

UDC 351.86:004.8:614.4

DOI <https://doi.org/10.32782/TNU-2663-6468/2026.4/22>**Shchekhovska L. M.**<https://orcid.org/0000-0002-6119-166X>

National University “Kyiv Aviation Institute”

ADAPTIVE GOVERNANCE OF ARTIFICIAL INTELLIGENCE IN BIOSECURITY

The article examines artificial intelligence as a dual-use technology in the field of biological security and substantiates directions for the adaptive regulation of public administration in this sphere. Its relevance stems from the fact that the integration of AI into biological research is expanding the possibilities of epidemiological monitoring and crisis management while simultaneously generating new categories of risk associated with a lowered threshold of entry for dangerous manipulations of biological agents. For Ukraine, the problem is particularly acute under conditions of war and the course towards European integration, while the current regulatory framework, as of 2026, does not take AI-related risks into account.

It is established that the governance gap is a multi-level phenomenon that manifests differently at the operational, scientific-technological, and institutional levels, requiring a differentiated rather than a uniform response – from procedural adaptation to the formation of accountability mechanisms. An original functional classification of the manifestations of AI's dual nature is proposed, together with a system of criteria for assessing the readiness of international (EU, USA) and national governance systems, which reveals a gap configuration specific to Ukraine – technological readiness outpacing managerial capacity.

The scientific novelty lies in substantiating an original conceptual model of the adaptive governance of AI in biosecurity that integrates the source of risk, the institutional challenge, the adaptation mechanism, and the managerial outcome into a coherent construct. The practical significance lies in identifying directions for integrating AI governance instruments already available in Ukraine into the biosecurity system.

Keywords: artificial intelligence, dual-use technology, biological security, public administration, adaptive governance, institutional gap (governance gap), regulatory sandbox.

Statement of the problem. The rapid development of generative artificial intelligence and its increasingly deep integration into biological research are substantially transforming the traditional understanding of biological security. AI technologies – in particular, large language models, biological design tools, and genomic-data analysis systems – simultaneously open new opportunities for strengthening epidemiological surveillance, laboratory activity, and crisis management, while also giving rise to fundamentally new categories of risk linked to a lowered threshold of entry for manipulating biological agents. In this context, artificial intelligence emerges as a dual-use technology that changes the very nature of biological risk and demands a rethinking of approaches to public administration in this domain.

For Ukraine, the problem is particularly acute. Under conditions of full-scale war and continued

heightened attention to potential CBRN threats, and against the background of the course towards European integration and the harmonisation of legislation with European standards, the capacity of the public administration system to adapt promptly to technological change directly affects national security. At the same time, the current regulatory and legal framework – in particular, the draft Law of Ukraine “On Biological Safety and Biological Protection” and the Biosecurity and Biological Protection Strategy – as of 2026 contains no provisions accounting for risks associated with artificial intelligence. This gap between the pace of technological development and the speed of the rule-making process manifests unevenly across the different levels at which the biosecurity system operates, which calls for a differentiated rather than a unified approach to overcoming it.

Analysis of recent research and publications. The theoretical foundations for governing emerging

technologies under conditions of uncertainty were laid by D. H. Guston, who introduced the concept of anticipatory governance [2], and by A. Klinke and O. Renn, whose adaptive and integrative risk-governance framework underlies the analysis of technological uncertainty applied in this study [17].

The concept of dual-use research of concern (DURC) originates from the 2004 National Research Council report, commonly known as the Fink Report, which recommended the creation of a national oversight body and laid the institutional groundwork for the National Science Advisory Board for Biosecurity [18]. The emergence of generative AI and biological design tools has substantially expanded this research agenda: recent studies by the Centre for the Governance of AI [6], the Center for Strategic and International Studies [7], the Center for AI Safety [9], and the International AI Safety Report [1] examine emerging biosecurity risks associated with large language models and AI systems in biological research.

In Ukraine, the regulatory foundations for AI governance are reflected primarily in the White Paper on Artificial Intelligence Regulation prepared by the Ministry of Digital Transformation [16], which outlines the conceptual basis for a national AI governance framework, though without addressing biosecurity-specific risks.

However, most existing studies address the technological, legal, or security dimensions of AI separately. The transformation of public administration in the context of AI-enabled biosecurity, the challenge of overcoming the governance gap, and the development of an adaptive governance model remain insufficiently explored, particularly in Ukrainian scholarship. Addressing this research gap constitutes the primary objective of the present study.

Task statement. The purpose of the article is to examine the influence of artificial intelligence as a dual-use technology on the biological security system and to substantiate directions for improving public administration mechanisms under conditions of rapid AI development.

Outline of the main material of the study. Understanding artificial intelligence as a dual-use technology in biosecurity is impossible without reference to the research tradition built around the concept of dual-use research of concern in synthetic biology. This concept emerged as a response to the recognition that the same scientific knowledge, methods, and technologies can simultaneously serve socially beneficial purposes and create the potential for harm, depending on the context of application

and the intentions of the actor. Over the past two decades, dual-use research has focused predominantly on classical objects of control – pathogenic microorganisms, toxins, and methods of genetic modification – while risk-management mechanisms have been built largely on list-based screening models oriented towards a limited and predefined list of dangerous agents.

The emergence of artificial intelligence – in particular, large language models, general-purpose foundation models, and specialised biological design tools – substantially changes the nature of the dual-use problem. Unlike traditional dual-use technologies, AI is not a narrowly specialised instrument confined to a specific subject area, but a general-purpose technology capable of simultaneously accelerating legitimate scientific research and lowering the threshold of entry for potentially dangerous manipulations of biological agents. The international expert consensus recorded in the International AI Safety Report 2026, prepared with the participation of researchers from more than thirty countries, confirms that AI capabilities in biological research are developing faster than the governance mechanisms capable of adequately assessing and controlling the associated risks [1].

The consequence of this asymmetry between the speed of AI development and the pace of adaptation of state regulatory mechanisms is the formation of an institutional gap (governance gap) – understood here as the gap between the speed of development of AI technologies and the capacity of the public administration system to adapt, in a timely manner, its mechanisms for assessing, regulating, and monitoring the associated risks. It is precisely this governance gap, rather than individual technological risks, that constitutes the central problem of contemporary public administration in AI-enabled biosecurity. Traditional dual-use risks could be anticipated and regulated through a list of controlled substances or procedures; risks associated with artificial intelligence, by contrast, are characterised by high dynamism, weak predictability, and the capacity for rapid scaling.

Working with this kind of uncertainty requires theoretical approaches in public administration specifically developed for high uncertainty and rapid technological dynamics. The classical theory of risk governance emphasises the need to integrate scientific risk assessment with public communication and decision-making under conditions of incomplete information – an emphasis particularly relevant for technologies whose consequences cannot be exhaustively assessed at the development stage.

A further development of this approach is anticipatory governance, which envisages not a reactive response to already realised risks but the systemic integration of foresight, stakeholder engagement, and adaptation of regulatory mechanisms throughout the technology's development cycle [2]. Related to it is adaptive governance, which emphasises institutions' capacity for continuous adjustment of administrative decisions in response to new information emerging during deployment, rather than only at the stage of initial regulation. For public administration, this implies a shift in regulatory logic: from a reactive model oriented towards responding after a problem arises, to an adaptive model presupposing continuous monitoring of technological change, inter-agency coordination, strategic forecasting, and regular updating of regulatory mechanisms. In such a model, the object of governance becomes not only existing risks but also the capacity of state institutions to adapt promptly to their evolution.

The practical embodiment of these approaches can already be observed internationally. The OECD, in its Framework for Anticipatory Governance of Emerging Technologies (2024), emphasises the need for flexible regulatory instruments, inter-agency coordination, experimental regulation, and strategic forecasting as the basis for governing technologies characterised by high uncertainty [3], confirming the gradual shift of international practice from reactive to anticipatory governance.

Applying these theoretical models to AI-enabled biosecurity nonetheless encounters a significant complication arising from the specific nature of the technologies themselves. Analytical studies show that regulatory approaches developed for general-purpose AI models – such as control over computing power or restrictions on access to training data – do not always transfer correctly to biological design tools, which have a fundamentally different risk architecture and a different nature of potential harm [4]. These features make it possible to integrate the concepts of dual-use, governance gap, and adaptive governance into a single analytical framework for studying AI in biosecurity, within which artificial intelligence is regarded not merely as an object of regulation but as a factor transforming the public administration system itself. Whereas regulation was previously directed mainly at controlling dangerous agents, the central task today is ensuring the adaptability of institutions to continuous technological evolution.

Similar approaches are reflected in current legislative initiatives. The Biosecurity Modernization and Innovation Act (2026) in the United States

envisages strengthening the institutional mechanisms for managing risks associated with new biotechnologies, indicating a shift from traditional control of individual agents towards more adaptive governance models [5].

The analysis conducted thus provides grounds for regarding AI in biosecurity not as a separate area of regulatory policy but as a new sphere of transformation of public administration, in which the effectiveness of the state response is determined less by the stringency of regulatory control than by institutions' capacity for continuous adaptation.

The dual nature of artificial intelligence in biosecurity: a functional analysis. It is appropriate to analyse AI applications in biological security not by separately considering benefits and risks, but through a paired comparison within each administrative function, since such a comparison most fully reveals the essence of a dual-use technology: the same algorithmic capabilities simultaneously expand the state's capacity to counter biological threats and create new vulnerabilities in the system that manages them. This study proposes an original functional classification of the manifestations of AI's dual nature in biosecurity – operational (direct epidemiological monitoring practice), scientific-technological (laboratory and research activity), and institutional (state administration processes). This approach assesses the impact of AI on the state's key biosecurity functions, complementing approaches common in the literature, which typically structure the analysis by risk type or class of AI technology.

At the operational level, the most evident application of AI is support for epidemiological monitoring and early warning. Machine-learning algorithms can analyse large volumes of heterogeneous data – from healthcare-facility visit indicators to transport flows and climate variables – detecting early signals of a possible outbreak long before it becomes evident to traditional surveillance systems. This same capacity for automated analysis, however, gives rise to a new category of administrative risk: forecast reliability depends directly on input-data quality, and algorithmic bias inherent in machine-learning models can systematically distort risk assessment for particular regions or population groups. International expert consensus points directly to a growing gap between the predictive capabilities of AI systems and institutions' capacity to critically evaluate the reliability of such forecasts before relying on them in decision-making [1]. For public administration, this means that introducing algorithmic forecasting requires not only technological integration but also

independent verification procedures preceding any use of results in administrative decisions.

The dual nature of AI is even more pronounced at the scientific-technological level – in laboratory activity and scientific research. Biological design tools built on large language models can substantially accelerate the analysis of genomic data, automate routine laboratory processes, and shorten the time required to develop biomedical solutions, which was previously measured in years. This same acceleration, however, is the source of a new category of risk – the “democratisation of capabilities,” whereby complex biotechnological tasks that previously required a highly qualified research team and substantial resources become accessible to a much wider circle of actors. The documented case of the Boltz-1 biological design model, created by a group of three students in only four months, illustrates how rapidly the threshold of entry for developing complex biological tools is falling with the aid of AI-based coding agents [6]. This acceleration creates a direct challenge for existing control mechanisms: current nucleic-acid synthesis screening systems are built largely on a list-based model of known dangerous sequences, whereas AI-generated variants that do not match any known agent can remain outside the detection range of such systems [7]. Administratively, this implies a need to shift from controlling individual biological agents to regulating the technological processes and tools that enable the creation of new biological constructs.

The balance between potential and risk at this level is not fixed but depends on the development of accompanying institutional infrastructure – legislative initiatives on the standardisation of biological data, for instance, are intended to address the absence of consistent, machine-readable formats, which currently limits the effective application of analytical algorithms [8]. The dual nature of AI in biosecurity is thus determined not solely by the technology itself but also by the quality of accompanying data standards and control mechanisms, which shift the balance in one direction or another.

The institutional level, which has received relatively less scholarly attention than the first two, concerns the application of AI directly within state administration – supporting situation centres, modelling crisis scenarios, and strategic forecasting. Here, AI’s potential lies in integrating disparate sources of information into a single analytical picture, accelerating decision-making under the time constraints characteristic of biological crisis situations. At the same time, integrating algorithmic systems into state administration raises new requirements for the

transparency of the models on which decisions are based and for accountability for the consequences of their application, since the opacity of algorithmic analysis complicates both external oversight of decision quality and the assignment of responsibility in the event of an erroneous forecast. The problem thus lies not only in algorithm quality but in the formation of institutional accountability mechanisms that make it possible to explain, verify, and review algorithmically supported administrative decisions. It is at this level that the technological and administrative dimensions of risk become inseparable: researchers working within the broader framework of catastrophic AI risk combine the risks of incorrect algorithm application in state administration with the risks of malicious use of AI for developing biological weapons within a single category of systemic threats, requiring a unified rather than technologically and administratively separated assessment system [9].

Across the three levels, one observes not only a persistent outpacing of AI’s technological capabilities relative to control mechanisms, but a clear progression in the depth of the administrative response required: procedural adaptation (verification procedures) suffices at the operational level; the scientific-technological level requires a structural reorientation of the object of regulation from individual agents to technological processes; and the institutional level requires fundamentally new mechanisms of accountability for algorithmically supported decisions. This progression provides empirical confirmation of the governance-gap thesis substantiated above, translating it from an abstract theoretical construct into concrete, functionally differentiated administrative challenges – and underscores that the gap should be treated as a multi-level institutional phenomenon rather than a single, undifferentiated one, a distinction that in turn determines the need to construct an adaptive governance model for AI-enabled biosecurity.

Institutional readiness of public administration: a comparative analysis. Assessing public administration systems’ readiness to respond to AI-related biosecurity challenges requires clear criteria that follow directly from the theoretical framework substantiated above. The features listed below operationalise these criteria as concrete, observable indicators of the extent to which a system corresponds to the principles of risk, anticipatory, and adaptive governance. Comparing international practice (the approaches of the EU and OECD, and United States legislative initiatives) with the Ukrainian context according to these indicators makes it possible to

identify, compactly and substantively, the institutional gaps that need to be addressed. Institutional readiness is assessed according to six criteria reflecting the key components of the adaptive governance of AI in biosecurity (Table 1).

Relationship between technological and managerial readiness: EU/OECD – balance, with governance development synchronous with technological readiness; USA – balance with technology in the lead, legislation catching up with rapid sector growth; Ukraine – technology outpacing governance, with a developed digital infrastructure that lacks corresponding managerial mechanisms for its use.

The comparative analysis shows that none of the jurisdictions examined, including the EU and USA, currently has a complete, specialised model for governing AI-related risks specifically in biosecurity, confirming the global rather than purely national character of the governance gap. The comparison nonetheless reveals a specific configuration of gaps in Ukraine. Unlike international partners, where the regulatory gap concerns mainly normative lag against an existing institutional and technological base, Ukraine's gap is more complex: it combines low indicators across almost all assessment criteria – from sector-specific regulation [10; 11] to coordination mechanisms under conditions of war [12; 13] – with a paradoxically high level of digital-infrastructure readiness [14]. This imbalance indicates that the key problem for Ukraine is not so much the development of digital infrastructure as the formation of an adaptive governance system capable of integrating existing technological potential into the mechanisms ensuring biological security. This thesis underlies the conceptual model proposed in the next section.

Conceptual model of the adaptive governance of AI in biosecurity and directions for its implementation. The theoretical substantiation of the relationship between dual-use technologies, the institutional gap, and risk/anticipatory/adaptive governance approaches; the functional progression identified in the depth of managerial adaptation, from procedural to systemic; and the empirically confirmed outpacing of technological readiness over managerial readiness in the Ukrainian context – together provide grounds for an original conceptual construct of the adaptive governance of AI in biosecurity. This study proposes a model of four interrelated elements: the source of risk (artificial intelligence as a dual-use technology), the institutional challenge (the governance gap), the adaptation mechanism (a differentiated managerial response at three functional levels), and the managerial outcome (a resilient AI-enabled biosecurity system). The generalised structure of the model is presented in Figure 1.

The sequence of the model's four components reflects the causal logic of the study: the source of risk forms the institutional challenge, whose resolution is ensured by the adaptation mechanism, which in turn determines the managerial outcome. The model's key distinction from existing theoretical frameworks is that the adaptation mechanism is not a one-off managerial decision but a set of interventions differing in depth, applied simultaneously and in a coordinated manner at the operational, scientific-technological, and institutional levels.

The model's adaptive component is operationalised through a system of institutional mechanisms. Continuous monitoring of AI risks provides the operational component, making it possible to detect new manifestations of dual use before they

Table 1

Matrix for assessing institutional readiness for the adaptive governance of AI in biosecurity

Criterion	EU / OECD	USA	Ukraine	Managerial implications
Sector-specific biosecurity regulation accounting for AI	medium [3]	high [5; 8]	low [10]	without substantive regulation, risk remains legally undefined
Inter-agency coordination mechanism	high [3]	medium [5]	low [12]	fragmented coordination slows response to fast-moving risks
Regulatory sandbox / experimental regulation	medium [3]	medium [5]	absent	without a sandbox, regulation cannot keep pace with innovation
Strategic forecasting (foresight)	high [3]	medium	low [11]	without foresight mechanisms, the state remains in a reactive model
Character of the regulatory model	anticipatory [1; 3]	transitional [5; 8]	reactive	determines the overall type of managerial response to the governance gap
Digital infrastructure for AI integration	developed	developed [8]	developed, but AI integration fragmentary [14]	data availability without analytics is unrealised, not absent, potential

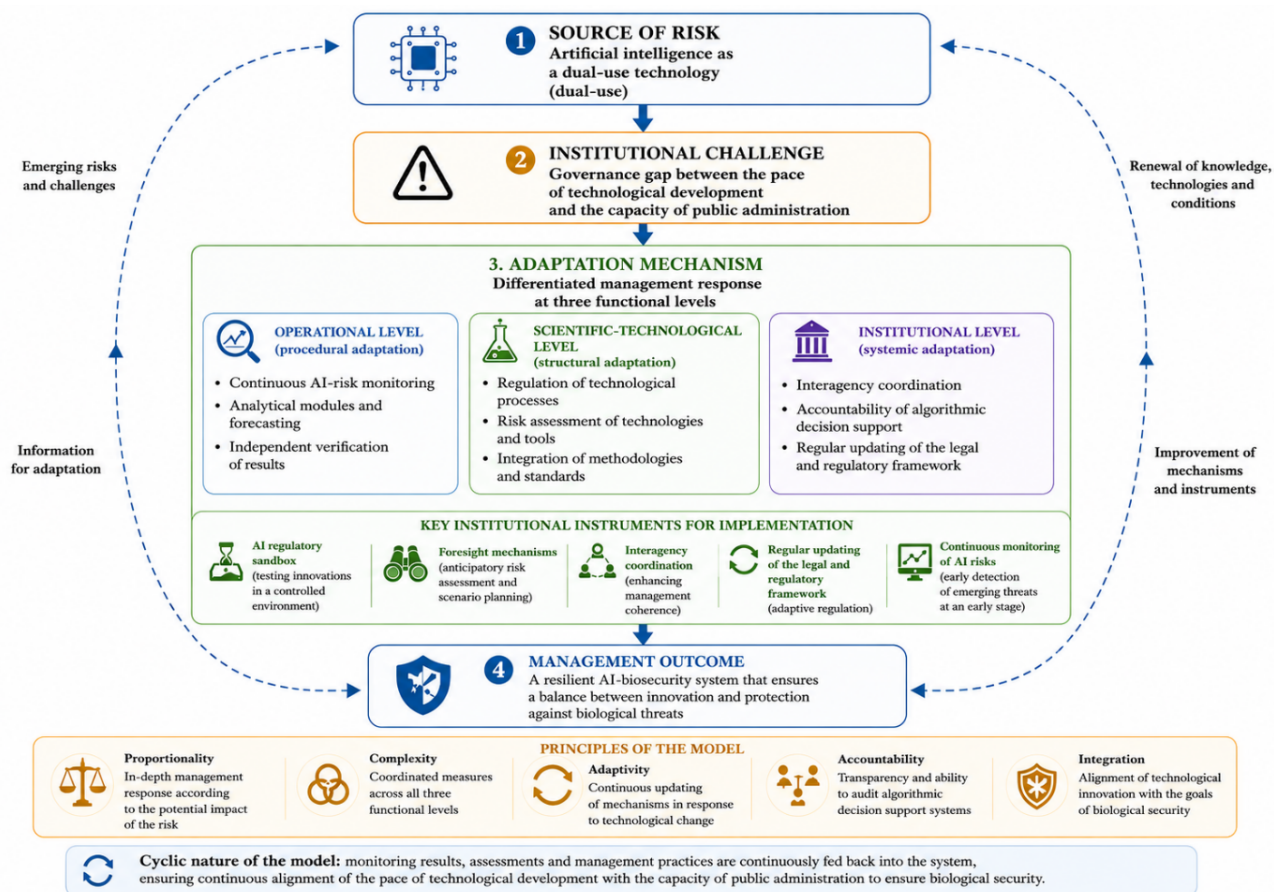


Fig. 1. Original conceptual model of the adaptive governance of AI in biosecurity

scale up; foresight mechanisms operationalise the principle of anticipatory governance; inter-agency coordination eliminates fragmentation; and the regular updating of the regulatory and legal framework turns regulation into a continuous process. Regulatory sandboxes have already become a mandatory element of the European AI governance model: the AI Act requires their establishment in all member states by August 2026 [15], confirming the gradual shift from reactive to experimental regulation of technologies characterised by high uncertainty.

For Ukraine, the central practical thesis is that the country already has AI governance instruments – a general regulatory sandbox, a White Paper on AI regulation, and a specialised committee under the Ministry of Digital Transformation [16] – yet none of them has so far been integrated into the biosecurity system, whose sector-specific legislation is being developed separately and in parallel [10]. This creates a configuration of opportunity distinct from the international one: rather than building the institutional infrastructure of adaptive governance from scratch, Ukraine's primary task is to integrate the general instruments already available into the biosecurity domain.

Directions for practical implementation should accordingly be structured by the same principle of differentiation by level. At the operational level, the priority is to expand the functionality of the existing epidemiological-surveillance infrastructure – in particular, the Electronic Epidemiological Surveillance System (EESS) – with analytical modules, provided that independent verification procedures for results are introduced [14]. At the scientific-technological level, it is necessary to extend the principles of regulating technological processes to sector-specific biosecurity legislation, integrating the risk-assessment methodology already piloted by the Ministry of Digital Transformation [16]. At the institutional level, it is necessary to form a specialised inter-agency coordination structure for AI and biosecurity issues – either by expanding the powers of the existing working group on adapting CBRN standards [12] or as a separate body under the specialised committee on artificial intelligence development.

The proposed concept thus treats adaptive governance not as a separate instrument of state policy but as a multi-level mechanism of institutional adaptation aimed at continuously aligning the

pace of technological development with the public administration system's capacity to ensure biological security.

Conclusions. The study examined artificial intelligence as a dual-use technology in biological security and substantiated directions for improving public administration mechanisms under conditions of its rapid development. The results can be summarised along three lines.

Theoretically, the emergence of AI qualitatively changes the nature of the dual-use problem: unlike traditional dual-use technologies, regulated through list-based control of a limited set of dangerous agents, AI, as a general-purpose technology, forms an institutional gap (governance gap) characterised by high dynamism and weak predictability. This gap is not a homogeneous phenomenon but a multi-level institutional phenomenon that manifests differently at the operational, scientific-technological, and institutional levels of the biosecurity system, requiring a differentiated response – from procedural adaptation to structural reorientation of regulation and, ultimately, to new mechanisms of institutional accountability.

Practically, the comparative analysis of international and national practice showed that overcoming the governance gap remains an unfinished task even for jurisdictions with developed governance systems, such as the EU and USA, confirming the global rather than purely national character of the problem. A specific configuration of institutional gaps was nonetheless identified for Ukraine, whose key feature is technological readiness outpacing managerial readiness: a developed digital infrastructure for collecting biomedical data (the Electronic Healthcare System and the Electronic

Epidemiological Surveillance System) operates without a corresponding analytical layer, and the general AI governance instruments already available – the regulatory sandbox, the White Paper on AI regulation, and the specialised committee under the Ministry of Digital Transformation – remain unintegrated into the biosecurity system. For Ukraine, the priority task is therefore not building institutional infrastructure from scratch but the purposeful integration of already available general mechanisms into the sector-specific domain.

The principal scientific result of the study is an original conceptual model of the adaptive governance of AI in biosecurity that integrates four interrelated elements – the source of risk, the institutional challenge, a level-differentiated adaptation mechanism, and the managerial outcome – into a coherent analytical construct. Unlike existing theoretical approaches that treat adaptive governance as a single, undifferentiated policy instrument, the proposed model reveals it as a multi-level mechanism of institutional adaptation capable of continuously aligning the pace of technological development with the public administration system's capacity to respond to the associated risks.

Prospects for further research include the empirical verification of the proposed model through in-depth analysis of specific cases of implementing adaptive governance mechanisms under Ukrainian conditions, the development of operational indicators for each identified functional level, and the exploration of possibilities for integrating the proposed approach into the broader AI governance system and strategic foresight in Ukraine's national security domain.

Bibliography:

1. International AI Safety Report 2026. 2026. URL: <https://www.internationalaisafetyreport.org> (accessed: 11.07.2026).
2. Guston D. H. Understanding 'anticipatory governance'. *Social Studies of Science*. 2014. Vol. 44, No. 2. P. 218–242. URL: <https://journals.sagepub.com/doi/10.1177/0306312713508669>
3. OECD Framework for Anticipatory Governance of Emerging Technologies. Paris: OECD Publishing, 2024. URL: https://www.oecd.org/en/publications/framework-for-anticipatory-governance-of-emerging-technologies_0248ead5-en.html (accessed: 11.07.2026).
4. Moulange R., Langenkamp M., Alexanian T., Curtis S., Livingston M. Towards Responsible Governance of Biological Design Tools. Workshop on Regulatable Machine Learning at the 37th Conference on Neural Information Processing Systems. 2023. DOI: <https://doi.org/10.48550/arXiv.2311.15936> (accessed: 11.07.2026).
5. Biosecurity Modernization and Innovation Act, S. 3741, 119th Congress (2026). URL: <https://www.congress.gov/bill/119th-congress/senate-bill/3741> (accessed: 11.07.2026).
6. GovAI. Coding agents are changing the biosecurity risk landscape. Centre for the Governance of AI, 2026. URL: <https://www.governance.ai> (accessed: 11.07.2026).
7. CSIS. Opportunities to strengthen U.S. biosecurity from AI-enabled bioterrorism. Center for Strategic and International Studies, 2026. URL: <https://www.csis.org/analysis/opportunities-strengthen-us-biosecurity-ai-enabled-bioterrorism-what-policymakers-should> (accessed: 11.07.2026).

8. AI-Ready Bio-Data Standards Act, H.R. 7907, 119th Congress (2026). URL: <https://www.congress.gov/bill/119th-congress/house-bill/7907/text> (accessed: 11.07.2026).
9. CAIS. AI risks that could lead to catastrophe. Center for AI Safety. URL: <https://safe.ai/ai-risk> (accessed: 11.07.2026).
10. Проект Закону України «Про біологічну безпеку та біологічний захист». № 14091 від 30.09.2025, М-во охорони здоров'я України. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/57476> (accessed: 11.07.2026).
11. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію біобезпеки та біологічного захисту»: Указ Президента України від 17.12.2021 № 668/2021. URL: <https://zakon.rada.gov.ua/laws/show/668/2021#Text> (accessed: 15.07.2026).
12. Відбулося засідання робочої групи з розробки та парламентського нагляду за впровадженням «Національного плану дій» з реагування на CBRN-загрози та відповідних регуляторних механізмів. Прес-служба Апарату Верховної Ради України. 2024. URL: https://www.rada.gov.ua/news/news_kom/245955.html (accessed: 11.07.2026).
13. Аналітичний огляд стану законодавства України щодо реагування на CBRN-загрози. Дослідницька служба Верховної Ради України. URL: https://research.rada.gov.ua/documents/analyticRSMaterialsDocs/nscur_defense/Guide_lg-nb/77679.html (accessed: 11.07.2026).
14. Електронна система епідеміологічного нагляду (ЕСЕН). М-во охорони здоров'я України. URL: <https://moz.gov.ua/uk/news/elektronna-sistema-epidemiologichnogo-naglyadu-esen> (accessed: 11.07.2026).
15. Article 57: AI Regulatory Sandboxes. EU Artificial Intelligence Act. 2026. URL: <https://artificialintelligenceact.eu/article/57/> (accessed: 12.07.2026).
16. Майбутнє регулювання штучного інтелекту в Україні: аналіз Білої книги з регулювання ШІ. Центр Дністрянського. URL: <https://dc.org.ua/news/maybutne-regulyuvannya-shtuchno-go-intelektu-v-ukrayini-analiz-biloyi-knygy-z-regulyuvannya-shi> (accessed: 12.07.2026).
17. Klinke A., Renn O. Adaptive and integrative governance on risk and uncertainty. Journal of Risk Research. 2012. Vol. 15, No. 3. P. 273–292. DOI: 10.1080/13669877.2011.636838 (accessed: 15.07.2026).
18. National Research Council. Biotechnology Research in an Age of Terrorism. Washington, DC: National Academies Press, 2004. DOI: 10.17226/10827 (accessed: 15.07.2026).

Щеховська Л. М. АДАПТИВНЕ ВРЯДУВАННЯ ШТУЧНИМ ІНТЕЛЕКТОМ У СФЕРІ БІОЛОГІЧНОЇ БЕЗПЕКИ

Стаття присвячена дослідженню штучного інтелекту як технології подвійного призначення у сфері біологічної безпеки та обґрунтуванню напрямів адаптивного регулювання у сфері публічного управління. Актуальність зумовлена тим, що інтеграція ШІ в біологічні дослідження розширює можливості епідеміологічного моніторингу й кризового управління, водночас породжуючи нові категорії ризиків, пов'язаних зі зниженням порогу входу для небезпечних маніпуляцій із біологічними агентами. Для України ця проблема набуває особливої гостроти в умовах війни та курсу на євроінтеграцію, тоді як чинна нормативна база станом на 2026 рік не враховує ризиків, пов'язаних із ШІ.

Встановлено, що інституційний розрив (governance gap) є багаторівневим феноменом, який по-різному проявляється на операційному, науково-технологічному та інституційному рівнях, що потребує диференційованої, а не уніфікованої відповіді – від процедурної адаптації до формування механізмів підзвітності. Запропоновано авторську функціональну класифікацію проявів подвійної природи ШІ, а також систему критеріїв оцінювання готовності міжнародних (ЄС, США) і національної систем управління, яка виявила специфічну для України конфігурацію розривів – випередження технологічної готовності над управлінською спроможністю.

Наукова новизна полягає в обґрунтуванні авторської концептуальної моделі адаптивного врядування штучним інтелектом у сфері біобезпеки, яка інтегрує в цілісну конструкцію джерело ризику, інституційний виклик, механізм адаптації та управлінський результат. Практичне значення полягає у визначенні напрямів інтеграції наявних в Україні інструментів врядування ШІ в систему біобезпеки.

Ключові слова: штучний інтелект, технологія подвійного призначення, біологічна безпека, публічне управління, адаптивне врядування, інституційний розрив (governance gap), регуляторна пісочниця.

Дата першого надходження статті до видання: 20.07.2026

Дата прийняття статті до друку після рецензування: 03.08.2026

Дата публікації (оприлюднення) статті: 15.10.2026