi D. (2023). Kompetentsiia orhaniv publichnoi vlady shchodo formuvannia derzhavnoi polityky u sferi ekolohichnoi bezpeky Ukrainy: normatyvno-pravovyi aspekt [Competence of public authorities in the formation of state policy in the field of environmental security of Ukraine: regulatory and legal aspect]. *Investytsii: praktyka ta dosvid*, no. 14, pp. 148–154. https://doi.org/10.32702/2306-6814.2023.14.148 (in Ukrainian).

5. Karpa, M., Kitsak, T. M. (2024). Kompetentsiia orhaniv derzhavnoi vlady ta orhaniv mistsevoho samovriaduvannia v umovakh detsentralizatsii: zaprovadzhennia yevropeiskykh pryntsypiv i standartiv [Competence of state authorities and local self-government bodies in the conditions of decentralization: implementation of European principles and standards]. *Investytsii: praktyka ta dosvid*, no. 3. https://doi.org/10.31470/2786-6246-2023-6-82-89 (in Ukrainian).

THE RUSSIAN-UKRAINIAN WAR: A TEST FOR THE INTERNATIONAL LEGAL ORDER AND GLOBAL DIPLOMACY

Krupenya I.,
Candidate of Political Science,
Associate professor of the Department of World History,
International Relations and Methods of Teaching
Historical Disciplines
Sumy State Pedagogical University named after A. S. Makarenko,
Sumy, Ukraine

We need to do everything possible to make sure
that Ukraine has what it needs,
in terms of training and equipment, to prevail in this fight,
which started in February 2022,
with the massive and unprovoked onslaught of Russia on Ukraine.
NATO's Secretary General, Mark Rutte

Abstract. The article examines the current issue — how Russia's open armed invasion into Ukraine has affected the international legal order and the effectiveness of global diplomacy. The russian-Ukrainian war is an immense test for global diplomacy, revealing both the strengths and limitations of existing diplomatic frameworks. While international efforts to support Ukraine and punish russian aggression demonstrate the power of collective action, the conflict has also exposed deep divisions within the international community. The ability of global leaders to balance their own national interests with the broader goal of peace and stability will ultimately determine the course of this war and its

long-term impact on international relations. It has been established that the war of aggression in Ukraine is a fatal mistake of the Putin regime and a terrible crime against humanity that will forever remain in the textbooks of world history. It was stated separately that the myth of russia as a peaceful state has been finally dispelled among the international community, and this is already becoming a bitter reality for its population. **The purpose** of the paper is to investigate how russia's an open armed invasion into Ukraine examined the international legal order and global diplomacy. **Methodology** of the study is based on general research methods of analysis and synthesis, induction and deduction, observation and abstraction, which are used to systematise achievements in the theory and practice of modelling systems of different nature in the humanities and, in particular, in political science. Using general research, logical and empirical research methods, the following tasks were solved: the impact of the russian-Ukrainian war on the state of the rule of international law was investigated; the consequences of russian aggression against Ukraine for national and regional security were analysed; it was found out which principles of international law and international conventions were violated by russia over the last ten years of the war. **Results** of the study showed that Russia has violated all currently valid principles of international law and committed war crimes, the crime of aggression, crimes against humanity, and genocide. The results of the research are of practical importance and can be used in education for teaching such disciplines as international relations and world politics, the history of international relations, the history of world diplomacy, international law, political science, international conflicts and the humanitarian factor in world politics, etc. In addition, the results of the study may be useful in bringing the aggressor to international responsibility for committing the crime of aggression against Ukraine.

Keywords: Russian-Ukrainian war, International legal order, Global diplomacy, Aggression, International law, Collective security system, Sovereignty and territorial integrity, Geopolitical transformation

1. Introduction

The study begins with the words of the NATO's Secretary General, Mark Rutte during a meeting of the Ukraine Defense Contact Group at the level of Ministers of Defence, hosted by the US Secretary of Defense, Lloyd Austin, at Ramstein Air Base (Germany) on 9 January 2025. Mark Rutte pointed out: "We need to do everything possible to make sure that Ukraine has what it needs, in terms of training and equipment, to prevail in this fight, which started in February 2022, with the massive and unprovoked onslaught of Russia on Ukraine" [1]. The common task of the partners is to ensure a strong position of Ukraine for the approach of a just and lasting peace [2].

Only a just peace can put an end to this war, which began in February 2014. Most countries in the world could not believe that the tragedy of this situation lies in the fact that this violator of international law in the 21st century was a country that was once part of the Soviet Union and had made a significant contribution to the victory of defeating Nazism [3, p. 11]. After the downing of the Boeing 777 Malaysia Airlines flight MH17 by a russian-made Buk anti-aircraft missile system on July 17, 2014, near Torez, Donetsk region, was it clearly demonstrated to the whole world what russian aggression really means, and that terror knows no borders. The flight was on its way from Amsterdam to Kuala Lumpur. On board were 283 passengers and 15 crew members. All 298 people on board lost their lives. This terrible event became the first manifestation of the unity of the civilized world against russia's unlawful behaviour and one of the

first visible manifestations of russia's armed aggression against Ukraine. It is no coincidence that this study was started by the words of NATO's Secretary General, Mark Rutte. At the time of the downing of the Malaysian plane, Mark Rutte was the Prime Minister of the Netherlands. He personally tried to resolve the situation through negotiations, but Russia is unwilling to stop its violations of international law. Mark Rutte the Prime Minister of the Netherlands paid the visit to Kharkiv and met with both the President of Ukraine and the Ukrainian investigators and rescuers who participated in the work of the joint investigative team on the criminal investigation of the crime of downing of flight MH17. During the meeting in Kharkiv, he once again recognised what is brutal terrorist war [4, p. 192–194]. To date, the russian federation has not acknowledged its responsibility for the downing of Malaysian Airlines Flight MH17. Moreover, the russian federation violated not only the Convention on Combating the Financing of Terrorism by Providing Weapons and Other Types of Assistance to Illegal Armed Forces [5] but also the Geneva Declaration on Terrorism [6], Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land [7], United Nations Charter [8], Helsinki Final Act [9], Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations [10], Memorandum on security assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapons [11] etc. The violation of above-mentioned international treaties during the russia's hybrid aggressions (2014–2022) and an open armed invasion by the russian army into Ukraine (24 February 2022 — till date) is a test for the international legal order and effectiveness of global diplomacy.

2. The ambiguous responses of international community on Putin's war against Ukraine

The russian-Ukrainian war represents a severe test for the international legal order. It challenges the norms and frameworks of international law in areas such as sovereignty, the use of force, human rights, and accountability for war crimes. Since the beginning of the armed aggression against Ukraine in 2014, russia has violated more than 400 international treaties to which Ukraine and the russian federation are parties and has disregarded 22 fundamental international documents since 2022 [12].

When Russia launched its aggressive war against Ukraine, it violated the *prohibition on the use of force* embodied in Article 2(4) of the United Nations Charter. This prohibition was imposed after World War II in 1945. When Putin launched his war, he put that underlying principle at risk. But the test of a legal rule — whether domestic or international — is not determined simply by whether it is violated. It is determined, too, by the response when it is violated [13]. On 23 February 2023, at the renewed 11th Emergency Special Session of the UN General Assembly regarding the aggression of the Russian Federation against Ukraine, only 141 states voted "YES" for the resolution "Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine" [14]. A similar situation occurred after Russia's armed occupation of the Crimean Peninsula. When voting for UN General Assembly Resolution № 68/262 dated March 27, 2014, on the territorial integrity of Ukraine at the 68th session of the UN General Assembly, 100 UN member states voted "for", 11 voted "against", and 58 countries abstained. The facts of the vote in the UN General Assembly clearly demonstrate to us the ambiguous reaction of the international community to the violation of international law [15].

On January 13, 2025, at the UN headquarters in New York, USA, at the initiative of Ukraine, a meeting of the UN Security Council under

the Arria formula was held on the topic "Violations of international humanitarian law against Ukrainian prisoners of war and civilians". Thus, Ukrainian diplomats tried to draw attention to the growing amount of evidence of gross violations of international humanitarian law by russia. In particular, the systematic use of torture by the russian authorities, which constitutes a crime against humanity, the ill-treatment of prisoners in places of detention, the use of torture, sexual violence and the complete lack of medical care, which leads to severe physical and psychological consequences [16].

As we see, the responses of international community on Putin's war against Ukraine to differ from condemnation and prosecution for crimes against humanity, war crimes the crime of aggression, genocide to support by some countries Putin's policies or taking a neutral position. If we are talking about adhering to the principle of the rule of international law, then such a position of the international community only undermines the international legal order and is a test of the survival of the international order that was created after the end of World War II.

3. **The russian-Ukrainian war is a severe test for the international legal order**

Analysing the behaviour of the Putin regime, it can be argued that the Kremlin is pursuing a purposeful policy of undermining the entire system of international law and world order, violating absolutely all the principles of international law. Supporting the opinion of Ukrainian scientists and diplomats, it is worth noting that the UN must be reformed or this organization will suffer the fate of the League of Nations, which ceased to exist after World War II. Destabilizing the system of international relations, russia is trying to impose the law of the strong on the world and openly refuses to fulfil the treaties it has signed if it considers it unprofitable for itself. Thus, violating Articles 26 and 27 of the Vienna Convention on the Law of Treaties

of 1969 and the fundamental principle of international law "pacta sunt servanda" ("every treaty in force is binding on its parties and must be performed by them in good faith").

At the same time, an analysis of compliance with international treaties and conventions clearly demonstrates that russia has never complied with its obligations, despite the fact that russia signed the Vienna Convention on the Law of Treaties of 1969 in 1980. Article 27 of the Vienna Convention states that "A party may not invoke the provisions of its internal law as a justification for its failure to perform a treaty" [17].

Ukraine has accordingly implemented this article into its domestic legislation. On June 28, 1996, the Verkhovna Rada of Ukraine approved in Article 9 a constitutional provision that effective international treaties are part of national legislation. The conclusion of international treaties that contradict the Constitution of Ukraine is possible only after making appropriate amendments to the Constitution of Ukraine [18].

A similar provision was contained in the russian Constitution. However, on December 8, 2020, V. Putin signed a package of laws that establish the priority of the Constitution of the russian federation over international treaties with the wording: "the application of the norms and rules of international treaties of the russian federation in their interpretation that contradicts the Constitution of the russian federation is not allowed." In addition, the Law "On International Treaties of the russian federation" stipulated that the Constitutional Court of the russian federation now has the authority to review decisions of international courts and intergovernmental bodies for compliance with the Constitution [19].

In the situation of armed aggression by russia against Ukraine, the UN demonstrates its powerlessness to guarantee the seven basic principles of international law (sovereign equality of states, non-use

or threat of force, equality and self-determination of peoples, peaceful settlement of international disputes, non-interference in internal affairs, cooperation, and good faith fulfilment of obligations under international law), which are enshrined in Article 2 of the UN Charter [8]. In the context of the UN's powerlessness, the focus of international attention has been primarily on the problem of transforming the most influential body of the United Nations, the Security Council. The structure of the UN Security Council and the mechanisms for approving decisions, which the victorious countries in World War II agreed on at the Yalta Conference in 1945 and which are based on the principle of division into permanent and non-permanent members and granting the former — the USA, the USSR (and today its successor the russian federation), the People's Republic of China, France and Great Britain — the right of veto, no longer correspond to current realities, because the exclusive possession of the right of veto by the leading players in world politics is a *direct violation of the principle of equality of UN member states.* Today we are witnessing a trend of crisis in the system of international law, when great powers increasingly neglect, proceeding from the primacy not of the power of law, but of the law of force [20].

The ambiguous attitude of the world's countries towards russia's aggression against Ukraine is a serious violation of *the principle of justice in international law*. Ukraine cannot forget and "reset" everything that russia did in Bucha, Olenivka, Avdiivka and in all other destroyed or damaged cities and villages of Ukraine" [21]. If we turn to the criminal law of any country in the world, no criminal code in the world justifies a murderer or a rapist! Accordingly, the position of many countries of the world, which took a neutral position when voting for the resolution "Territorial Integrity of Ukraine: Compliance with the Principles of the United Nations Charter", is incomprehensible [22].

All these arguments demonstrate Moscow's revanchist attempt to influence the historical turn that occurred in 1989. According to the

President of Ukraine, which he publicly expressed on December 11, 2023, during his speech at the US National Defense University, russia needs Ukraine purely as a springboard to be able to behave again like the empire that died in 1989 and to question the leadership of freedom wherever the russian Tsar pleases. Putin must lose so that all others who perceive russia's war against Ukraine as a personal lecture at the so-called university of aggression receive this message loud and clear. Putin must lose [23]!

On February 24, 2022, russia violated another *fundamental principle of international law — the inviolability of borders* and carried out an open armed invasion of the territory of a sovereign state. The armed invasion of russian soldiers into the territory of Ukrainian land was accompanied by mass killings of civilians, shelling of kindergartens, hospitals, residential areas, use of cruise missiles against the civilian population, shooting of school buses, blocking of ambulances, sexual violence, destruction of cities, civilian infrastructure, cultural heritage sites, healthcare facilities, outright looting, kidnapping and forced resettlement of Ukrainian children, nuclear terrorism, strikes on critical energy infrastructure of Ukraine, forcing citizens to participate in military operations against their own state, blockade of Ukrainian ports and theft of Ukrainian grain, etc. This is a gross violation of *the principle of international humanitarian law*. Moreover, the terrorist state, through the mouth of President V. Putin made illegal demands, including: to change Ukraine's domestic and foreign policy; to renounce the right to self-defense, to implement the national idea of building an independent, democratic state; to shift responsibility for the crimes committed from the aggressor to the victim; to recognize his superiority and the correctness of his own illegal actions — the occupation of territories, the destruction of the population, the destruction of settlements, the destruction of law in his understanding and perception recognized by the entire civilized world [24].

4. The Russian version of the justification for an open military attack

For the world community, the russian federation has prepared another lie, justifying the so-called "special military operation in Ukraine" after "the authorities of the DPR and LPR requested assistance in repelling Kyiv's aggression". This was announced by russian President V. Putin in an emergency address. On February 24, 2022, he announced the start of a special operation by russia to "demilitarize" and "denazify" Ukraine.

Professor Chekalenko L. D., a well-known Ukrainian professor, in her next professional study, investigated the origin of the concept of denazification. This term comes from the German word "*Entnazifizierung*", it was introduced into international practice after World War II. This term meant a set of measures aimed at cleansing post-war German and Austrian society, culture, press, economy, education, jurisprudence and politics from the influence of Nazi ideology.

V. Putin noted in his public addresses that the purpose of the military operation is "to protect people who have been subjected to abuse and genocide by the Kiev regime for eight years". To this end, russia will strive for the "demilitarization and denazification" of Ukraine. Thus, the russian side accused Ukraine of introducing fascism in its country. This means shifting responsibility for the crimes committed by russia during the war in Ukraine from the aggressor to the victim. A similar means of shifting responsibility to another was widely used by Goebbels during World War II [25].

Russia's invasion into Ukraine is part of a larger ambition to regain influence and challenge the Western-dominated world order. The Kremlin frames its actions as a defensive response to NATO's expansion, appealing to domestic audiences nostalgic for Soviet-era power. However, this justification has been widely dismissed on the international stage, leaving russia increasingly isolated.

The invasion is not only a blatant violation of Ukraine's sovereignty and international law but also signals a broader goal: to rewrite the norms established after the Cold War. The use of its UN Security Council veto to block meaningful resolutions further reveals weaknesses in global institutions.

The russian-Ukrainian war has proven to be a fundamental challenge for global diplomacy, impacting not just the two countries involved but the entire international community. The conflict tests the ability of diplomatic institutions, international alliances, and global governance systems to manage crises in an interconnected world.

The war has deeply tested the cohesion of NATO and the European Union. The EU have shown remarkable solidarity in supporting Ukraine. Military aid, humanitarian assistance, and sanctions against Russia are examples of this united front. NATO's strategic response has involved reinforcing the defense of member states in Eastern Europe while providing military and economic support to Ukraine. This has highlighted the significance of collective defense agreements but has also raised tensions, particularly with russia.

The United States has played a leading role in providing military aid to Ukraine, along with sanctions aimed at crippling russia's economy. However, the division of opinion among NATO members over how to balance support for Ukraine with avoiding direct conflict with russia has added complexity.

China's role is also crucial, as it has largely stayed neutral while maintaining strong economic ties with russia. Beijing has pushed for peace but is reluctant to condemn russian actions outright, given its strategic interests. This neutrality is a significant diplomatic balancing act. India, on the other hand, has used its relationships with both the West and russia to secure favourable trade agreements, prioritizing its own interests. For example, India has maintained its trade relations with russia, abstained from United Nations resolutions condemning

russian actions in Ukraine and continued to engage in trade with russia, including purchasing russian oil.

The imposition of sanctions against russia by the U.S., the EU, and other allies has been a central diplomatic tool aimed at pressuring Moscow to de-escalate. However, these sanctions have far-reaching global consequences, including energy price volatility, supply chain disruptions, and inflation, affecting economies worldwide. Russia's countermeasures and its pivot toward China, India, and other non-Western countries illustrate the complex nature of global economic interdependence [26].

5. The russian-Ukrainian war is no longer a bilateral conflict

Professor Humeniuk B.I. in his study "Russia's war against Ukraine and its impact on regional and global processes" emphasizes that the current crisis of the regional security system due to the full-scale aggression of the russian federation against Ukraine is a unique opportunity for the creators of this system to understand all its shortcomings and take them into account in order to avoid old mistakes during future reforms, because the updated security system should become a reliable protection of the guaranteed, stable existence of the countries of the European continent. Ukraine's heroic, effective resistance to the "second army of the world" seemed to awaken Europe from a dream in which it dreamed that it was possible to come to an agreement with evil, that it could be bought off with a condescending attitude, with pretended respect. Ukraine proved with the blood and lives of its defenders that nothing had changed after World War II, and that evil, barbarism, and savagery could only be eradicated radically — physically, not verbally.

In this context, it is important to emphasize that Ukraine's heroic resistance to the aggressive, full-scale invasion of the russian federation gave rise to a new phenomenal phenomenon in the European security

system — the Armed Forces of Ukraine, while the Ukrainian state itself became a symbol of courage and indomitability, a guarantor of the protection of ancient European values. The renewed post-war system of European security is now impossible to imagine without the multilateral participation of Ukraine in it as its basic element. All this greatly enhances our chances for both European integration progress, the ultimate goal of which is to become a full-fledged member of the EU, and for close cooperation with NATO [27].

According to Doctor of Historical Sciences Hai-Nyzhnyk P. P., the russian-Ukrainian war is no longer a bilateral conflict, but it has clear signs of a general crisis of the world security system, which will lead to global transformations. The beginning of a large-scale transformation of the Eurasian space has been laid, a review of the foundations of the global economy and the world security system has been initiated, the world order will be based on new rules and will acquire a qualitatively new configuration [28].

During the speech of the President of Ukraine on February 17, 2024, at the Munich Security Conference, it was emphasized that Ukraine's resistance, supported by partners, *stopped the destruction of the world order* and 2024 should be the time for the full restoration of a rules-based world order. International connivance with the lack of rule of law in russia after 1991 and Putin's policy of managed poverty have led to the fact that human life is worth nothing for the russian state. One can have different attitudes towards international institutions, but the International Criminal Court's arrest warrant for V. Putin in the case of the abduction and forced deportation of children from Ukraine clearly demonstrates where his career should end. The world has a document that defines the basic rules of coexistence of peoples — this is the UN Charter, which legally enshrines the principles of peaceful coexistence of states, but russia disregards it and pursues a purposeful policy to undermine the entire system of international law and world order [29].

A few months later, on November 23, 2024, President of Ukraine Volodymyr Zelensky, while talking to journalists at the Third International Conference "Grain from Ukraine", emphasized that the G20 Summit in Rio de Janeiro, Brazil, was held with *weak support from Ukraine* and without a clear position from major countries — the USA, Brazil, Asian and African countries. Ukraine is not asking its international partners for anything extraordinary, just reforming the UN Security Council in view of its inefficiency and restoring the rule of international law. All steps proposed by Ukraine to end the war are based on the UN Charter. And the world has a document that defines the basic rules of coexistence of peoples — the UN Charter, which legally enshrines the principles of peaceful coexistence of states, but russia disregards it and pursues a purposeful policy to undermine the entire system of international law and world order [30].

On November 26, 2024, during a working meeting between NATO Secretary General Mark Rutte and Greek Prime Minister Kyriakos Mitsotakis, the Secretary General emphasized that we need *to change the trajectory of the conflict* by providing Ukraine with critical air defense and fulfill the commitments made at the NATO summit in Washington. Separately, the NATO Secretary General emphasized that russia is waging an illegal war in Ukraine and is using North Korean weapons and troops, Iranian drones, and Chinese dual-use goods for its defense industry. All of this is a challenge to global peace and security [31].

6. Just and lasting peace in Ukraine

In such circumstances, the demand for justice and the inevitability of punishment of the aggressor is more relevant than ever. Establishing justice is also one of the points of the peace formula that Ukrainian President Volodymyr Zelensky announced at the G20 summit on November 15, 2022 [32]. Other conditions for ending the war are: radiation and nuclear safety, food and energy security, the release of

all prisoners and deportees, the withdrawal of russian troops and the cessation of the war, justice, the prevention of ecocide, the protection of nature, the prevention of escalation, and the fixing of the end of the war [33]. At the same time, the President stressed that this aggressive russian war must end on the basis of the implementation of the UN Charter and the restoration of the territorial integrity of Ukraine, and any issues related to negotiations on ending the war in Ukraine must be brought to the public stage, and not take place behind the scenes. The world must recognize a special tribunal for the crime of russian aggression against Ukraine and create an international mechanism to compensate for all the damage caused by the war. The aggressor must do everything to restore the justice it has violated.

In October 2022, the Dutch parliament supported a resolution calling for the establishment of a special tribunal in The Hague to bring to justice those responsible for russia's war against Ukraine. Dutch Foreign Minister Wopke Hoekstra said that if there was a need for such an "aggression tribunal", it could be established in The Hague [34].

On February 23, 2023, the vision of the President of Ukraine V. Zelenskyy on the ways to achieve peace in Ukraine was clearly reflected in the UN General Assembly resolution "Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine", which was supported by 141 states of the world [35]. This resolution clearly demonstrated strong support for the importance of restoring a comprehensive, just and lasting peace in Ukraine on the principles enshrined in the UN Charter and within the framework of Volodymyr Zelensky's Ten-Point Peace Formula. At the same time, the resolution renewed its call for russia to immediately withdraw all troops from the territory of Ukraine within its internationally recognized borders and cease hostilities. Another important outcome was that the UN recognized the need to guarantee accountability for crimes committed in accordance with international

law on the territory of Ukraine. Thus, the resolution became an important step towards the further implementation of the Peace Formula of the President of Ukraine V. Zelenskyy for the restoration of peace, territorial integrity and sovereignty of Ukraine, and thus the restoration of justice [36].

The requirement of modernity dictates the creation of an international tribunal for the aggressor in order to save the world from the Third World War. The Head of the Office of the President of Ukraine during the conference "United for Justice" emphasized that there are only two acceptable options that indicate the readiness of the international community to deal a powerful legal blow to specific international criminals — this is the creation of a special tribunal on the basis of an agreement between Ukraine and the UN with the adoption of a corresponding resolution of the UN General Assembly or the formation of a tribunal on the basis of a multilateral open international agreement between the states of the civilized world. The Parliamentary Assembly of the Council of Europe, the NATO Parliamentary Assembly, the OSCE Parliamentary Assembly, and members of the European Parliament hold the same opinion. The need to create a special tribunal is due to the fact that neither the International Court of Justice, nor the International Criminal Court, nor the European Court of Human Rights have the legal ability to hold the highest military-political leadership of the russian federation accountable for the crime of aggression. And war crimes, the crime of genocide, crimes against humanity are the jurisdiction of the International Criminal Court in The Hague. It is worth noting separately that on March 17, 2023, a historic decision was made in The Hague, which is another step towards restoring the principle of justice and the rule of law — the International Criminal Court issued an arrest warrant for V. Putin and the russian President's Plenipotentiary for Children's Rights Maria Lvova-Belova, who officially became

suspects in a war crime, in particular in the deportation of Ukrainian children [24, p. 118].

Thus, russia's war against Ukraine has a significant impact not only on the transformation of the entire system of modern international relations but also test for the international legal order and global diplomacy. Russia's war against Ukraine has influenced the foreign policy and security policy of many countries in the world. It is probably no coincidence that russia's aggression against Ukraine, through which Moscow planned to create a powerful springboard for a future large-scale invasion of Europe, has forced the latter to talk about organizing its own continental army, which should protect against the self-proclaimed "second in the world", and individual European countries — to increase military budgets and reorganize and strengthen their defense potential.

After February 24, 2022, the world is constantly teetering on the brink of another hot world war. German President F.–W. Steinmeier stated on this occasion that russia's war against Ukraine put an end to the idea of a common European home, voiced by the first and last president of the USSR M. Gorbachev, and became the reason for the intensification of the dynamics of geopolitical and geoeconomic changes, and the world is "on the threshold of a new era" and "the consequences of these changes are unpredictable". "We must make our democracies, our economies sustainable, without forgetting our goals— a rules-based world order and a liberal, fair and climate-friendly global economy," he emphasized. And former British Prime Minister Tony Blair warns that the era of Western political and economic dominance is coming to an end due to russia's actions in Ukraine, the strengthening of China as the world's "second superpower", and therefore Western powers need to increase defense spending to maintain their military superiority, while simultaneously expanding their "soft power" by building ties with developing countries.

It is worth noting separately that russia's large-scale aggression against Ukraine on February 24, 2022, led to unprecedented international support for Ukraine and powerful pressure on russia, consolidated the democratic world around the goal of the victory of the Ukrainian people in their heroic struggle against the russian occupiers and the protection of the UN Charter, and accordingly, the principles of international law and legal order [20, p. 13–15].

The professor Volodymyr Horbulin warned in his study "The World Hybrid War: Ukrainian Forefront" back in 2015 that based on the status of the nuclear state, the Russian Federation seeks a global revenge. At the beginning of XXI centuries the model of the world order is being replaced with a model of the world in chaos. European stability and security are possible only by providing a termination of Putin's war against Ukraine and overcoming the consequences of war. Any other option, for example, appeasement on the terms of freezing the conflict, actual recognition of the russian occupation, leaves space for destabilizing the situation in the future in the European region [37, p. 127].

7. Conclusions

The russian war against Ukraine challenges not only the post-World War II world security system, particularly the assumption that large-scale wars between major powers were unlikely but also challenges the international legal order and efficiency of global diplomacy. Russia's invasion into Ukraine, violating the principles of territorial integrity and sovereignty enshrined in international law, raises fundamental questions about the reliability of international norms and institutions meant to prevent such conflicts.

The russian-Ukrainian war is an immense test for global diplomacy, revealing both the strengths and limitations of existing diplomatic frameworks. While international efforts to support Ukraine and

punish russian aggression demonstrate the power of collective action, the conflict has also exposed deep divisions within the international community. The ability of global leaders to balance their own national interests with the broader goal of peace and stability will ultimately determine the course of this war and its long-term impact on international relations.

In the context of the russian-Ukrainian war, it is worth emphasizing that russia has not only violated all principles of international law, which are legally enshrined in the UN Charter, the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations dated 1970, Helsinki Final Act dated 1975 (*the principle of sovereign equality of states; the principle of non-use of force or threat of force; the principle of equality and self-determination of nations and peoples; the principle of peaceful settlement of disputes; the principle of non-interference in the internal affairs of countries; the principle of peaceful cooperation; the principle of conscientious fulfilment of international obligations; the principle of inviolability of borders; the principle of territorial integrity of states; the principle of universal respect for and protection of human rights*), but at the same time is committing *war crimes; crimes against humanity, genocide, and the crime of aggression*.

At the same time, we observe the fact that russia continues the practice of the USSR and uses the veto right to serve its national interests, to defend its foreign policy in contradiction to the rule of international law. Putin's regime is criminal in its essence and challenges both regional and global security. The criminality of Putin's regime is confirmed by facts that meet the criteria of a terrorist state were also defined by international law 39 years ago in the 1987 Geneva Declaration on Terrorism [38; 39]. The European Parliament also supported a resolution on November 23, 2022, recognizing the

russian federation as a state sponsor of terrorism [40]. Therefore, the russian federation must be held accountable for all violations of international law in or against Ukraine, including, aggression, and must bear the legal consequences of all its internationally unlawful actions, including compensation for damage, in order to prevent the outbreak of wars in the future and don't create the precedent to other potential aggressors. The first steps in this direction have already been taken, such as the adoption of the European Parliament Resolution of January 19, 2023 on the establishment of a tribunal for the crime of aggression against Ukraine [41].

The analysis of the above materials / facts and the study of both national and international law allow to confirm the words of NATO's Secretary General, Mark Ruttethat "We need to do everything possible to make sure that Ukraine has what it needs, in terms of training and equipment, to prevail in this fight, which started in February 2022, with the massive and unprovoked onslaught of Russia on Ukraine"[1]. The whole world watches for the lessons from this war which will influence how future crises/wars are addressed, how effective global diplomacy and how works the international legal order. And it remains crucial for the EU to support Ukraine steadfastly, "as long as it takes and whatever it takes" [42].

The international community must pass the test of the effectiveness of global diplomacy and the rule of international law with dignity. Ukrainian partners must ensure a strong position of Ukraine for the approach of a just and lasting peace. As Volodymyr Zelensky noted on December 31, 2024, during the President's New Year's greetings, "Putin cannot win. Ukraine will prevail". Russia's aggression against Ukraine is a serious violation of the principle of justice in international law. Ukraine cannot forget all the crimes that were committed as a result of russia's unprovoked military attack on the sovereign territory of Ukraine [21].

According to the well-known Ukrainian researcher, Professor S. O. Shergin, with whom the author of the study fully agrees, the aggressive war against Ukraine is a fatal mistake of the Putin regime and a terrible crime against humanity, which will forever remain in textbooks on world history and international relations. The myth of russia as a peace-loving state has finally been dispelled, and this will become a bitter reality for its population. The image and international authority of the aggressor state are incompatible with its pre-war status and presence in influential international organizations. The next generation of russians will one way or another have to learn from their own mistakes so as not to be a people incapable of learning the lessons of history. In the historical memory of the Ukrainian people and, perhaps, many other peoples of the post-Soviet space, the war on the territory of Ukraine will remain as a reminder of the terrible phenomenon that changed their lives and fates [43].

References:

1. NATO Secretary General hails US leadership and urges continued support to Ukraine at meeting of Ukraine Defense Contact Group. (2025). The North Atlantic Treaty Organization. Retrieved from https://www.nato.int/cps/en/natohq/news_232053.htm?selectedLocale=en (in English).

2. Strengthening Air Defense and Engaging NATO Countries in Procuring Ukrainian Weapons under the Danish Model: President Meets NATO Secretary General. (2025). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from https://www.president.gov.ua/news/posilennya-ppo-ta-zaluchennya-krayin-nato-do-zakupivli-ukray-95365 (in Ukrainian).

3. Mahda Ye. (2018). Russia's hybrid aggression: lessons for the world. Kyiv: Kalamar. 284 p. (in English).

4. Krupenya I. (2024) The crash of the MH17 aircraft is one of the first visible manifestations of russia's armed aggression against Ukraine. *Consensus*. № 4. P. 191–204. Retrieved from https://konsensus.net.ua/index.php/konsensus/article/view/140 (in English).

5. International Convention for the Suppression of the Financing of Terrorism. (1999). United Nations. Retrieved from https://treaties.un.org/doc/db/terrorism/english-18-11.pdf (in English).

6. The Geneva declaration on terrorism. (1987). UN General Assembly Doc. A/42/307, 29 May 1987, Annex, 1 sheet, Retrieved from https://i-p-o.org/GDT.HTM (in English).

7. IV CONVENTION on the Laws and Customs of War on Land and its Annex: Regulations on the Laws and Customs of War on Land. (1907). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/995_222#Text (in Ukrainian).

8. United Nations Charter. (1945). United Nations. Retrieved from https://www.un.org/en/about-us/un-charter/full-text (in English).

9. Helsinki Final Act. (1975). The Organization for Security and Co-operation in Europe. Retrieved from https://www.osce.org/helsinki-final-act?download=true. (in English).

10. Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations. (1970). Audiovisual Library of International Law. Retrieved from http://legal.un.org/avl/ha/dpilfrcscun/dpilfrcscun.html. (in English).

11. Memorandum on Security Assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapons. (1994). Zakonodavstvo Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/998_158#Text (in Ukrainian).

12. Since the beginning of the aggressive war, Russia has neglected 22 fundamental international documents — Andriy Yermak. (2025). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from https://www.president.gov.ua/news/

vid-pochatku-agresivnoyi-vijni-rosiya-znehtuvala-22-osnovopo-94697(in Ukrainian).

13. Oona, A. (2023). Hathaway How Russia's invasion of Ukraine tested the international legal order. Brookings. Retrieved from https://www.brookings.edu/articles/how-russias-invasion-of-ukraine-tested-the-international-legal-order/ (in English).

14. Comment of the MFA of Ukraine regarding the UNGA resolution "Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine". (2023). The Ministry of Foreign Affairs of Ukraine. Retrieved from https://mfa.gov.ua/en/news/komentar-mzs-ukrayini-shchodo-rezolyuciyi-ga-oon-principi-statutu-oon-shcho-lezhat-v-osnovi-vseohoplyuyuchogo-spravedlivogo-ta-stalogo-miru-v-ukrayini (in English).

15. Sidorenko, S. (2014). General semi-support. Ukrainska pravda. Retrieved from https://www.pravda.com.ua/articles/2014/03/27/7020491/(in Ukrainian).

16. At the initiative of Ukraine, a meeting of the UN Security Council was held on the topic of Russian crimes against Ukrainian prisoners of war and civilians. (2025). Ministerstvo zakordonnykh sprav Ukrainy. Retrieved from https://mfa.gov.ua/news/za-iniciativi-ukrayini-vidbulos-zasidannya-rb-oon-na-temu-rosijskih-zlochiniv-proti-ukrayinskih-vijskovopolonenih-ta-civilnih (in Ukrainian).

17. Vienna Convention on the Law of Treaties. (1986). Verkhovna Rada Ukrainy. https://zakon.rada.gov.ua/laws/show/995_118#Text (in Ukrainian).

18. Constitution of Ukraine. (1996). Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (in Ukrainian).

19. Hunkel E. (2020). Putin signed laws on the priority of the Constitution of the Russian Federation. DW. Retrieved from https://www.dw.com/ru/putin-podpisal-zakony-o-prioritete-konstitucii-nad-mezhdunarodnym-pravom/a-55872285 (in Russian).

20. Vidnianskyi S. V., Martynov A. Yu. (2023). Russia's war against Ukraine and the international community. Kyiv : Parlam. vyd-vo, 336 s. (in Ukrainian).

21. New Year's greetings from the President of Ukraine Volodymyr Zelensky. (2024). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from https://www.president.gov.ua/news/novorichne-privitannya-prezidenta-ukrayini-volodimira-zelens-95297 (in Ukrainian).

22. Commentary of the Ministry of Foreign Affairs of Ukraine on the adoption by the UN General Assembly of the resolution "Territorial integrity of Ukraine: protection of the principles of the UN Charter". (2022). Ministerstvo zakordonnykh sprav Ukrainy. Retrieved from https://mfa.gov.ua/news/komentar-mzs-ukrayini-shchodo-uhvalennya-generalnoyu-asambleyeyu-oon-rezolyuciyi-teritorialna-cilisnist-ukrayini-zahist-principiv-statutu-oon (in Ukrainian).

23. Freedom must always prevail when challenged — speech by the President of Ukraine at the National Defense University of the United States. (2023). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from https://www.president.gov.ua/news/svoboda-povinna-peremagati-zavzhdi-koli-htos-kidaye-yij-vikl-87673 (in Ukrainian).

24. Krupenya, I. M. (2023). The principle of justice and restoration of the supremacy of international law is a requirement of the time and a necessary tool for punishing the aggressor. Konfrontashiia ta spivrobitnytstvo v miznarodnykh vidnosynakh: teotiia i praktyka: zbirnyk naukovykh praz / za zag. red. kand. ist. nauk, doz. S. V. Tolstova; DU «Instytut vsesvitnoi istorii NAN Ukrainy». K. : Detzavna ustanova «Instytut vsesvitnoi istorii NAN Ukrainy», S. 111–120. URL: https://ivinas.gov.ua/images/Confrontation-cooperation-2023.pdf (in Ukrainian).

25. Chekalenko, L. D. (2023). Living in an era of change (on the issue of the future development of Ukraine). *Problemy vsesvitnoi istorii: naukovyi zhurnal*. № 3(23). S. 67–82. (in Ukrainian).

26. Haile Eleonor (2024). The Russian-Ukrainian War: A Test of Global Diplomacy and International Law. Modern Diplomacy. Retrieved from https://moderndiplomacy.eu/2024/12/12/the-russian-ukrainian-war-a-test-of-global-diplomacy-and-international-law/ (in English).

27. Humeniuk, B. I. (2022). Russia's war against Ukraine and its impact on regional and global processes. Naukovyi shchorichnyk «Ukraina dyplomatychna». Vypusk XXIII. S. 18–30. (in Ukrainian).

28. Hai-Nyzhnyk, P. P. (2022). War for life. *Naukovyi shchorichnyk "Ukraina dyplomatychna"*. Vypusk XXIII. S. 31–52. (in Ukrainian).

29. Do not ask Ukraine when the war will end. Ask yourself — why Putin is still able to continue it — speech by President Volodymyr Zelenskyy at the Munich Security Conference. (2024). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from https://www.president.gov.ua/news/ne-pitajte-ukrayinu-koli-zakinchitsya-vijna-pitajte-v-sebe-c-89021 (in Ukrainian).

30. The President: Without a Clear Stance from Major Countries, Agreements with Putin Will Amount to Mere Stalling Tactics. (2024). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from https://www.president.gov.ua/news/prezident-bez-chitkoyi-poziciyi-velikih-krayin-domovlenosti-94653 (in Ukrainian).

31. Press statement by NATO Secretary General Mark Rutte with the Prime Minister of Greece, Kyriakos Mitsotakis. The North Atlantic Treaty Organization. 2024. URL: https://www.nato.int/cps/en/natohq/opinions_230817.htm (in English).

32. Ukraine has always been a leader in peacemaking efforts; if Russia wants to end this war, let it prove it with actions — speech by the President of Ukraine at the G20 Summit. (2022). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from https://www.president.gov.ua/news/ukrayina-zavzhdi-bula-liderom-mirotvorchih-zusil-yaksho-rosi-79141 (in Ukrainian).

33. Philosophy of the Ukrainian Peace Formula. (2023). Prezident Ukrainy. Ofitsiine internet-predstavnytstvo. Retrieved from

https://www.president.gov.ua/storage/j-files-storage/01/19/45/a0284f6fdc92f8e4bd595d4026734bba_1691475944.pdf (in Ukrainian).

34. Deputy Chairman of the Committee on Anti-Corruption Policy Olena Moshenets: A special international tribunal is a necessary tool for establishing justice. (2022). Pres-slyzba Aparatu Verkhovnoi Rady Ukrainy. Retrieved from https://www.rada.gov.ua/news/razom/231610.html (in Ukrainian).

35. Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine. (2023). United Nations. URL: https://digitallibrary.un.org/record/4003921 (in English).

36. Comment of the MFA of Ukraine regarding the UNGA resolution "Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine". (2023). Ministerstvo zakordonnykh sprav Ukrainy. Retrieved from https://mfa.gov.ua/news/komentar-mzs-ukrayini-shchodo-rezolyuciyi-ga-oon-principi-statutu-oon-shcho-lezhat-v-osnovi-vseohoplyuyuchogo-spravedlivogo-ta-stalogo-miru-v-ukrayini (in Ukrainian).

37. Horbulin Volodymyr (2017). The World Hybrid War: Ukrainian Forefront. Kharkiv: Folio. 160 p. (in English).

38. The Geneva declaration on terrorism. UN General Assembly. Doc. A/42/307, 29 May 1987, Annex, 1 sheet, URL: https://i-p-o.org/GDT.HTM (in English).

39. Krupenya I. (2023). State terrorism on example of Putin's regime: present and history. *Przegląd Nauk Historycznych*. Vol. XXII, № 2. URL: https://czasopisma.uni.lodz.pl/pnh/article/view/16927 (in English).

40. European Parliament resolution of 23 November 2022 on the recognition of the Russian Federation as a state sponsor of terrorism (2022/2896(RSP)). (2022). Evropeiskyi parlament. URL: https://ukraine.europarl.europa.eu/cmsdata/260974/1267924UK.pdf (in Ukrainian).

41. European Parliament resolution of 19 January 2023 on the establishment of a tribunal for the crime of aggression against

Ukraine(2022/3017(RSP)). (2022). Evropeiskyi parlament. Retrieved from https://ukraine.europarl.europa.eu/cmsdata/265562/1270878UK.pdf (in Ukrainian).

42. Tony van der Togt (2024). Did Russia's war in Ukraine lead to a European Zeitenwende? Clingendael Spectator. URL: https://spectator.clingendael.org/nl/publicatie/did-russias-war-ukraine-lead-european-zeitenwende (in English).

43. Shergin S.O. (2023). Politychnyi fenomen rosiisko-ukrainskoi viiny. [The political phenomenon of the Russian-Ukrainian war]. *Problemy vsesvitnoi istorii: naukovyi zurnal*. № 3(23). S. 7–17. (in Ukrainian).

Izdevniecība “Baltija Publishing”
Avotu iela 8 k-1-25, Rīga, LV-1011
E-mail: office@baltijapublishing.lv

Iespiests tipogrāfijā SIA “Izdevniecība “Baltija Publishing”
Parakstīts iespiešanai: 2026. gada 24. jūnijs
Tirāža 300 eks.