

The article examines the theoretical and practical aspects of the use of artificial intelligence technologies in public administration and the risks associated with their application. The potential opportunities for using intelligent information systems to automate certain administrative procedures, process large volumes of data, forecast socio-economic processes, and provide information and analytical support for managerial decision-making are identified. The need to develop mechanisms for the state regulation of the use of artificial intelligence technologies, taking into account the nature and scale of the potential adverse consequences of their application, is substantiated.

The author proposes a systematization of the main risks associated with the use of artificial intelligence technologies in public administration, distinguishing legal, organizational, technological, socio-ethical, and security risks. The feasibility of applying a risk-based approach is substantiated, according to which the nature and intensity of state regulation should be determined with due regard to the field of application of the technology, the degree of its autonomy, the nature of the information being processed, and the potential adverse consequences. The main components of such an approach are identified: identification and assessment of potential risks, organizational coordination, verification of system reliability, monitoring of system performance, and adjustment of regulatory measures. Prospective directions for the development of the legal, organizational, and human resource

УДК 351:004.8:005.334

Старков В., здобувач, КЗВО «Дніпровська академія неперервної освіти»
Дніпропетровської обласної ради»,
м. Дніпро

**Ризики використання технологій
штучного інтелекту в державному
управлінні**

**(Risks Of Using Artificial Intelligence
Technologies In Public Administration)**

framework for the use of artificial intelligence technologies in Ukraine are proposed. It is substantiated that the application of a risk-based approach makes it possible to ensure the proportionality of state intervention and contributes to achieving a balance between the development of technological innovations, ensuring security, and protecting the rights and legitimate interests of citizens.

Keywords: *artificial intelligence, public administration, state regulation, risk-based approach, information technologies, automated systems, e-government, information security, risk assessment, managerial decision-making.*

The rapid development of artificial intelligence technologies and the expanding possibilities for their practical application create new opportunities for improving the system of public administration. The use of intelligent information technologies makes it possible to increase the efficiency of processing large volumes of data, automate certain administrative procedures, improve the provision of public services, and enhance information and analytical support for managerial decision-making. At the same time, the introduction of such technologies is associated with a number of legal, organizational, technological, and social risks, particularly those related to the protection of personal data, information security, the transparency of automated decisions, the potential for discriminatory outcomes, and the determination of responsibility for the results produced through the use of artificial intelligence systems.

The growing use of artificial intelligence technologies raises the issue of developing appropriate approaches to regulating their application. Of particular importance is the need to align the nature of regulatory intervention with the potential threats and possible adverse consequences associated with the use of such technologies. This approach involves taking into account the field in which artificial intelligence systems are used, the degree of their autonomy, the nature of the information being processed, and the potential impact of automated decisions

on the rights and legitimate interests of citizens. This necessitates a balance between promoting technological innovation and establishing legal and organizational safeguards aimed at minimizing potential risks.

For Ukraine, these issues are particularly relevant in view of the development of e-government, the increasing use of digital technologies by public authorities, and the need for further modernization of public administration mechanisms. The prospects for the use of artificial intelligence technologies require the early identification of potential risks associated with their implementation and the development of appropriate approaches to state regulation. In this regard, an important scientific task is to systematize the main risks associated with the application of artificial intelligence technologies in public administration and to identify promising directions for the development of mechanisms for their regulation in Ukraine.

Analysis of Recent Research and Publications. The use of modern information technologies and artificial intelligence is gradually gaining importance in research in the fields of public administration, law, and information technology. The development of e-government, the increasing use of automated information systems, and technologies for processing large volumes of data create the prerequisites for the application of artificial intelligence elements in the activities of public authorities and raise questions concerning the opportunities, limitations, and risks associated with their use.

The theoretical and applied aspects of the digitalization of public administration, the development of e-government, information support for administrative activities, and the improvement of public administration mechanisms have been studied by Ukrainian scholars V. Kuibida, O. Karpenko, V. Namestnik, V. Lipkan, V. Zalizniak, and others [1–4]. Their works address the introduction of information and communication technologies in public administration, the development of e-government, information security, and the modernization of mechanisms for interaction between public authorities and citizens.

A significant contribution to the study of the theoretical foundations and prospects for the development of artificial intelligence has been made by foreign scholars N. Bostrom, E. Brynjolfsson, A. McAfee, K. Bansak, and others [5–7]. Their works examine the technological

and socio-economic consequences of the development of intelligent systems, the prospects for automation, issues related to artificial intelligence safety, and the potential impact of these technologies on society and public institutions.

The development of artificial intelligence technologies is increasingly raising the issue of establishing legal, ethical, and organizational frameworks for their use. Within the international scientific and expert community, growing attention is being paid to the safety of intelligent systems, the protection of personal data, the transparency of automated decision-making, the prevention of discrimination, and the preservation of human control over technological systems. These trends indicate the gradual emergence of prerequisites for developing specific approaches to the regulation of artificial intelligence technologies.

At the same time, an analysis of the existing literature indicates that the use of artificial intelligence technologies directly within the system of public administration remains insufficiently studied. This is particularly true of the systematization of risks that may arise from the use of intelligent and automated systems by public authorities, the identification of possible mechanisms for mitigating such risks, and the substantiation of approaches to the state regulation of these technologies in Ukraine. This highlights the need for further theoretical research into these issues.

Statement of the Research Objective. The purpose of the article is to identify and systematize the main risks associated with the use of artificial intelligence technologies in public administration, as well as to substantiate approaches to the development of mechanisms for the state regulation of their application in Ukraine, taking into account the need to ensure security, protect citizens' rights, and promote technological innovation.

Presentation of the Main Research Material. The development of artificial intelligence technologies and the expanding possibilities for their practical use create the prerequisites for the gradual introduction of such technologies into the system of public administration. The application of intelligent information systems may contribute to the automation of certain administrative procedures, the processing of large volumes of data, the forecasting of socio-economic processes, and the provision of information and analytical support for managerial

decision-making. At the same time, the use of such technologies is associated with legal, organizational, technological, social, and security risks, which highlights the need to develop appropriate mechanisms of state regulation.

State regulation of the development and use of advanced technologies should ensure a balance among the interests of the state, society, and economic actors by combining legal, organizational, economic, and informational instruments of influence. A particular feature of regulating artificial intelligence technologies is the need to strike a balance between promoting technological development and ensuring security and the protection of citizens' rights and legitimate interests. Under these conditions, the application of a risk-based approach appears promising, whereby the nature and intensity of regulatory intervention should be determined with due regard to the nature and scale of the potential adverse consequences arising from the use of the relevant technologies.

Such an approach should be based on the principle of proportionality of regulatory intervention. Its essence lies in ensuring that the scope of regulatory requirements corresponds to the potential risks associated with the field and conditions of use of a particular artificial intelligence system. The use of technologies that do not pose significant threats to security or to the rights and legitimate interests of citizens should not be subject to excessive administrative restrictions. By contrast, the use of systems whose erroneous or uncontrolled operation may result in significant adverse consequences requires additional procedures for verification, oversight, and assessment of the results of their application.

The need for a differentiated approach to the regulation of advanced technologies is also determined by the specific characteristics of artificial intelligence development. Systems used to provide information and analytical support for administrative activities, automate routine operations, or deliver information services may differ significantly in terms of their potential consequences from systems whose outputs directly affect decisions concerning citizens' rights and interests. Accordingly, when determining the nature of state regulation, it is appropriate to take into account the field of application of the technology, the degree of its autonomy, the nature

of the information being processed, the possibility of verifying the results obtained, and the scale of potential adverse consequences.

At the same time, a risk-based approach should not be limited solely to the preliminary identification of potential threats. The effectiveness of its application depends on the capacity of public institutions to identify risks in a timely manner, assess them, monitor the performance of the relevant systems, and adjust the regulatory measures applied. Particular importance should be attached to ensuring the appropriate quality of input data, the possibility of verifying the results of automated information processing, the identification of responsible actors, and the preservation of opportunities for human intervention in the process of making socially significant decisions.

In Ukraine, the development of appropriate mechanisms of state regulation should proceed gradually, taking into account the level of development of information infrastructure, the capacities of public authorities, the state of the regulatory and legal framework, and the prospects for the further introduction of artificial intelligence technologies. At the same time, it is important to avoid both excessive regulatory intervention, which could hinder technological innovation, and insufficient oversight of technologies that may potentially pose threats to citizens' rights, information security, and the proper functioning of the public administration system.

In the author's view, the development of a risk-based approach to the state regulation of the use of artificial intelligence technologies should primarily involve identifying the main groups of potential risks, determining the factors affecting the extent to which they may arise, and selecting appropriate organizational and legal measures for their prevention and mitigation. Such an approach makes it possible to differentiate regulatory intervention according to the nature of potential adverse consequences while simultaneously creating conditions for the further development and use of promising technologies.

In view of the above, a systematization of the main groups of risks associated with the use of artificial intelligence technologies in public administration and possible mechanisms for their mitigation is proposed (Table 1).

Table 1

Main Risks Associated with the Use of Artificial Intelligence Technologies in Public Administration and Possible Mechanisms for Their Mitigation

Risk Group	Main Manifestations	Possible Mitigation Mechanisms
Legal	Violations of citizens' rights and legitimate interests; uncertainty regarding responsibility for the outcomes of automated decisions; insufficient legal and regulatory framework	Legal and regulatory measures; legal review; determination of the responsibility of relevant actors
Organizational	Insufficiently defined powers and responsibilities; lack of coordination among public authorities; inadequate interagency coordination	Clear allocation of powers and responsibilities; organizational support; interagency coordination
Technological	Inadequate quality of input data; difficulties in verifying the outputs of intelligent systems; technical errors and failures	Preliminary testing; technical assessment; verification of the reliability of results; data quality control
Social and ethical	Potential discriminatory effects of automated decisions; violations of the principles of fairness; insufficient transparency in the use of technologies	Compliance with ethical principles; ensuring transparency; maintaining human control over socially significant decision-making
Security-related	Unauthorized access to information; data leakage; external interference with the operation of information systems; cyber threats	Information protection; technical and organizational security measures; monitoring of system performance; state oversight

Source: compiled by the author based on the results of the study.

As evidenced by the data presented in Table 1, the risks associated with the use of artificial intelligence technologies in public administration are complex in nature and cannot be mitigated through the application of a single instrument of state intervention. Each of the proposed groups of risks requires the use of appropriate legal, organizational, technological, and informational measures for their prevention and mitigation.

The proposed systematization makes it possible not only to structure the main threats associated with the application of artificial intelligence technologies, but also to identify promising directions for improving state policy in this field. Particular importance should be attached to the consistency of the measures applied, since effective risk management requires the

timely identification and assessment of risks, the prevention of potential adverse consequences, and the monitoring of the results of the use of the relevant technologies.

In the author's view, the specific characteristics of artificial intelligence technologies make it appropriate to apply a differentiated approach to their state regulation. The nature and scope of regulatory requirements should be determined with due regard to the field of application of the relevant technology, the degree of its autonomy, the nature of the information being processed, the possibility of verifying the results obtained, and the scale of potential adverse consequences. Such an approach makes it possible to ensure the proportionality of state intervention, avoid unjustified administrative restrictions on technologies associated with a low level of potential risk, and, at the same time, strengthen oversight in areas where errors in automated systems may have significant adverse consequences.

A risk-based approach to the use of artificial intelligence technologies should be regarded not only as a means of systematizing potential threats, but also as a principle for developing mechanisms of state regulation that involves aligning the nature of state intervention with the level of potential risk. Its application should ensure a balance between the need to promote technological innovation, security requirements, and the protection of citizens' rights and legitimate interests.

In the author's view, the development of such an approach in Ukraine may be based on the interrelationship of five main components: risk identification and assessment, organizational coordination, verification of system reliability, monitoring of system performance, and adjustment of the regulatory measures applied.

The first component is the identification and assessment of potential risks, which should be carried out prior to the practical application of the relevant technology. Such an assessment should take into account the field of application of the system, the nature of the data used, the degree of process automation, the potential consequences of erroneous decisions, and their impact on citizens' rights and legitimate interests.

The second component is the organizational coordination of the activities of the actors involved in the development, implementation, and use of the relevant technologies. Particular

importance should be attached to clearly defining the powers and responsibilities of public authorities, establishing effective interagency cooperation, and involving research institutions and information technology specialists in addressing the relevant issues.

The third component should be the verification of the reliability of artificial intelligence systems before and during their practical use. This may include testing software solutions, assessing the quality of input data, verifying the reliability of the results obtained, identifying potential errors, and determining whether the systems comply with established technical and legal requirements.

The fourth component is the monitoring of the performance of artificial intelligence systems. Such monitoring makes it possible to identify deviations and undesirable consequences that were not detected during the preliminary assessment, as well as to determine the effectiveness of the measures applied to mitigate risks.

The fifth component is the timely adjustment of regulatory measures in light of the results of the practical use of the relevant technologies. The rapid pace of technological change necessitates the periodic review of legal, organizational, and technical requirements and their adaptation to new conditions.

Thus, a risk-based approach may be regarded as a set of interrelated measures aimed at the timely identification, assessment, and mitigation of potential adverse consequences associated with the use of artificial intelligence technologies. Its application in public administration should contribute to creating conditions for the safe use of new technologies without imposing unjustified restrictions on their further development.

The development of appropriate approaches in Ukraine requires improvements in the legal, regulatory, and organizational framework governing the use of artificial intelligence technologies. At the same time, given the early stage of their introduction into public administration, regulatory mechanisms should be developed gradually, with the possibility of their subsequent refinement in accordance with technological advances and the accumulation of practical experience.

One of the priority tasks is to develop methodological approaches to identifying and assessing potential risks. Such assessments should take into account the field of application of the technology, the nature and volume of the information being processed, the degree of automation of the relevant processes, the possibility of verifying the results, and the scale of potential adverse consequences.

Another important direction is to strengthen the organizational and human resource capacity of public authorities to use advanced information technologies. This involves training appropriate specialists, developing interagency cooperation, engaging research institutions, and creating conditions for the technical and expert assessment of systems intended for use in public administration.

Equally important is the gradual development of a legal and regulatory framework that takes into account the specific characteristics of advanced technologies while ensuring the protection of citizens' rights, information security, and an appropriate level of state oversight. At the same time, regulatory requirements should be sufficiently flexible so as not to create unjustified barriers to technological development.

The further development of mechanisms for the state regulation of the use of artificial intelligence technologies in Ukraine should be based on the principles of proportionality of state intervention, preliminary assessment of potential risks, responsibility of the actors using such technologies, verifiability of the results of automated decisions, and the preservation of appropriate human oversight.

Based on the findings of the study, the author identifies promising directions for the development of a risk-based approach to the state regulation of the use of artificial intelligence technologies in Ukraine, which are systematized in Table 2.

Table 2

Promising Directions for the Development of a Risk-Based Approach to State Regulation of the Use of Artificial Intelligence Technologies in Ukraine

Area for Improvement	Main Content	Priority Measures	Expected Outcome
Development of the legal and regulatory framework	Establishing the legal foundations for the use of artificial intelligence technologies, taking into account the specific features of their application in public administration	Analysis of existing legislation, identification of legal gaps, and preparation of proposals for the legal regulation of the use of advanced technologies	Creation of legal prerequisites for the safe and responsible use of artificial intelligence technologies
Development of approaches to risk assessment	Identification of the main factors and potential adverse consequences associated with the use of artificial intelligence systems	Development of criteria for assessing potential risks, taking into account the field of application, the nature of the data, the degree of automation, and possible consequences	Ensuring differentiated and proportionate state intervention
Strengthening organizational and human resource capacity	Improving coordination among public authorities and developing the necessary professional competencies	Defining powers and responsibilities, developing interagency cooperation, training specialists, and engaging research institutions and experts	Enhancing the preparedness of public authorities for the use and regulation of advanced technologies
Introduction of system verification and performance monitoring	Identification of potential technical errors, undesirable consequences, and deviations in the operation of artificial intelligence systems	Preliminary testing, technical and expert assessment, verification of data quality and system outputs, and monitoring of practical application	Improving the reliability and safety of the use of artificial intelligence systems
Improvement of regulatory measures	Reviewing and adjusting the instruments of state regulation applied in light of technological development and the results of their practical use	Analysis of technology application practices, assessment of the effectiveness of regulatory measures, and periodic refinement of legal and organizational requirements	Increasing the flexibility and effectiveness of state regulation

Source: compiled by the author based on the results of the study.

As demonstrated by the results of the study, the development of a risk-based approach cannot be limited to improving individual legal and regulatory acts or state oversight procedures. Its effectiveness requires the coordinated application of legal, organizational, informational, and technological measures aimed at the timely identification and assessment of potential risks, verification of the reliability of relevant systems, monitoring of the results of their practical use, and adjustment of the regulatory measures applied. The implementation of these directions will create the necessary prerequisites for the safe and effective use of artificial intelligence technologies in public administration.

The study provides grounds for asserting that the development of mechanisms for the state regulation of the use of artificial intelligence technologies in Ukraine should take into account the need for the early identification of possible adverse consequences arising from their application. Under this approach, state intervention should be aimed not only at eliminating the consequences of identified violations, but also at preventing them through the assessment of potential risks and the selection of proportionate regulatory measures.

Conclusions. The study substantiates the feasibility of applying a risk-based approach to the development of mechanisms for the state regulation of the use of artificial intelligence technologies in Ukraine. It is determined that this approach should be based on differentiating the nature and intensity of regulatory intervention depending on the field of application of the relevant technology, the degree of its autonomy, the nature of the information being processed, and the scale of potential adverse consequences. The application of such an approach makes it possible to combine the need to promote technological innovation with ensuring security and protecting the rights and legitimate interests of citizens.

A systematization of the main risks associated with the use of artificial intelligence technologies in public administration is proposed, distinguishing legal, organizational, technological, social and ethical, and security-related risks. For each of these groups, possible measures for their prevention and mitigation are identified, providing a basis for the differentiated selection of state regulatory measures.

The main components of developing a risk-based approach to the state regulation of the use of artificial intelligence technologies are identified: identification and assessment of potential risks, organizational coordination, verification of system reliability, monitoring of system performance, and adjustment of the regulatory measures applied. The need for their coordinated application, taking into account the specific features of the use of relevant technologies in public administration, is substantiated.

Promising directions for the development of a risk-based approach in Ukraine are proposed, including the development of the legal and regulatory framework, the establishment of methodological approaches to assessing potential risks, strengthening the organizational and human resource capacity of public authorities, introducing procedures for system verification and performance monitoring, and periodically adjusting regulatory measures in accordance with technological developments and the results of their practical application.

The practical significance of the results obtained lies in the possibility of applying the proposed approaches in the preparation of legal, regulatory, and organizational decisions concerning the use of artificial intelligence technologies in public administration, the identification of potential risks associated with their application, and the selection of appropriate measures for their prevention and mitigation.

Prospects for further research should be associated with the development of methodological approaches to assessing the risks arising from the use of artificial intelligence technologies, the establishment of criteria for verifying the reliability of automated systems, the study of organizational and legal mechanisms for their application in public administration, and the generalization of international experience in regulating the relevant technologies.

Список використаних джерел:

1. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. Вісник Національної академії державного управління при Президентові України. Серія: Державне управління. 2018. № 1. С. 5–10.

2. Ліпкан В. А., Залізник В. А. Систематизація інформаційного законодавства України : монографія. Київ : ФОП О. С. Ліпкан, 2012. 304 с.
3. Яненко І. Г. Цифрова трансформація промисловості України: ключові акценти. Проблеми економіки. 2017. № 4. С. 179–184.
4. Забейворота Т. Сучасна концепція е-врядування як основа модернізації системи державного управління. Актуальні проблеми державного управління. 2017. № 1 (51). С. 35–42.
5. Bostrom N. Superintelligence: Paths, Dangers, Strategies. Oxford : Oxford University Press, 2014. 352 p.
6. Brynjolfsson E., McAfee A. Machine, Platform, Crowd: Harnessing Our Digital Future. New York : W. W. Norton & Company, 2017. 416 p.
7. Bansak K., Ferwerda J., Hainmueller J., Dillon A., Hangartner D., Lawrence D., Weinstein J. Improving refugee integration through data-driven algorithmic assignment. Science. 2018. Vol. 359, № 6373. P. 325–329. DOI: <https://doi.org/10.1126/science.aao4408>.

References:

1. Kuibida, V. S., Karpenko, O. V., & Namestnik, V. V. (2018). Tsyfrove vriaduvannia v Ukraini: bazovi definitsii poniatiino-katehorialnoho aparatu [Digital governance in Ukraine: basic definitions of the conceptual and categorical apparatus]. Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Seriia: Derzhavne upravlinnia, 1, 5–10.
2. Lipkan, V. A., & Zalizniak, V. A. (2012). Systematyzatsiia informatsiinoho zakonodavstva Ukrainy [Systematization of information legislation of Ukraine]. Kyiv: FOP O. S. Lipkan. 304 p.
3. Yanenkova, I. H. (2017). Tsyfrova transformatsiia promyslovosti Ukrainy: kliuchovi aktsenty [Digital transformation of Ukrainian industry: key aspects]. Problemy ekonomiky, 4, 179–184.
4. Zabeivorota, T. (2017). Suchasna kontseptsiiia e-vriaduvannia yak osnova modernizatsii systemy derzhavnoho upravlinnia [Modern concept of e-governance as a basis for

modernization of the public administration system]. Aktualni problemy derzhavnoho upravlinnia, 1(51), 35–42.

5. Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press. 352 p.

6. Brynjolfsson, E., & McAfee, A. (2017). *Machine, Platform, Crowd: Harnessing Our Digital Future*. New York: W. W. Norton & Company. 416 p.

7. Bansak, K., Ferwerda, J., Hainmueller, J., Dillon, A., Hangartner, D., Lawrence, D., & Weinstein, J. (2018). Improving refugee integration through data-driven algorithmic assignment. *Science*, 359(6373), 325–329. DOI: <https://doi.org/10.1126/science.aao4408>.