**DOI: 10.52363/passa-2026.1-23**
**UDC 351:004.8:004.056**

***Sychenko V.,*** *doctor of science in public administration, professor, rector, CIHE «Dnipro academy of continuing education» Dnipropetrovsk regional council»*
*ORCID: 0000-0001-9655-2317*

***Starkov V.,*** *postgraduate, CIHE «Dnipro academy of continuing education» Dnipropetrovsk regional council»*
*ORCID: 0000-0001-8400-2457*

***Сиченко В.,*** *доктор наук з державного управління, професор, ректор, КЗВО «Дніпровська академія неперервної освіти» Дніпропетровської обласної ради»*

***Старков В.,*** *аспірант, КЗВО «Дніпровська академія неперервної освіти» Дніпропетровської обласної ради»*

# SCIENTIFIC ASPECTS OF ENSURING SECURITY AND TRANSPARENCY OF ARTIFICIAL INTELLIGENCE ALGORITHMS IN THE CONTEXT OF DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION

# НАУКОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ПРОЗОРОСТІ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ

*The article examines the scientific aspects of ensuring security and transparency of artificial intelligence algorithms in the context of digital transformation of public administration. It is substantiated that the implementation of artificial intelligence technologies enhances the efficiency of administrative processes, but at the same time is associated with increasing security risks, including cyber threats, data breaches, algorithmic bias, and lack of transparency in decision-making.*

*The main security threats to AI algorithms are systematized and their multi-level structure is identified. An analytical model for assessing the level of AI implementation in public administration bodies is proposed, along with an algorithmic model for ensuring security and transparency that integrates technical and governance aspects of AI systems.*

***Keywords:*** *artificial intelligence, public administration, digital transformation, digitalization, security, transparency, accountability, algorithmic systems, cybersecurity, trust*

*У статті досліджено наукові аспекти забезпечення безпеки та прозорості алгоритмів штучного інтелекту в умовах цифрової трансформації державного управління. Обґрунтовано, що впровадження технологій штучного інтелекту сприяє підвищенню ефективності управлінських процесів, однак одночасно супроводжується зростанням безпекових ризиків, пов'язаних із кіберзагрозами, витоком даних, алгоритмічною упередженістю та недостатньою прозорістю прийняття рішень.*

*Систематизовано основні загрози безпеці алгоритмів штучного інтелекту та визначено їх багаторівневу структуру. Запропоновано аналітичну модель оцінювання рівня впровадження штучного інтелекту в органах державного управління, а також алгоритмічну модель забезпечення безпеки та прозорості, що інтегрує технічні та управлінські аспекти функціонування алгоритмічних систем.*

***Ключові слова:*** *штучний інтелект, державне управління, цифрова трансформація, цифровізація, безпека, прозорість, підзвітність, алгоритмічні системи, кібербезпека, довіра.*

Problem statement. The current stage of the digital transformation of public administration in Ukraine is characterized by the active introduction of artificial intelligence (AI) technologies into the sphere of public administration, in particular into the processes of managerial decision-making, the analysis of large data sets, the provision of administrative services, and the functioning of e-government. The use of AI algorithms contributes to enhancing the

effectiveness of public administration, optimizing resources, and accelerating administrative procedures.

At the same time, the expanding practice of applying AI in the activities of state authorities brings to the fore the issue of ensuring state security, since algorithmic systems are increasingly being used in spheres of strategic importance, including information security, cyber defense, the defense sector, the management of critical infrastructure, and the processing of personal and sensitive data.

The existing strategic documents and concepts of digital development cover the issues of AI regulation only partially and do not contain clear mechanisms for the control, audit, and certification of the algorithms used by state authorities [1–3]. On the whole, the relevance of the study is determined by the need for the scholarly substantiation of approaches to ensuring the security and transparency of artificial intelligence algorithms under the conditions of the digital transformation of public administration, as well as the formation of an effective regulatory and legal basis for their use with due regard for the challenges of national security.

Analysis of recent research and publications. In examining the problem of applying artificial intelligence in the system of public administration, researchers devote particular attention to the issues of the effectiveness of algorithmic solutions, their legal regulation, ensuring transparency, accountability, and data protection, as well as the minimization of security risks arising in the process of the digital transformation of public authority.

Among the Ukrainian scholars who laid the groundwork for conceptualizing the opportunities and risks of using artificial intelligence in the public sector, mention should be made of V. Vasylenko, V. Furashev, I. Korzh, I. Kostenko, M. Chabanna, V. Marenichenko, O. Donchenko, T. Yarovyi, and V. Paliukh [4–5, 9–12].

Contemporary approaches to the introduction of artificial intelligence in public administration and the directions of its application are outlined in the works of O. Dykan, U. Storozhylova, O. Vasyliev, M. Tretiak, A. H. Diadko, O. Musii, I. Bovsunivska, and others [6, 7].

The analysis of recent research and publications attests to a noticeable growth of interest among Ukrainian scholars in the problem of using artificial intelligence in public administration. At the same time, most contemporary works focus predominantly on the general prospects of digitalization, the legal foundations of introducing AI, or particular applied aspects of its use. By contrast, the issues of the comprehensive assurance of the security and transparency of artificial intelligence algorithms specifically in the context of state security, regulatory certainty, accountability, and trust in algorithmic solutions have not yet received sufficient and systematic coverage, which determines the relevance of further scholarly inquiry.

Statement of the task. The aim of the study is to synthesize scholarly approaches to ensuring the security and transparency of artificial intelligence algorithms in the system of public administration and to determine the key directions for their improvement under the conditions of digital transformation.

Presentation of the main material. The contemporary digital transformation of public administration in Ukraine is accompanied by the active introduction of artificial intelligence technologies, which encompass both internal managerial processes and the interaction of the state with citizens. In particular, algorithmic systems are used for the analysis of big data, the forecasting of socio-economic processes, the automation of administrative services, and the enhancement of the effectiveness of managerial decisions.

At the same time, the introduction of AI in the public sector cannot be regarded solely as a technological process. It is directly connected with the issues of state security, respect for human rights, the transparency of the activities of public authorities, and ensuring the accountability of the decisions taken. In this context, the formation of a comprehensive approach to the regulation and control of algorithmic systems acquires particular significance.

In contemporary scholarly discourse, AI algorithms in the public sector are examined through the prism of three fundamental characteristics that form the basis of trust in digital governance — transparency, security, and accountability (Table 1).

e-ISSN 2786-5533

Table 1

Key characteristics of AI algorithms in public administration

| Characteristic | Substance | Significance for public administration |
|---|---|---|
| Transparency | The intelligibility of the algorithm's operating logic and access to information about decision-making | Ensures the trust of citizens and the possibility of oversight |
| Security | Protection against interference, errors, and data leakage | Guarantees the stable functioning of state systems |
| Accountability | The possibility of establishing responsibility and verifying decisions | Ensures the legitimacy of managerial actions |

The presented characteristics of artificial intelligence algorithms — transparency, security, and accountability — should appropriately be regarded as interconnected and mutually complementary elements of a unified system for ensuring the effective and legitimate functioning of digital public administration.

First and foremost, the transparency of algorithms serves as a fundamental prerequisite for trust in the results of their operation. In the context of public administration, transparency acquires particular significance, since it is directly connected with the realization of the principles of the openness of government provided for, in particular, by the Law of Ukraine "On Information" [1]. At the same time, it should be borne in mind that the full openness of algorithms is not always possible in view of the need to protect state secrets, official information, or personal data, which gives rise to the need to introduce differentiated regimes of access to algorithmic information.

The second key characteristic is the security of artificial intelligence algorithms, which encompasses both technical and organizational-legal aspects. Under contemporary conditions, the security of algorithms extends beyond the classical understanding of cyber defense and includes the issues of the resilience of models to manipulation, protection against attacks on data, and ensuring the integrity of information-processing procedures. In public administration, this characteristic is of particular importance, since algorithmic systems may be used in critically important spheres such as defense, security,

financial control, or infrastructure management. Accordingly, a breach of the security of algorithms may lead not only to technical failures but also to large-scale negative consequences for national security, which is consistent with the provisions of the Law of Ukraine "On the Basic Principles of Ensuring the Cybersecurity of Ukraine" [3].

The third component is the accountability of algorithmic systems, which provides the possibility of establishing responsibility for the results of their functioning. In traditional management models, responsibility is clearly personified, whereas in the case of using AI there arises the problem of distributed responsibility among developers, system operators, and the authorities that employ them. In this context, accountability presupposes not only the existence of legal mechanisms for holding parties responsible but also the creation of procedures for auditing, monitoring, and documenting algorithmic decisions.

The interconnection of transparency, security, and accountability forms the conceptual basis of so-called "trustworthy artificial intelligence," which meets the requirements of contemporary public administration. It is precisely the comprehensive assurance of these characteristics that makes it possible to achieve a balance between the effectiveness of using AI and the guarantees of protecting human rights and state security.

At the same time, in the process of applying AI in public administration, a complex of threats arises that may be of both a technical and a socio-legal nature (Table 2).

Table 2

Principal threats to the security of AI algorithms

| Group of threats | Characteristic | Potential consequences |
|---|---|---|
| Cyber threats | Hacking of systems, interference in algorithms | Disruption of the functioning of state services |
| Data-related threats | Leakage or substitution of data | Violation of citizens' rights, manipulation |
| Algorithmic | Bias of models, training errors | Discriminatory or incorrect decisions |
| Institutional | Absence of control and audit | Decline of trust in the state |

The presented classification of threats to the security of artificial intelligence algorithms makes it possible to provide a systematic characterization of the risks that arise in the process of their use in public administration. It is important to emphasize that the indicated groups of threats are comprehensive in nature and are closely interconnected, forming a multilevel system of challenges to state security.

It is important to stress that the indicated groups of threats do not exist in isolation. For example, cyber threats may lead to the compromise of data, which, in turn, affects the quality of algorithmic decisions. In view of this, ensuring the security of artificial intelligence algorithms in public administration must be carried out on the basis of a comprehensive approach that provides for the simultaneous consideration of technical, legal, and organizational aspects. A particular role in this process is played by the integration of the principles of cybersecurity, data protection, algorithmic fairness, and institutional accountability.

With the aim of summarizing the current state of the introduction of artificial intelligence technologies in the bodies of public administration of Ukraine and assessing the related security and transparency aspects, we have conducted an analytical study based on the synthesis of scholarly publications, regulatory and legal acts, strategic documents in the sphere of digital transformation, and open data on the functioning of state information systems.

In the course of the study, the main directions of the application of artificial intelligence algorithms in the public sector were analyzed, in particular in the spheres of the provision of administrative services, tax administration, law enforcement, social security, cybersecurity, and the administration of justice. The assessment was carried out according to such criteria as the level of technology adoption, the nature of the artificial intelligence tools used, the potential security risks, and the level of transparency of the algorithmic systems.

The results of the analysis conducted are summarized in the form of an analytical model that reflects the current state of the use of artificial intelligence in the bodies of public administration of Ukraine and makes it possible to

identify the key problematic aspects associated with ensuring the security and transparency of algorithms (Table 3).

Table 3

Level of artificial intelligence adoption in the bodies of public administration

| Sphere of application | Level of adoption in Ukraine | Main AI tools | Security risks | Level of transparency |
|---|---|---|---|---|
| Administrative services (ASC, Diia) | Medium | chatbots, automation of application processing | data leakage, algorithm errors | Medium |
| Tax administration | Medium | risk analysis, Big Data | data manipulation | Low |
| Law enforcement | Low–medium | video analytics, recognition | violation of human rights | Low |
| Social sphere | Low | automated decisions on payments | discrimination | Low |
| Cybersecurity | Medium–high | attack detection systems | complexity of control | Low |
| Judicial system | Low | analytics of decisions | risk of bias | Very low |

The analysis of the level of the introduction of artificial intelligence technologies in the bodies of public administration of Ukraine attests to the unevenness of their application depending on the sphere of activity. AI is used most actively in the sphere of administrative services and cybersecurity, which is conditioned by the need to automate processes and to handle significant volumes of information.

At the same time, in such sensitive spheres as law enforcement and the judicial system, the level of AI adoption remains limited, which is associated with the high risks of violating human rights, an insufficient level of regulatory regulation, and the absence of effective control mechanisms.

Particular attention is drawn to the imbalance between the level of technology adoption and the level of its transparency. In most spheres, the transparency of algorithmic systems remains low, which creates the

preconditions for a decline in trust in state institutions and complicates the realization of the principles of accountability.

In addition, the results of the analysis attest to the fact that even in those spheres where the level of AI adoption is relatively high, the issues of security remain insufficiently regulated. This confirms the need to form a comprehensive state policy aimed at ensuring a balance between the effectiveness of using the technologies and the guarantees of security and transparency.

With the aim of systematizing the approaches to ensuring the security and transparency of artificial intelligence algorithms under the conditions of the digital transformation of public administration, it is expedient to use generalized analytical models that make it possible to integrate the technical, legal, and institutional aspects of the functioning of AI.

In this context, we have proposed an adapted model that conditionally reflects the interaction of the key levels of ensuring the reliability of algorithmic systems in the public sector. This model is based on the combination of the technological (algorithmic) and managerial (institutional-legal) dimensions, which makes it possible to comprehensively assess the risks and to determine the directions for their minimization (Table 4).

Table 4

Model for ensuring the security and transparency of AI

| Level of the model | Technological dimension | Managerial dimension | Main risks | Assurance instruments |
|---|---|---|---|---|
| Data | Quality, completeness, representativeness of data | Legal regulation of data processing | Distortion, data leakage | Data protection, audit of sources |
| Algorithms | AI models, decision-making logic | Requirements for transparency and explainability | Bias, the “black box” | Testing |
| Infrastructure | IT systems, computing resources | Organization of cyber defense | Cyberattacks, failures | Cybersecurity, monitoring |

| | | | | |
|---|---|---|---|---|
| Institutions | Interaction of systems and users | Control and supervisory bodies | Absence of responsibility | Regulators, audit |
| Society | Impact of AI outcomes on citizens | Ethical and social norms | Distrust, discrimination | Codes of ethics, transparency |

The technological dimension of the model reflects the internal logic of the functioning of artificial intelligence systems, beginning with the stage of data collection and processing and concluding with the implementation of algorithmic solutions in a specific infrastructure. It is precisely at this level that the principal technical risks are formed, associated with the quality of the data, the reliability of the algorithms, and the resilience of information systems to external influences.

In turn, the managerial dimension encompasses regulatory and legal regulation, institutional control mechanisms, and ethical standards for the use of AI. It determines the framework conditions for the functioning of algorithmic systems and ensures their conformity with the principles of legality, accountability, and the protection of human rights.

The interaction of the indicated dimensions at each level of the model acquires particular significance. For example, even technologically perfect algorithms may create threats in the absence of proper legal regulation or institutional control. At the same time, strict regulatory regulation without corresponding technical implementation does not ensure a real level of security.

The proposed approach has applied significance, since it can be used as a basis for developing state policy in the sphere of artificial intelligence, as well as for conducting audits of algorithmic systems in the public sector. In addition, the model contributes to the formation of a holistic vision of the problem that combines technological innovations with the requirements of state security, transparency, and accountability.

Conclusions. As a result of the study conducted, it has been established that the introduction of artificial intelligence technologies into the system of public administration is an integral component of digital transformation, which

contributes to enhancing the effectiveness of managerial processes, optimizing resources, and improving the quality of public services. At the same time, the use of algorithmic systems is accompanied by a growth in security challenges associated with the risks of cyber threats, data leakage, algorithmic bias, and insufficient transparency in decision-making.

It has been demonstrated that the key characteristics of the reliable functioning of artificial intelligence in the public sector are transparency, security, and accountability, which form the basis of trust in state institutions under the conditions of digitalization. Their interdependent nature has been established, which determines the need for a comprehensive approach to their assurance.

In the course of the study, the principal threats to the security of artificial intelligence algorithms were systematized, and their cumulative nature was demonstrated. This made it possible to determine the need for a multilevel system of protection that takes into account the entire life cycle of algorithmic systems.

The results obtained may expediently be used in the formation of state policy in the sphere of artificial intelligence, the development of regulatory and legal support, and the introduction of procedures for the control and audit of algorithmic solutions in public administration.

The further development of the research is associated with the elaboration of comprehensive mechanisms for the legal regulation of artificial intelligence, the harmonization of national legislation with international standards, and the creation of applied approaches to assessing the security and transparency of algorithmic systems.

**References**

1. Law of Ukraine. (1992, October 2). *On information* (No. 2657-XII). https://zakon.rada.gov.ua/laws/show/2657-12

2. Law of Ukraine. (2010, June 1). *On personal data protection* (No. 2297-VI). https://zakon.rada.gov.ua/laws/show/2297-17

3. Law of Ukraine. (2017, October 5). *On the basic principles of ensuring cybersecurity of Ukraine* (No. 2163-VIII). https://zakon.rada.gov.ua/laws/show/2163-19

4. Vasylenko V. M. (2025). Integration of artificial intelligence systems into public administration: Risks, legal challenges, and security guarantees. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*, 35(2), 574–585. https://doi.org/10.32631/vca.2025.2.82

5. Furashev, V. M., Korzh, I. F. (2025). Artificial intelligence and administrative activity of public authorities: European approach. *Informatsiia i pravo*, 1(52), 51–61. https://doi.org/10.37750/2616-6798.2025.1(52).324667

6. Dykan, O. V., Storozhylova, U. L., Vasyliev, O. L., Tretiak, M. V. (2024). Implementation of artificial intelligence in public administration. *Visnyk ekonomiky transportu i promyslovosti*, 60–71. https://doi.org/10.18664/btie.90.337078

7. Kostenko, I. V. (2025). Artificial intelligence in the system of public administration: Institutional challenges and legal guidelines. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*, 206–212. https://doi.org/10.24144/2307-3322.2025.92.3.27

8. Musii, O. I. (2025). Use of artificial intelligence in public administration: Challenges and prospects. *Analitychno-porivnialne pravoznavstvo*, 392–399. https://doi.org/10.24144/2788-6018.2025.06.2.64

9. Chabanna, M. V. (2025). Use of artificial intelligence in EU public policy. *Empirio*, 2(2), 34–42. https://doi.org/10.18523/3041-1718.2025.2.2.34-42

10. Sychenko, V. V., Marenichenko, V. V., Donchenko, O. S. (2025). Ensuring openness of public administration based on a participatory approach. *Naukovi perspektyvy. Seriia: Derzhavne upravlinnia*, 5(59), 450–463. https://doi.org/10.52058/2708-7530-2025-5(59)-450-463

11. Yarovoi, T. S. (2023). Opportunities and risks of using artificial intelligence in public administration. *Economic Synergy*, 2(8), 36–47. http://dx.doi.org/10.53920/es-2023-2-3

12. Paliukh, V. V., Novak, V. M. (2025). Vulnerabilities of information communications under hybrid threats: Mechanisms of state counteraction. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy*, 2(23), 103–107. https://doi.org/10.52363/2414-5866-2025-2-12

Funding. This research received no external funding.
Use of AI. Artificial intelligence was used solely for the technical editing of the text. The author bears full responsibility for the content of the articl
Acknowledgments. The author declares no acknowledgments.

Received: 12.04.26
Accepted: 28.05.26
Published: 26.06.26