UDC 351.74+351.86: 355.45: 341.222 (477)



A. Manko **V. Klishin** **L. Bilenkova**

ANALYSIS OF REGULATORY AND LEGAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN MILITARY MANAGEMENT SYSTEMS

Based on an analysis of current regulatory and legal aspects, attention is focused on important legal issues and risks associated with the use of AI in combat management: responsibility and legal accountability, compliance with international humanitarian law (IHL), protection of personal data and intelligence data, dual use and export restrictions, reliability, explainability and testing, ethical and human rights issues. Indicative regulatory practices are presented: formalization of internal rules for defense forces, application of accountability and audit mechanisms, compliance with international documents and compatibility with partners, control over the export/import of technologies, and cooperation with industry. Practical recommendations are proposed for the implementation of AI in Ukrainian. military affairs: a national concept/strategy for regulating AI in the field of defense procedures, certification and testing for DSS (Decision Support System) used in combat management, a mechanism for distributing responsibility between the manufacturer, operator, and state, rules for processing and protecting data in defense AI systems, professional development, and cooperation with international partners. International standards and the influence of external regulations are described; international experience, ethical principles, and national security needs are taken into account; aspects of the current national legal framework and initiatives for the application of artificial intelligence in military command and control systems are outlined.

Areas for further research necessary for the process of improving the regulatory framework for the use of AI in military command are outlined: analysis of cases of AI application in Ukrainian combat realities (legal, ethical, operational); study of legal norms (international law, international humanitarian law) regarding responsibility for the actions of autonomous or semi-autonomous systems; development of a methodology for risk assessment and auditing of AI systems in military standards; study of vectors for integrating AI solutions with cybersecurity systems, personal and operational data protection, intellectual property, and state secrets; empirical research in the context of the attitudes of civilians, military personnel, and commanders toward the use of AI in combat management, taking into account social and psychological factors in regulatory regulation.

Keywords: *national security, military command, artificial intelligence (AI), decision support systems, regulatory and legal regulation, security and defense forces.*

Statement of the problem. In modern military conflicts, where response time and information are critically important, AI systems for combat management and decision support are a strategic and extremely important resource. They can provide rapid analysis of intelligence data, prediction of enemy activity, optimization of resources, and planning of operations. However, without clear legal guarantees and ethical standards, there is a risk of violating international law, causing harm to the civilian population, manipulation, abuse, loss of trust, legal conflicts, and liability.

Artificial intelligence (AI) is increasingly being implemented in military command and control systems and decision-support systems (DSS). These technologies increase the speed of data processing, the quality of forecasts, and the scale of analytics, but at the same time create new legal, ethical, and operational challenges-from issues of responsibility for decisions to the protection of personal data and ensuring compatibility with international humanitarian law. For Ukraine, which is operating in the context of an ongoing armed conflict, the issue of the regulatory and legal use of AI in the defense sector is particularly acute and relevant.

Analysis of recent research and publications. The issue of AI application in military command systems has been addressed by a number of researchers, including S. Belay [6], G. Drobakha [10], V. Yemanov [8], O. Iokhov [10], V. Lisitsyn [10], O. Oleshchenko [10], O. Onoprienko [6], E. Smirnov [13], K. Sporyshev [6, 8, 11, 12], V. Tkachenko [13], and others. The works of these authors consider the general principles of

informatization of security and defense forces, the construction of information and analytical support systems for combat operations, structural and functional models of decision support systems, theoretical foundations of military management, algorithms for processing intelligence data, and automation of operations planning processes.

Considerable attention is paid to the organization of information flows, the architecture of management information systems, improving the efficiency and soundness of commanders' decisions, as well as general aspects of the regulatory and legal support of information and analytical systems for security forces.

At the same time, most of these studies focus primarily on the organizational, technical, and informational-analytical aspects of military management systems, while a specialized comprehensive analysis of the regulatory and legal aspects of the specific application of AI in military management is presented in a fragmented manner. The following issues remain insufficiently addressed: the distribution of legal responsibility between the developer, operator, and state for decisions made using AI components; ensuring the compliance of such systems with the requirements of international humanitarian law; the legal regime for processing large amounts of operational and personal data in AI systems; the regulation of dual-use technologies and export and import restrictions; and the establishment of requirements for transparency, explainability, auditing, and certification of defense AI solutions.

The purpose of the article is to analyze the current regulatory framework and standards governing the use of AI in military command and control systems, as well as to develop practical recommendations for improvement in Ukraine, taking into account international experience, ethical principles, and national security needs.

Summary of the main material. First, we will analyze national regulations and strategic documents, such as the "White Paper of the Ministry of Digital Transformation on the Regulation of AI in Ukraine: The Vision of the Ministry of Digital Transformation," published in June 2024 as analytical material prepared for consultation [9]. It outlines the principles that should be taken into account when regulating artificial intelligence: protection of human rights, responsibility, transparency, risk management, and business preparation. The White Paper suggests that Ukraine may adopt a law similar to the European AI Act in the future and create a regulatory body [1].

It should be noted that the initial steps in the legal framework and initiative to regulate AI in Ukraine were the publication of the White Paper and recommendations on the responsible use of AI by the Ministry of Digital Transformation, which outlined the principles and directions of state policy on the use of artificial intelligence. These documents laid the foundation for the further development of the regulatory framework, including the development of specialized provisions in the defense and education sectors (in particular, internal regulations and instructions for educational and defense institutions) [8].

After all, there is still no publicly known special law that directly regulates the use of AI in military systems or combat control systems. Regulation is partially carried out through legal norms: the Law of Ukraine "On the Protection of Personal Data" [16], "On State Secrets" [14], "On National Security of Ukraine" [15].

In its AI Strategy [4], NATO establishes principles for the responsible use of AI in the field of defense, including:

– legality: compliance with national and international law, in particular international humanitarian law and human rights in general;
– responsibility and accountability;
– explainability and traceability;
– reliability: clear definition of use cases, testing throughout the life cycle;
– controllability: ability to interact with humans, avoid undesirable consequences, possibility of shutdown or deactivation;
– prevention of biased, unethical, or discriminatory cause-and-effect relationships.

One of the key provisions of the EU AI Act, adopted by the European Parliament on June 14, 2023, is particularly valuable for our research: the exclusion of AI systems developed or used exclusively for military, defense, or national security purposes from the scope of the regulation [7].

This means that although many civil AI systems fall under the AI Act, those that are solely for military use may not be subject to regulation under this law. However, this exception raises the question of how to classify dual-use systems [2].

Therefore, when comparing, within the scope of scientific research, the paradigms of Ukrainian strategic documents on AI, especially in the military sphere, with the regulatory framework of other countries, we note

that their experience shows that successful regulation of military AI includes mandatory ethical principles, audit systems, accountability, testing requirements, and the human-in-loop concept. Such standards are reflected in NATO documents, in the practices of military departments, for example, in the United States, and in international discussions on autonomous weapons systems [2, 3, 4].

However, in our opinion, attention should be paid to the relevance of the main legal problems and risks of using AI in military command and control systems:

1. Responsibility and legal accountability.

When a DSS provides a recommendation (or disseminates an automatic decision), who is responsible for the consequences: the algorithm developer, the operator/commander, the hardware manufacturer, or the state? Without a clear logic for the distribution of responsibility, there is a risk of "guilt by proxy algorithm" and complications in investigating incidents.

2. Compliance with international humanitarian law (IHL).

The use of AI for target identification, classification, and selection must comply with the rules of proportionality, distinction, and necessity. Autonomous or semi-autonomous systems must ensure human control so that decisions on the use of force remain within the limits of IHL.

3. Protection of personal data and intelligence data.

DSSs process large amounts of data, including personal data of civilians and confidential information. This raises questions of compliance with national data protection laws and international standards, as well as risks of leakage/misuse.

4. Dual use and export restrictions.

AI technologies are often dual-use. Foreign partners and suppliers may impose export restrictions and require compliance with their national principles (particularly in countries with strict regulations on the use of AI).

5. Reliability, explainability, and testing.

Assessing trust in AI conclusions, verifying system behavior in combat conditions, and documenting model training processes (training data provenance) are necessary for the legal validity of decisions made.

6. Ethical and human rights issues.

The use of biometric tools and facial recognition technologies, as well as examples of cooperation with commercial providers (particularly questionable practices), raise concerns about human rights and possible abuses.

In practical terms, specific projects and partnerships are already being established for the application of AI in defense. For example, the use of image analysis technologies for forensic identification.

At the same time, the absence of a single specific law on AI (with clear rules on military application) creates legal uncertainty for military command and control systems [12].

In accordance with international standards and the influence of external regulations, alliances are already developing priority principles that will influence national policy on the use of AI in military affairs.

For example, NATO has approved the Principles of Responsible Use of AI in Defense [5] and strategies for integrating AI into defense capabilities, with an emphasis on legality, transparency, risk management, and human control. For member countries and partners, this creates guidelines for compatibility based on ethical principles when conducting joint operations.

It is important to note, in the context of the issue raised, that the European Union has adopted the AI Act, which imposes strict requirements on the market for civilian AI systems. At the same time, the text provides for a specific "exclusion" – the application of the law does not extend to systems used exclusively for military, defense, or national security purposes, although the limits of this exclusion may be subject to interpretation (especially for dual-use systems or when the same system is used for both civilian and law enforcement/military purposes) [2]. This paradigm has direct implications for Ukraine in terms of approaches to import, cooperation, and standardization.

Thus, we note the following in the practice of regulating the use of AI in the national security system:

1. Formalization of internal rules for military command and control systems. It is advisable to adopt interdepartmental standards and internal regulations (provisions, orders) for the use of AI in military command systems: requirements for algorithm certification, testing procedures in experimental conditions, rules for logging decisions and storing training data. A partial example is the provisions developed in individual institutions on the use of AI as supporting documents, but a unified national methodology is needed [12].

2. Ensuring human control (human-in-the-loop / human-on-the-loop). Standards should explicitly require that human decision-makers retain control in critical situations, especially when it comes to the use of firepower or operations that pose a high risk to the civilian population. NATO principles support this approach [12].

3. Application of accountability and audit mechanisms.

Introduction of audit systems (ex-post and ex-ante), logging of AI decisions, and incident investigation procedures. Clear standards are needed for collecting evidence and assessing the correctness of algorithmic decisions in the event of disputes or violations.

4. Compliance with international documents and compatibility with partners.

Ukraine must coordinate its regulations with NATO standards and EU legal norms and take into account the provisions of international acts, especially in the case of cooperation, procurement, and integration of allied systems (technical, legal, organizational, cultural/ethical) [4].

5. Control over the export/import of technologies and cooperation with industry.

A transparent policy is needed regarding contracts with vendors, confidentiality conditions, manufacturers guarantees regarding security and access to basic models, as well as requirements for the localization of important components (to avoid hidden motives).

We see the following specific steps as recommendations for regulating AI in the military command system:

1. Adopt a national concept/strategy for regulating AI in the defense sector, which defines legal, ethical, and technical standards; coordinate it with the Ministry of Digital Transformation, the Ministry of Defense, the Ombudsman, and international partners [4].

2. Introduce mandatory certification and testing procedures for DSS used in combat management (evidence base and model validation).

3. Enforce the principle of human control in regulatory acts (orders, instructions), define categories of decisions where humans have the final say [5].

4. Create a mechanism for distributing responsibility between the manufacturer, operator, and state, including a procedure for criminal or administrative response in the event of a crime.

5. Develop rules for data processing and protection in defense AI systems, taking into account human rights and requirements for the storage/transfer of intelligence data [1].

6. Build in transparency and accountability: logging, log files, testing reports, explainability requirements where critical for legal and ethical justification of decisions.

7. Training and professional development: prepare operators, commanders, and legal departments to work with AI, including courses on ethics, responsibility, and understanding model limitations.

8. Cooperation with international partners: implement compatible technical standards and exchange best practices (NATO, EU), while defending the position on humanitarian guarantees in the international arena [4].

In view of the above, introduce a regulatory framework, establish mandatory levels of human control in decisions that may lead to the use of force or civilian casualties, provide operational instructions that clearly define who, how, and when to intervene or has the right to stop/interrupt the operation of an AI system, establish accountability and audit mechanisms (legal procedures for bringing to justice in case of violations – administrative, civil, criminal), cybersecurity: ensuring protection against failures, attacks, and manipulation in cyberspace, cooperation with international partners, education, and training – will ensure the regulation of AI in the military sphere.

Conclusions

Thus, Ukraine is on the verge of forming a comprehensive regulatory framework for the application of AI potential, including the White Paper of the Ministry of Digital Transformation, but at present, there are no specialized laws that would clearly and constructively regulate the use of artificial intelligence in combat management. International standards (NATO, EU) provide useful guidelines, but they have limitations: exceptions for military systems, difficulties with dual-use technologies, and the opacity of some approaches.

The use of AI in defense requires clear legal responsibility, strict compliance with international humanitarian law, protection of personal and strategic data, and ethics. Without these elements, there are significant risks of legal, moral, and operational problems. Practical steps for Ukraine should include legislative changes, standards, certification, human control, international harmonization, as well as training and the development of practical audit and monitoring procedures.

Thus, AI in military command and control systems can significantly enhance the operational capabilities of Ukraine's Armed Forces and security forces, but full and safe implementation is only possible with a clear regulatory framework. The combination of internal rules (orders, regulations, certification), international standards (NATO principles), and measures aimed at protecting human rights and distributing responsibility will minimize risks and ensure the legality of AI use in critical military processes. It should take into account both the speed of innovation in the defense sector and the need for accountability and transparency in making decisions that could have fatal consequences.

We see prospects for further research in a detailed analysis of specific cases of AI application in military command systems in Ukraine (judicial, ethical, operational); the study of legal precedents (in international law, international humanitarian law) regarding responsibility for the actions of autonomous or semi-autonomous systems; developing a methodology for risk assessment and auditing of AI systems in defense department standards; researching issues of integrating AI solutions with cybersecurity systems, protection of personal and operational data, intellectual property, and state secrets; empirical research on the attitudes of society, military personnel, and commanders toward the use of AI in combat management in order to take social and psychological factors into account in regulatory frameworks.

References

1. AI House, Roosh, and other sources of data on the Ukrainian AI market: statistics on startups and investments (as cited in the White Paper) (2024). Retrieved from: https://surl.li/xcisyh (accessed 14 October 2025) [in English].

2. ECNL (European Center for Not-for-Profit Law) (2025). EU AI Act needs clear safeguards for AI systems for military and national security purposes. Retrieved from: EU AI Act needs clear safeguards for AI systems for military and national security purposes ECNL (accessed 14 October 2025) [in English].

3. Forbes Digital (2024). Ministry of Digital Transformation proposes adopting an analogue of the European AI Act and creating a regulatory body. Article, June 26 (2024). Retrieved from: https://surl.li/mwqzmy (accessed 15 October 2025) [in English].

4. NATO. Strategy on Artificial Intelligence (2021) and updated version (2024). Retrieved from: https://www.bing.com/ (accessed 15 October 2025) [in English].

5. NATO Watch. *Briefing Paper No. 88: NATO's AI Strategy.* Retrieved from: https://surl.li/ohrhqx (accessed 15 October 2025) [in English].

6. Belyi S. V., Sporyshev K. O., Onopriienko O. S. (2024). *Henezys informatsiino-analitychnoho zabezpechennia sluzhbovo-boiovoi diialnosti syl bezpeky Ukrainy: suchasni vyklyky derzhavnoho upravlinnia* [Genesis of information and analytical support for the operational and combat activities of the security forces of Ukraine: current challenges of public administration]. *Current Issues in Modern Science. Public Administration.* no. 1 (19), pp. 105-113 [in Ukrainian].

7. *Ievropeiskyi parlament. Rehlament pro shtuchnyi intelekt (AI Act) (2023). Ofitsiinyi tekst ukhvalenyi 14 chervnia 2023 roku.* [European Parliament. Regulation on Artificial Intelligence (AI Act). Official text adopted on June 14, 2023]. Retrieved from: Texts adopted - Artificial Intelligence Act - Wednesday, June 14, 2023 (accessed 17 October 2025) [in Ukrainian].

8. Yemanov V. V., Sporyshev K. O. (2024). *Dosvid funktsionuvannia systemy informatsiino-analitychnoho zabezpechennia sylovykh struktur providnykh krain svitu.* [Experience of the functioning of the information and analytical support system for the security forces of the world's leading countries]. *Scientific perspectives. Public administration.* No. 1 (43), pp. 132-142 [in Ukrainian].

9. *Ministerstvo tsyfrovoi transformatsii Ukrainy. Bila knyha z rehuliuvannia ShI v Ukraini: bachennia Mintsyfry* (2024). [Ministry of Digital Transformation of Ukraine. White Paper on AI Regulation in Ukraine: The Vision of the Ministry of Digital Transformation]. Kyiv, June. Retrieved from: https://surl.li/siupkp (accessed 15 October 2025) [in Ukrainian].

10. *Osnovy informatyzatsii Natsionalnoi hvardii Ukrainy: navch. Posib.* (2016). [Fundamentals of Informatization of the National Guard of Ukraine: textbook]. G. Drobakha, O. Oleshchenko, O. Iokhov, V. Lisitsyn, et al. Kharkiv: National Academy of Sciences of Ukraine, Municipal Printing House, 366 p. [in Ukrainian].

11. Sporyshev K. O. (2024). *Analiz normatyvno-pravovoi bazy informatsiino-analitychnoho zabezpechennia syl bezpeky Ukraini* [Analysis of the regulatory and legal framework for information and analytical support of Ukraine's security forces]. *Honor and Law*. No. 1 (88), pp.142-149 [in Ukrainian].

12. Sporyshev K. O. (2024). *Zasady avtomatyzatsii informatsiinykh system upravlinskoho pryznachennia syl bezpeky peredovykh krain YeS ta NATO* [Principles of automation of management information systems for security forces in advanced EU and NATO countries]. *Public Administration: Improvement and Development.* Issue 2. Retrieved from: https://surl.li/ogcfrs (accessed 15 October 2025) [in Ukrainian].

13. Tkachenko V. I., Smirnov E. B., et al. (2008). *Teoriia pryiniattia rishen orhanamy viiskovoho upravlinnia: monohrafiia*. [Theory of decision-making by military authorities: monograph]. V.I. Tkachenko, E.B. Smirnov et al. Edited by V.I. Tkachenko, E.B. Smirnov. Kharkiv: Kharkiv University of Public Security, 542 p. [in Ukrainian].

14. *Zakon Ukrainy "Pro derzhavnu taiemnytsiu": № 1079-XIV* [Law of Ukraine "On State Secrets": no. 1079-XIV]. (1999, September 21). Retrieved from :https://zakon.rada.gov.ua/laws/show/3855-12#Text (accessed 14 October 2025) [in Ukrainian].

15. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 2469-VIII* [Law of Ukraine "On the National Security of Ukraine": no 2469- VIII].(2018, June 21). Retrieved from : https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 14 October 2025). [in Ukrainian].

16. *Zakon Ukrainy "Pro zakhyst personalnykh danykh" № 4240-IX* [Law of Ukraine "On the Protection of Personal Data" no. 4240-IX]. (2025, February 12). Retrieved from : https://zakon.rada.gov.ua/laws/show/2297-17#Text (accessed 14 October 2025) [in Ukrainian].

The article was submitted to the editorial office on 27 November 2025

УДК 358:004.8

А. В. Манько, В. М. Клішин, Л. М. Біленкова

АНАЛІЗ НОРМАТИВНО-ПРАВОВИХ АСПЕКТІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ВІЙСЬКОВОГО УПРАВЛІННЯ

На підставі аналізу чинних нормативно-правових аспектів акцентовано увагу на важливих правових проблемах і ризиках застосування ШІ у бойовому управлінні: відповідальності та юридичній підзвітності, дотриманні міжнародного гуманітарного права (МГП), захисті персональних даних та розвідданих, подвійному призначенні та експортних обмеженнях, надійності, пояснюваності і тестуванні, етичних та правозахисних проблемах. показано орієнтовну практику врегулювання: формалізація внутрішніх правил для сил оборони, застосування механізмів відповідальності та аудиту, конформність із міжнародними документами та сумісність із партнерами, контроль за експортом/імпортом технологій і співпраця з промисловістю. Запропоновано рекомендації впровадження ШІ в українську військову справу: національна концепція/стратегія регулювання ШІ у сфері оборонних процедур, сертифікація та тестування для DSS (Decision Support System – Системи підтримки прийняття рішень), що використовуються у бойовому управлінні, механізм розподілу відповідальності між виробником, оператором і державою, правила обробки та захисту даних в оборонних ШІ-системах підвищення кваліфікації, співпраця з міжнародними партнерами. Охарактеризовано міжнародні стандарти та вплив зовнішніх нормативних актів; враховано міжнародний досвід, етичні принципи і потреби національної безпеки; окреслено аспекти поточної національної правової бази та ініціативи щодо застосування штучного інтелекту в системах військового управління.

Окреслено напрями подальших досліджень, необхідних для процесу удосконалення нормативного врегулювання у межах використання ШІ в умовах військового управління: аналіз кейсів застосування ШІ в українських бойових реаліях (судові, етичні, операційні); вивчення правових норм (міжнародне право, міжнародне гуманітарне судочинство) стосовно відповідальності за дії автономних або напівавтономних систем; розробка методології щодо оцінок ризику та аудиту ШІ-систем у військових стандартах; вивчення векторів інтеграції ШІ-рішень із системами кібербезпеки, захисту

персональних та оперативних даних, інтелектуальної власності, державної таємниці; емпіричне дослідження в контексті ставлення суспільства, військовослужбовців і командирів до використання ШІ в бойовому управлінні, щодо врахування соціальних й психологічних чинників у нормативному врегулюванні.

Ключові слова: *державна безпека, військове управління, штучний інтелект (ШІ), системи підтримки прийняття рішень, нормативно-правове регулювання, сили безпеки та оборони.*

Manko Andrii – PhD, Head of the National Academy of the National Guard of Ukraine
https://orcid.org/0009-0002-9860-9561

Klishin Viktor – Candidate of Military Sciences, Associate Professor, Head of the Educational and Scientific Institute for Training Management Personnel, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-5291-5160

Bilenkova Lidiia – Candidate of Pedagogical Sciences, Junior Researcher at the Research Laboratory for Construction and Operational Application of the National Guard of Ukraine, Educational and Scientific Institute for Training of Management Personnel, Associate Professor, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-2683-3794