Electronic scientific and practical journal

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

#38(2026)
August '26

WWW.SMART-SCM.ORG
ISSN 2708-3195
DOI.ORG/10.46783/SMART-SCM/2026-38

ISSN 2708-3195
9772708319005

Electronic scientific and practical collection
INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

Electronic scientific and practical publication in economic sciences

Electronic scientifically and practical journal “Intellectualization of logistics and Supply Chain Management” included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): **Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).**

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations)
D3 – Management
D5 – Marketing

ISSN 2708-3195
DOI: https://doi.org/10.46783/smart-scm/2026-38

The electronic magazine is included in the international scientometric databases:
Index Copernicus, Google Scholar

Released 6 times a year

№ 38 (2026)
August 2026

Kyiv - 2026

Founder: Viold Limited Liability Company

The electronic scientific and practical journal is registered in international scientometric data bases, repositories and search engines. The main characteristic of the edition is the index of scientometric data bases, which reflects the importance and effectiveness of scientific publications using indicators such as quotation index, h-index and factor impact (the number of quotations within two years after publishing).

In 2020, the International Center for Periodicals (ISSN International Center, Paris) included the Electronic Scientific and Practical Edition "Intellectualization of logistics and Supply Chain Management" in the international register of periodicals and provided it with a numerical code of international identification: ISSN 2708-3195 (Online).

Recommended for dissemination on the Internet by the Academic Council of the Department of Logistics NAU (No. 7 of February 26, 2020). Released 6 times a year. Editions references are required. The view of the editorial board does not always coincide with that of the authors.

Electronic scientifically and practical journal "Intellectualization of logistics and Supply Chain Management" included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): ***Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).***

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations); D3 – Management; D5 – Marketing

facebook.com/Smart.SCM.org
DOI: https://doi.org/10.46783/smart-scm/2026-38
тел.: (063) 593-30-41
e-mail: support@smart-scm.org
https://smart-scm.org

Contents

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

89-99
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-6

UDC 351.86:004.8
JEL Classification: H56, H83, O33.

Received: 2026-07-12
Accepted: 2026-08-20
Published: 2026-08-30

Dabizha V.V. PhD in Public administration, Associate Professor, Associate Professor of the Department of International Relations and Political Consulting, HEI "Open International University of Human Development "UKRAINE" (Ukraine)

ORCID – 0000-0002-7000-4635
Researcher ID GPX-2585-2022
Scopus author id: – 57218620866
E-Mail: verynchik@ukr.net

Nekriach A.I. Doctor of Political Science, Professor, Professor of the Department of International Relations and Political Consulting, HEI "Open International University of Human Development "UKRAINE" (Ukraine)

ORCID – 0000-0001-5058-4145
Researcher ID JDM-2733-2023
Scopus author id: – 57226269387
E-Mail: anastasian1947@gmail.com

ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF THE SECURITY AND DEFENSE FORCES OF UKRAINE: PUBLIC AND ADMINISTRATIVE ASPECT

Vira Dabizha, Anastasiia Nekriach "Artificial intelligence in the activities of the security and defense forces of Ukraine: public and administrative aspect". *The article examines the use of artificial intelligence in the activities of Ukraine's security and defence forces from the perspective of public administration. It is substantiated that, under conditions of digital transformation, increasing volumes of information, and a more complex security environment, artificial intelligence is becoming not only a technological tool but also an instrument for information and analytical support of management processes in the field of national security and defence. The functional roles of the security forces and defence forces are distinguished, and the specific features of AI application are identified in accordance with the competences and tasks of individual actors. The main areas of artificial intelligence use in the activities of the Armed Forces of Ukraine and other components of the defence forces, the National Guard of Ukraine, the State Border Guard Service of Ukraine, the Security Service of Ukraine, intelligence agencies, the National Police of Ukraine, civil protection forces, and cybersecurity and cyber defence actors are systematised. The information and analytical, monitoring, forecasting, planning, coordination, and management decision-support functions of AI are identified. Particular attention is paid to the potential of artificial intelligence to facilitate interagency interaction, integrate relevant data, develop shared situational awareness, and improve the timeliness of responses to complex threats to national security. The necessity of distinguishing between the output generated by an AI system and a management decision is substantiated. It is argued that artificial intelligence should be*

89-99
v.38 (2026)
https://smart-scm.org

regarded as an intelligent tool for supporting public management decisions, while final decision-making and responsibility for its consequences should remain with the authorised public authority or official. Prospective areas for further integration of artificial intelligence into the public administration system of Ukraine's security and defence forces are identified.

***Keywords**:* artificial intelligence, public administration, security forces, defence forces, security and defence sector, national security, management decisions, interagency interaction, information and analytical support, digital transformation

Віра Дабіжа, Анастасія Некряч «Штучний інтелект у діяльності сил безпеки і оборони України: публічно-управлінський аспект». *У статті досліджено використання штучного інтелекту в діяльності сил безпеки і оборони України з позицій публічного управління. Обґрунтовано, що в умовах цифрової трансформації, зростання обсягів інформації та ускладнення безпекового середовища штучний інтелект набуває значення не лише технологічного засобу, а й інструменту інформаційно-аналітичного забезпечення управлінських процесів у сфері національної безпеки і оборони. Розмежовано функціональне призначення сил безпеки та сил оборони та визначено особливості застосування технологій ШІ відповідно до компетенції і завдань окремих суб'єктів. Систематизовано основні напрями використання штучного інтелекту у діяльності Збройних Сил України та інших складових сил оборони, Національної гвардії України, Державної прикордонної служби України, Служби безпеки України, розвідувальних органів, Національної поліції України, сил цивільного захисту та суб'єктів кібербезпеки і кіберзахисту. Виокремлено інформаційно-аналітичну, моніторингову, прогностичну, планувальну, координаційну функції ШІ та функцію підтримки прийняття управлінських рішень. Особливу увагу приділено потенціалу штучного інтелекту у забезпеченні міжвідомчої взаємодії, інтеграції релевантних даних, формуванні спільної ситуаційної обізнаності та підвищенні оперативності реагування на комплексні загрози національній безпеці. Обґрунтовано необхідність розмежування результату функціонування системи ШІ та управлінського рішення. Доведено, що штучний інтелект доцільно розглядати як інтелектуальний інструмент підтримки публічно-управлінських рішень, тоді як остаточне рішення та відповідальність за його наслідки мають залишатися за уповноваженим суб'єктом. Визначено перспективні напрями подальшої інтеграції ШІ в систему публічного управління силами безпеки і оборони України.*

Ключові слова: штучний інтелект, публічне управління, обороноздатність, сили безпеки і оборони, сектор безпеки і оборони, національна безпека, управлінські рішення, міжвідомча взаємодія, інформаційно-аналітичне забезпечення, цифрова трансформація

Introduction. The development of artificial intelligence is one of the key determinants of the contemporary digital transformation of public administration systems and, at the same time, has a significant impact on the nature of national security and defence provision. The ability of artificial intelligence systems to process large volumes of heterogeneous data, identify patterns, detect potential threats, model possible scenarios, and provide information and analytical support for decision-making creates new opportunities for the activities of security and defence sector actors. Accordingly, artificial intelligence is gradually becoming not only a technological tool but also an important element of modern management processes in the security and defence domain.

For Ukraine, these processes are of particular importance in the context of the full-scale armed aggression of the Russian Federation, the hybrid nature of contemporary threats, the highly dynamic

security environment, and the need to make management decisions under severe time constraints and considerable information uncertainty. Modern confrontation takes place simultaneously across military, information, cyber, technological, and other domains, which significantly increases the volume of information requiring analysis and complicates the processes of forecasting, planning, and coordinating the activities of relevant public institutions.

Under these conditions, the use of artificial intelligence technologies is becoming one of the factors enhancing the capacity of the security and defence forces to detect threats in a timely manner, assess risks, analyse changes in the operational environment, and provide information support for management decision-making. The potential of AI can be realised in intelligence and analytical activities, situational awareness, cybersecurity, state border protection, critical infrastructure protection, logistics, threat forecasting, the operation of unmanned systems, information security, and other areas of activity of the security and defence forces.

At the same time, the use of artificial intelligence in this field should not be limited exclusively to the introduction of individual technological solutions. From the perspective of public administration, the integration of AI capabilities into the system of management relations is of fundamental importance. Such a system encompasses the delineation of actors' competences, the organisation of information exchange, interagency interaction, coordination of activities, formulation of management decisions, monitoring of their implementation, and evaluation of their effectiveness.

Another specific feature of the issue is that the security forces and defence forces, while constituting components of Ukraine's security and defence sector, have different functional purposes. However, under contemporary conditions, addressing a significant proportion of security challenges requires their systematic interaction. Threats to national security are increasingly complex in nature and are not confined to the area of responsibility of a single public authority. This necessitates interagency data exchange, interoperability of information systems, harmonisation of analytical procedures, and the establishment of a shared information environment.

It is in this context that artificial intelligence can be regarded as an instrument for strengthening both horizontal and vertical interaction among security and defence sector actors. The integration of data from various sources, their automated analysis, and the timely provision of relevant information to the appropriate levels of management can reduce the time between threat detection and decision-making, enhance situational awareness, and enable a more informed allocation of forces and resources.

At the same time, the proliferation of AI is transforming the traditional mechanism of management decision-making. In the classical management model, the decision-maker receives information, analyses it, identifies alternatives, and makes a decision. The application of artificial intelligence, however, introduces an additional information and analytical layer between the acquisition of primary data and the formulation of a management decision. Algorithmic systems can preprocess information, identify hidden patterns, assess risks, forecast possible scenarios, and generate recommendations for an authorised official.

This provides grounds for considering AI as an intelligent tool for supporting public management decisions in the security and defence domain rather than as an independent decision-making actor. The final decision, particularly where it may entail legal, security-related, or other socially significant consequences, should remain within the competence and responsibility of the authorised actor. Based on the above, the technological advantages of AI must be

combined with the fundamental principles of public administration, namely legality, accountability, responsibility, and the controllability of management activities.

A relevant scientific task is therefore to conduct a comprehensive study of the use of artificial intelligence in the activities of Ukraine's security and defence forces specifically from the perspective of public administration. This requires identifying the system of actors involved in such use, systematising the main areas of AI application, determining its role in the performance of management functions, examining the potential of intelligent technologies for interagency coordination, and substantiating their impact on the mechanisms for preparing, making, and implementing management decisions in the field of national security and defence.

Analysis of recent research and publications. The issue of the use of artificial intelligence in the field of national security and defence has received increasing attention in recent years in both Ukrainian and international academic research. Scholars primarily focus on the practical applications of AI technologies, their use in the military domain, ensuring state security and cybersecurity, the automation of specific processes, threat forecasting, and decision-making support.

S. Hurzhii examines the role and significance of artificial intelligence technologies in the military-technical sphere, analyses global trends in their application, the specific features of AI use by armed forces, as well as the associated risks and threats. The research conducted by S. Bielai, V. Hladkov, O. Pivnenko, D. Pokhodenko, and M. Skliar is also important for the issues under consideration, as the authors substantiate conceptual directions for the implementation of artificial intelligence to meet the needs of Ukraine's security and defence sector. The researchers propose an approach to establishing nationwide, departmental, and interagency artificial intelligence platforms and emphasise the need for cooperation among the defence forces, public institutions, the academic community, and civilian technology developers.

In turn, Yu. Danyk, A. Dykyi, V. Shestakov, and R. Shyrshov provide a comprehensive analysis of the possibilities for the implementation and use of artificial intelligence to meet the needs of Ukraine's security and defence sector. The authors examine the application of AI in cybersecurity, critical infrastructure protection, information operations, and other areas of national security. Particular attention is paid to the need to establish an effective system for managing AI implementation processes, ensuring the safety of its use, managing risks, training personnel, and applying human-machine models.

V. Hmyria, V. Korniienko, and M. Styshuk examine the organisational and legal foundations for the use of artificial intelligence in the field of state security, including law enforcement activities. In their research, they focus on the legislative framework governing the use of AI, issues of responsibility, personal data protection, cybersecurity, and compliance with ethical principles in the application of relevant technologies.

Thus, existing academic research provides a sufficient theoretical foundation for identifying the technological, military, security, organisational, and legal aspects of artificial intelligence use. At the same time, the application of AI specifically from the perspective of public administration of Ukraine's security and defence forces remains insufficiently systematised. In particular, further research is required into the system of actors involved in the use of AI, its management functions, the possibilities for ensuring interagency information and analytical interaction, and the impact of AI technologies on the processes of preparing, making, and implementing management decisions in the field of national security and defence.

The formulation of the goals of the article. The purpose of the article is to provide a theoretical substantiation of the public administration principles governing the use of artificial intelligence in the activities of Ukraine's security and defence forces, to determine its functional role within the national security system, and to reveal the potential of AI as a tool for information and analytical support, interagency coordination, and enhancing the soundness of management decision-making.

Presentation of the main results. The study of the use of artificial intelligence in the activities of the security and defence forces requires, first and foremost, determining the place of the relevant actors within the overall system of ensuring Ukraine's national security. This approach is of fundamental methodological importance, since the concepts of the "security and defence sector", "security forces", and "defence forces" are not identical, and treating them as equivalent complicates the identification of management functions and areas of application of AI technologies [13].

According to the Law of Ukraine "On National Security of Ukraine", the security and defence sector constitutes a system comprising public authorities, the Armed Forces of Ukraine, other military formations, law enforcement and intelligence agencies, state bodies of special purpose with law enforcement functions, civil protection forces, the defence-industrial complex, and other entities defined by law whose activities are aimed at protecting Ukraine's national interests from threats [13].

According to the legislation, the structure of the sector comprises four interconnected components: the security forces; the defence forces; the defence-industrial complex; and citizens and public associations that voluntarily participate in ensuring national security. Therefore, the security forces and defence forces should not be regarded as synonymous concepts but rather as functionally distinct yet interconnected components of a unified national security system.

Under the legislation, the security forces are defined as law enforcement and intelligence agencies, state bodies of special purpose with law enforcement functions, civil protection forces, and other bodies entrusted with functions related to ensuring national security. The defence forces comprise the Armed Forces of Ukraine, other military formations, law enforcement and intelligence agencies, and state bodies of special purpose with law enforcement functions that are entrusted with functions related to ensuring the defence of the state [14].

Such a regulatory distinction indicates that whether a particular actor belongs to the security forces or the defence forces is determined not only by its institutional status but primarily by the nature of the functions it performs. Moreover, certain actors may perform tasks both within the security forces and as part of the defence forces, depending on the applicable legal regime, the nature of threats, and the tasks assigned to them. A notable example is the National Guard of Ukraine, which in peacetime forms part of the security forces and performs law enforcement functions, while simultaneously developing the capabilities required to perform tasks as part of the defence forces.

From the perspective of public administration, this specific feature is directly relevant to determining the model for the use of artificial intelligence. AI does not operate independently of the competence of the respective public authority. The areas of its application should be determined by the functional purpose of the respective actor, the nature of the tasks assigned to it, the type of information being processed, the level of the management decision, and the potential consequences of such a decision [15].

In this regard, it is appropriate to distinguish between the institutional and functional dimensions of artificial intelligence application. The institutional dimension characterises the range of bodies and

structures that use, implement, coordinate, or support the functioning of AI systems. The functional dimension reflects the specific management tasks for which the relevant technologies are applied, including monitoring, analysis, forecasting, planning, coordination, resource allocation, information support, and decision-making support [3].

It is the functional approach that makes it possible to explain why the same artificial intelligence technology may serve different management purposes. For example, computer vision technologies may be used by the defence forces to analyse the operational environment and recognise objects, by border guard units to monitor the state border, by law enforcement agencies to perform security tasks defined by law, and by civil protection actors to assess the consequences of emergencies. The technological basis may be similar; however, the management purpose, legal regime governing data, level of risk, and responsibility of the respective actors differ significantly [1].

In this context, the concept of the management function of AI becomes particularly important. This does not imply granting artificial intelligence any public authority or decision-making powers; rather, it involves identifying those stages of the management process at which AI technologies can enhance the speed, completeness, and soundness of the activities of public administration actors [6].

In our view, six main functional areas of AI use can be distinguished in the activities of the security and defence forces:

1. information and analytical – automated processing of large volumes of structured and unstructured data, their systematisation, identification of interrelationships, and generation of analytical information;

2. monitoring – continuous observation of changes in the security environment, information and cyberspace, as well as the condition of individual facilities and systems;

3. forecasting – identification of trends, risk assessment, forecasting of potential threats, and modelling of possible scenarios for the development of a situation;

4. planning – information support for strategic, operational, and resource planning, identification of alternative courses of action, and assessment of their potential consequences;

5. coordination – facilitating the rapid exchange of relevant information among actors, harmonising data from different sources, and creating a shared information environment;

6. management decision-making support – generating analytical assessments, forecasts, and possible alternatives for subsequent decision-making by the authorised actor.

This classification demonstrates that, from the perspective of public administration, the greatest potential of AI lies not in replacing humans in the management process, but in reducing the time between receiving primary information and formulating a well-founded decision [2]. This is particularly important in the field of national security and defence, where time itself often constitutes an independent factor in management effectiveness.

At the same time, it should be taken into account that the application of artificial intelligence changes the traditional configuration of information flows. Under the classical model, information sequentially passes through individual organisational levels, units, and officials, at each of which it is summarised, analysed, and transmitted to the next level [9]. Where a large number of actors are involved, such a model may lead to duplication of information, delays in its transmission, and institutional fragmentation.

The use of AI technologies potentially enables a transition towards an integrated model in which data from different sources are combined within a shared information

89-99
v.38 (2026)
https://smart-scm.org

and analytical environment, processed automatically, and provided to the relevant management actor in accordance with its competence [10]. Within such a model, AI does not function as an independent management centre but rather as a technological element that facilitates information exchange between different stages of the management cycle.

Therefore, interagency coordination becomes critically important. Contemporary threats to national security are characterised by their interconnected nature and their ability to manifest simultaneously across military, information, cyber, economic, and social domains. Accordingly, the effectiveness of responses increasingly depends on the capacity of public institutions not only to collect their own data but also to promptly integrate them with information obtained from other actors, develop a shared understanding of the security environment, and coordinate management actions.

In this context, artificial intelligence can serve as an integrative element within the information and analytical framework of interagency interaction, facilitating the processing of heterogeneous data and their transformation into information suitable for use at the relevant level of management. However, establishing such an integrated framework requires not only the technological interoperability of systems but also a clear delineation of powers, rules governing access to information, responsibility for data quality, procedures for data exchange, and appropriate oversight mechanisms [12].

The public administration approach to the use of artificial intelligence in the activities of the security and defence forces therefore requires AI to be considered not as an isolated technology but as an integral component of the management cycle, embedded within a system of actors, functions, information flows, and interagency interaction.

Table 1. Functional Areas of Artificial Intelligence Use in the Activities of Ukraine's Security and Defence Forces

Subjects / Functional Area	Prospective Areas of AI Use	Management Functions	Expected Management Effect
Armed Forces of Ukraine and other components of the Defence Forces	analysis of the operational environment; processing of intelligence data; computer vision; unmanned and robotic systems; forecasting; logistics	analysis; forecasting; planning; organisation; decision-making support	enhanced situational awareness; reduced information processing time; resource optimisation; increased timeliness of decision-making
National Guard of Ukraine	analysis of the security environment; monitoring; protection of designated facilities; use of unmanned systems; data analysis while performing tasks as part of the Defence Forces	monitoring; analysis; forecasting; coordination; decision-making support	integration of security and defence capabilities; more rapid response; improved coordination efficiency
State Border Guard Service of Ukraine	intelligent monitoring of the state border; analysis of photo and video data; anomaly detection; risk forecasting; unmanned monitoring	monitoring; risk identification; forecasting; control	enhanced effectiveness of border control; early detection of threats; optimisation of the use of forces and resources
Security Service of Ukraine and intelligence agencies	analysis of large datasets; identification of relationships and patterns; threat analysis; information-analytical and counterintelligence support	analysis; forecasting; risk assessment; information support for decision-making	early detection of threats; improved quality of analytical information; enhanced forecasting capacity
National Police of Ukraine	intelligent data analytics; analysis of information resources as provided by law; support for situational analysis; risk identification	monitoring; analysis; forecasting; organisation of response measures	faster response; more efficient use of resources; enhanced situational awareness

89-99
v.38 (2026)
https://smart-scm.org

State Emergency Service of Ukraine and civil protection forces	forecasting of emergencies; analysis of the consequences of destruction; monitoring of hazardous areas; analysis of geospatial information; resource planning	forecasting; planning; coordination; control	early identification of risks; optimisation of response measures; increased effectiveness of rescue operations
Cybersecurity and cyber defence actors	automated anomaly detection; cyber threat analysis; forecasting of cyberattacks; detection of malicious activity	monitoring; analysis; forecasting; prevention	faster detection of cyber incidents; enhanced cyber resilience; reduced response time
Strategic and interagency governance bodies	data integration; scenario modelling; strategic forecasting; assessment of complex risks	strategic analysis; planning; coordination; control	development of a comprehensive picture of the security environment; enhanced evidence-based strategic decision-making

Source: systematised by the author.

The systematisation presented in Table 1 provides grounds for asserting that the use of artificial intelligence in the activities of the security and defence forces is characterised by a cross-sectoral and interagency nature. Despite differences in the competences of the respective actors, a common management logic of AI application can be identified, encompassing data acquisition and processing, detection of potential threats, risk assessment, forecasting of situational developments, formulation of alternative scenarios, and provision of information support for management decision-making.

At the same time, the most significant differences between the use of AI by the security forces and the defence forces are manifested not so much at the level of the technologies themselves as in the objectives of their application and the nature of management tasks. For the defence forces, the primary focus is on the use of AI technologies to ensure national defence, enhance situational awareness, support planning, intelligence, logistics, and military management decision-making. For the security forces, priority areas include threat detection and prevention, state border protection, ensuring state and public security, cybersecurity, civil protection, and critical infrastructure protection [11].

At the same time, the contemporary nature of threats is gradually reducing the possibility of a clear organisational separation between these areas of activity. A cyberattack on critical infrastructure, an information operation, sabotage activities, or a combined attack may simultaneously require the involvement of actors with different competences [4]. Consequently, the effectiveness of AI application depends not only on the technological capabilities of an individual authority but also on the state's capacity to ensure effective interagency information exchange and interaction.

On this basis, it is proposed to distinguish three levels of artificial intelligence use within the public administration system of security and defence.

The first is the institutional level, at which AI technologies are used by an individual actor in accordance with its competence and functional purpose. At this level, internal processes of information collection, processing and analysis, forecasting, and planning are automated and enhanced through intelligent technologies.

The second is the interagency level, at which AI facilitates the analytical integration of information generated by different actors within the security and defence forces. Its purpose is to overcome institutional fragmentation of information, develop shared situational awareness, and provide information and analytical support for coordinated responses to complex threats.

The third is the strategic level, at which the results of intelligent analysis are used to assess threats to national security, conduct scenario-based forecasting, support strategic

89-99
v.38 (2026)
https://smart-scm.org

planning, determine state priorities, and assist decision-making by the highest public authorities in the field of national security and defence

The proposed three-level approach makes it possible to consider AI not as a set of isolated technological solutions applied by different public authorities, but as a potential element of an integrated information and analytical management framework in the field of security and defence.

One of the key challenges of public administration in the field of national security is the need to coordinate a significant number of institutions, each of which generates its own information resources, exercises powers defined by law, and uses respective departmental systems. Under such conditions, the mere availability of large volumes of data does not guarantee an improvement in the quality of governance [5]. Of crucial importance is the capacity to transform heterogeneous data into relevant information in a timely manner and to ensure its use by the actor authorised to make the respective decision.

The traditional model of interagency interaction is largely based on the sequential transmission of information between authorities and levels of management. Under crisis conditions, such a model may result in time delays, duplication of analytical work, and the formation of different assessments of the same security situation [7]. Artificial intelligence technologies potentially make it possible to transform this approach through the automated integration, structuring, and analysis of information from various sources [8].

From the perspective of public administration, the result of such a transformation should not be the centralisation of all information within a single authority, but rather the establishment of an integrated information and analytical framework in which each actor retains its legally defined competence, while technological interaction ensures the necessary level of data exchange and shared situational awareness.

Accordingly, the functioning of such a framework can be represented by the following sequence: data sources → departmental information systems → integration of relevant data → intelligent processing → threat detection → risk assessment → scenario forecasting → identification of competent actors → management decision support → interagency coordination → response → evaluation of results

A fundamental feature of the proposed approach is that artificial intelligence is positioned within the information and analytical, rather than the authoritative decision-making, segment of the system. AI may perform analysis and forecasting, rank risks, and generate alternatives; however, it does not acquire the status of a public administration actor and does not substitute for the competence of a public authority or an authorised official.

The public administration value of artificial intelligence lies not only in its ability to process information more rapidly. Of considerably greater importance is its potential to transform interaction among security and defence forces from a predominantly departmental model of information support towards an integrated model of situational awareness, coordination, and management decision support.

The analysis demonstrates that the public administration potential of artificial intelligence in the activities of Ukraine's security and defence forces is determined not only by the technological possibilities of its application but, above all, by its capacity to be integrated into management processes, provide information and analytical support, enhance situational awareness, and facilitate interagency coordination. At the same time, the use of AI technologies does not alter the subjectivity of public administration: management decision-making and responsibility for its consequences must

remain with the respective public authority or authorised official. Therefore, AI should be regarded as a tool for enhancing analytical capacity and management effectiveness in the field of security and defence rather than as a substitute for the actor exercising management functions.

Conclusions.

The study has demonstrated that the use of artificial intelligence in the activities of Ukraine's security and defence forces should be considered not only as a direction of technological development but also as an important component of the transformation of public administration in the field of national security and defence. AI has the potential to enhance the information and analytical capabilities of public administration actors, accelerate data processing, threat detection and risk assessment, as well as support forecasting and management decision-making.

The main management functions of artificial intelligence in the activities of the security and defence forces have been systematised, including information and analytical, monitoring, forecasting, planning, coordination, and management decision-support functions. It has been established that specific areas of AI application are determined by the functional purpose, competence, and nature of the tasks performed by the respective actor.

The use of AI is of particular importance in ensuring interagency interaction between the security and defence forces. The integration and intelligent analysis of relevant data can contribute to the development of shared situational awareness, reduce information fragmentation, and improve the timeliness of coordination and response to complex threats to national security.

Artificial intelligence should be regarded as an intelligent tool for supporting public management decisions rather than as an independent management actor. The final decision and responsibility for its consequences should remain with the authorised public authority or official. Prospects for further research are associated with the development of an organisational and functional mechanism for integrating AI technologies into the public administration system of Ukraine's security and defence forces, as well as with improving mechanisms for interagency information and analytical interaction.

References

1. Boulanin, V., Saalman, L., Topychkanov, P., Su, F., & Peldán Carlsson, M. (2020). Artificial intelligence, strategic stability and nuclear risk. Stockholm International Peace Research Institute. Retrieved from: https://www.sipri.org/publications/2020/policy-reports/artificial-intelligence-strategic-stability-and-nuclear-risk

2. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. Retrieved from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

3. Korniienko, V., Hmyria, V., & Styshuk, M. (2025). Organizational and legal principles of use of artificial intelligence in the field of state security. Honor and Law, 1(92), 59–69. DOI: https://doi.org/10.33405/2078-7480/2025/1/92/332039. Retrieved from: https://chiz.nangu.edu.ua/article/view/332039

4. National Security Commission on Artificial Intelligence. (2021). Final report. National Security Commission on Artificial Intelligence. Retrieved from: https://www.dwt.com/-/media/files/blogs/artificial-intelligence-law-advisor/2021/03/nscai-final-report--2021.pdf

5. NATO. (2024). Summary of NATO's revised artificial intelligence (AI) strategy. Retrieved from: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

6. Sayler, K. M. (2020). Artificial intelligence and national security (CRS Report R45178). Congressional Research Service. Retrieved from: https://www.congress.gov/crs-product/R45178

7. Taddeo, M., Ziosi, M., & Tsamados, A. (2022). Artificial intelligence for national security: The predictability problem. Centre for Emerging Technology and Security, The Alan Turing Institute. Retrieved from: https://cetas.turing.ac.uk/publications/artificial-intelligence-national-security-predictability-problem

8. U.S. Department of Defense. (2022). Responsible artificial intelligence strategy and implementation pathway. U.S. Department of Defense. Retrieved from: https://www.ai.mil/Portals/137/Documents/Resources%20Page/DoD%20Responsible%20AI%20Strategy%20and%20Implementation%20Pathway.pdf

9. Hurzhii, S. V. (2024). Trends in the application of artificial intelligence technologies in the military-technical sphere. Information and Law, 3(50). DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311713. Retrieved from: https://il.ippi.org.ua/article/view/311713

10. Husak, Yu. A., Kitik, S. V., & Kanduiev, D. V. (2023). Modern aspects of the use of artificial intelligence by the Armed Forces of Ukraine under martial law. Current Issues of National Jurisprudence, (2), 91–95. DOI: https://doi.org/10.32782/39221475

11. Danyk, Yu., Dykyi, A., Shestakov, V., & Shyrshov, R. (2025). Analysis and substantiation of the introduction and use of artificial intelligence for the needs of the security and defence sector of Ukraine. Society and Security, 6(12), 64–76. DOI: https://doi.org/10.26642/sas-2025-6(12)-64-76. Retrieved from: https://sas.ztu.edu.ua/article/view/349744

12. Pivnenko, O., Hladkov, V., Bielai, S., Skliar, M., & Pokhodenko, D. (2025). Substantiation of conceptual directions for the implementation of artificial intelligence for the needs of the security and defence sector of Ukraine. Society and Security, 3(9), 48–55. DOI: https://doi.org/10.26642/sas-2025-3(9)-48-55. Retrieved from: https://sas.ztu.edu.ua/article/view/334358

13. Verkhovna Rada of Ukraine. (2018). On National Security of Ukraine: Law of Ukraine No. 2469-VIII of June 21, 2018. Bulletin of the Verkhovna Rada of Ukraine, (31), Art. 241. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19

14. President of Ukraine. (2021). On the Decision of the National Security and Defense Council of Ukraine of March 25, 2021 "On the Military Security Strategy of Ukraine": Decree of the President of Ukraine No. 121/2021 of March 25, 2021. Retrieved from: https://zakon.rada.gov.ua/laws/show/121/2021

15. Cabinet of Ministers of Ukraine. (2020). On approval of the Concept for the Development of Artificial Intelligence in Ukraine: Order No. 1556-r of December 2, 2020. Retrieved from: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80