**UDC 342.9, 351, 004.8**

**V. Korniienko**

**V. Hmyria**

**M. Styshuk**

# ORGANIZATIONAL AND LEGAL PRINCIPLES OF USE ARTIFICIAL INTELLIGENCE IN THE FIELD OF STATE SECURITY

*An analysis of the use of artificial intelligence in the field of ensuring state security, in particular in the law enforcement sector, was conducted. Based on the analysis of the studied sources, current national and international legislation, as well as practical experience, the risks of using the capabilities of neural networks were identified. Substantiated recommendations were proposed for improving the regulatory framework regarding liability, personal data protection, cybersecurity, and ethical use of artificial intelligence tools.*

***Keywords:*** *artificial intelligence, neural networks, service and combat activities of the National Guard of Ukraine, state security, legislative support, cybersecurity.*

**Statement of the problem.** The modern world is characterized by an unprecedented level of digital transformation, which opens up new opportunities for the harmonious development of society and the state as a whole. Neural networks, artificial intelligence (AI) tools are rapidly integrating into all spheres of life, including ensuring state security, creating both unprecedented opportunities and serious challenges and threats. On the one hand, AI is able to significantly improve the effectiveness of actions in preventing cyber threats, terrorist activities and their neutralization, on the other hand, its use requires careful legal analysis in order to avoid various abuses, uncontrolled actions and ensure the ethical use of its capabilities.

The relevance of the study is due to the lack of a clearly defined organizational and legal framework for the use of AI in the field of ensuring state security both in Ukraine and in the world. Current legislation does not fully take into account the specifics of the use of AI, which leads to legal uncertainty and limits the effectiveness of its use. Therefore, the development of proposals to improve the organizational and legal framework for the use of AI in the field of ensuring state security is seen as an important task, the solution of which will contribute to increasing the level of national security and the protection of human rights.

**Analysis of recent research and publications.** The study is based on the theoretical principles set out in the works of A. Turning, C. Shenon, O. Kryvetsky and some other scientists. Certain aspects of the use of artificial intelligence have become the subject of research by such scholars: M. Karchevskyi, A. Petrenko, I. Horodyskyi, N. Shyshka, K. Piper, M. Watney, O. Radutnyi, T. Katkova, O. Yastrebov, V. Kharytonov etc. However, the issue of defining the concept of "artificial intelligence" remains debatable. The legislative regulation of its application is unresolved, and the issue of standards for the formation of an appropriate legal model that will ensure the proper functioning of the sphere of state security and defense not only in Ukraine, but also in the world is becoming more relevant.

**The purpose of the article** is consists in analyzing the organizational and legal prerequisites for the use of artificial intelligence tools and developing recommendations for creating an effective and ethically balanced system for regulating the use of artificial intelligence in the field of ensuring state security in Ukraine, including in service and combat use by units of the National Guard of Ukraine.

**Summary of the main material.** The idea of creating machines capable of imitating human intelligence arose a long time ago. The initial concepts of the idea of artificial intelligence were laid down in the middle of the 20th century. The origins of AI can be traced back to the work of

© V. Korniienko, V. Hmyria, M. Styshuk, 2025

the British mathematician A. Turing. In his article "Computing Machinery and Intelligence" (1950), the scientist asked the question: can machines think? [1]. In response, he developed a test (*Turing Test)*, which was a conceptual attempt to determine whether a machine could communicate in a way that would make it indistinguishable from a human. This work by A. Turing became the basis for further research in the field of artificial intelligence, as it was the first time that the limits of the capabilities of machines were publicly questioned.

The official beginning of scientific research in the field of AI is considered to be 1956, when the term "artificial intelligence" was proposed at a seminar at Dartmouth College. The organizers of the event, in particular J. McCarthy, M. Minsky, K. Shannon , sought to develop software that could learn and solve problems. A 17-page document called the "Dartmouth Proposal" was presented. The document covered topics that scientists considered fundamental to this field of research: neural networks, the theory of computability, creativity, language processing. According to the authors, it is enough to describe in detail any feature of the human mind and transfer this information to a machine created to imitate it [2, 3].

In the following decades, artificial intelligence developed in the areas of automation, machine learning, and expert systems. In the 1960s and 1970s, research focused on creating specialized expert systems that would make recommendations based on input data. Well-known systems, such as DENDRAL for chemistry or MYCIN for medicine, demonstrated the ability to automate complex intellectual tasks. However, these systems were quite specialized and did not have the general ability to adapt to new industries.

An important breakthrough was the revival of scientific research in the field of neural networks, in particular through the development of the error backpropagation method for training multilayer neural networks [4]. This opened up new possibilities for processing large amounts of data and improving pattern recognition algorithms, which gave impetus to the further development of intelligent systems [5].

In the early 2000s, the rapid development of computing power began, which, together with access to large data sets (Big Data), stimulated a new wave of scientific research. Machine learning algorithms and deep analysis methods began to show significant results in areas such as image recognition, voice, game simulations, and robotics.

The last decades have been a stage of key scientific and technological breakthroughs in the development of artificial intelligence. One of its most common applications has been the automation of routine tasks. Software equipped with AI can perform repetitive actions much faster and more accurately than humans. Today, neural networks allow you to conduct analytical work, detect fraudulent actions, assess risks, optimize costs, etc. They are also capable of generating realistic images based on text descriptions.

The modern understanding of artificial intelligence has two aspects. The first is *the ideological* component, which determines the form in which a particular functionality should be performed. The second is the platform, that is, *the technical* component, which determines who and what set of tools will manage AI processes. A person creates developing algorithms, neural networks, as well as robotics, which is the physical shell of artificial intelligence. In this regard, the question of the responsible attitude of developers, who must understand and foresee certain limitations in the activities of AI, arises acutely.

Currently, the problem of the uncertainty of the concept of "artificial intelligence" significantly complicates the development of adequate legal support for its application, especially in such an important area as state security. The lack of a single, generally accepted definition of AI creates certain difficulties:

a) the vagueness of the regulatory scope causes gaps in the legislation;

b) it becomes more difficult to classify different AI systems by level of autonomy, which also adds to the difficulties in developing differentiated legal norms;

c) legal uncertainty complicates the issue of liability for the actions (or inaction) of artificial intelligence systems, especially in cases of harm: who is responsible – the developer, owner or user;

d) different approaches to the terminology and definition of the concept of "artificial intelligence" in different jurisdictions complicate international cooperation in the field of regulation of artificial intelligence.

To address these issues, it is necessary to develop a clear and balanced definition of AI, taking into account its various aspects and capabilities. Such a definition should form the basis of legal norms regulating the use of AI in the field of ensuring state security, taking into account the specifics of various areas of application.

Let's consider the leading areas of application of artificial intelligence in the field of ensuring state security.

*1. Cybersecurity.* Since the beginning of the war in Ukraine, cyberattacks on both national infrastructure and private companies have increased exponentially [6]. AI-based software tools are capable of effectively detecting and neutralizing cyberattacks by analyzing huge amounts of data in real time. It is known that cybercriminals have learned to use AI to create malicious code in an automated manner. Despite the fact that technology giants are trying to prevent the use of their language models to write malicious programs-viruses, hackers are constantly inventing new ways to circumvent restrictions. Target platforms (HackedGPT, WormGPT) help create malicious software. This makes the dynamics of cyberattacks very complex and unpredictable.

In the future, automated cyber threats based on artificial intelligence may become much more serious. For example, a group of cybersecurity experts "Hyas" created a "laboratory" virus "BlackMamba", which can dynamically change its code using ChatGPT . During the experiment, this "keylogger worm" successfully adapted to any scenario and avoided detection by antivirus software [7]. It is difficult to imagine how much such viruses can complicate the work of cybersecurity specialists and what damage their spread in private and public organizations can cause.

*2. Artificial intelligence on the guard of law and order and combating crime*. The introduction of artificial intelligence in legal research has the potential to assist specialists in the field of state security and the restructuring of the entire law enforcement system. As an example, artificial intelligence algorithms simplify the analysis of large arrays of intelligence data, in particular visual and text information, which significantly speeds up the decision-making process and improves the accuracy of forecasts. This makes it possible to respond more effectively to potential threats and plan preventive measures. Video surveillance systems based on artificial intelligence significantly expand the possibilities of controlling public places (streets) and the state border, automatically detecting suspicious activity and potential violations. Unique algorithms for recognizing a person's face, body movements (by gait and structure) already help to identify individuals who have committed crimes and are wanted [8].

*3. Artificial intelligence is on the watch to counter disinformation.* Modern IT technologies based on artificial intelligence are already producing algorithms that help detect and neutralize disinformation campaigns by analyzing texts, images, and videos on social networks and other sources. Some studies indicate the effectiveness of this method [9, 10].

*4. Artificial intelligence on the Guard of Security and Defense.* The importance of using AI to ensure national security and defense is confirmed by the results of research by the NATO Scientific and Technical Organization, which identifies the most significant technologies for the development of technologies for the next two decades [11]. Key technologies are considered to be, in particular, the following: BigData, neural networks, autonomous vehicles, space, hypersonic aircraft, quantum technologies, biotechnology, new materials, etc. [12]. This approach gives impetus to the re-equipment of industrial complex facilities, a radical change in approaches to the production of weapons and military equipment.

The armed forces of some developed countries of the world equip their combat systems and weapons with artificial intelligence, using it on air, sea and land platforms. The application of AI on combat platforms has contributed to the emergence of effective warfare systems that are completely independent of human influence. Under these circumstances, there is an increase in the productivity of platforms, increased efficiency and interaction between combat systems, as well as simplification of their maintenance.

Robotic combat platforms first appeared in the troops of Western armies at the stage of experimental operation in the early 2000s. With the beginning of the russian-ukrainian war in 2014 and, especially after the full-scale russian invasion of Ukraine in 2022, they began to be actively used on the battlefield [13]. Currently, there are the following Ukrainian developments of robotic ground combat platforms: "Shable" (a ground platform that is essentially a robotic machine gun turret), "Ironclad", "Lynx", "Myrotvorets", "Scorpion-2, 3", etc. These combat platforms are self-propelled vehicles that are remotely controlled, capable of independently assessing the surrounding situation using video cameras and AI-based software and performing various combat missions.

*Logistics*. Artificial intelligence already plays a crucial role in logistics and supply chain management, as identifying alternative safe routes for transporting military cargo and troops is

essential to a successful military operation. Integrating AI into transportation and logistics chains reduces support staff costs, eliminates corruption among suppliers, and minimizes human error. In transport aviation and the navy, AI also enables rapid detection of component failures in equipment, which directly prevents accidents or disasters.

*Target detection and recognition*. In complex combat conditions, artificial intelligence increases the accuracy of recognition of unknown targets. This allows defense/offensive forces to achieve a complete understanding of the potential field of activity through in-depth analysis of documents, reports, maps, news and other important information that helps in identifying a potential target. AI-based target recognition systems have several specific advantages: predicting enemy behavior; assessing the terrain and all unknown objects located in the territory; determining the environmental consequences of the use of a particular weapon. Thus, in early 2020, Reuters announced the deployment of the ISTAR reconnaissance, surveillance and targeting system on the UK Air Force Sentinel aircraft. This system is based on AI and provides detection of ground and sea objects and monitoring their movement [14].

*Assistance to combat medics*. Robotic ground platforms equipped with AI are used to provide emergency care to wounded soldiers in the zone of active combat operations for their subsequent evacuation from the dangerous zone. Such platforms quickly diagnose a wounded soldier, determine the level of his damage, recommend treatment methods, which helps combat medics in the field to make the right decisions in stressful situations [15, 16]. It should be noted that regardless of the location of the contact line, AI has access to a database of hospitals and military medical records, which allows algorithms to detect and sort health problems in the military.

*Threat monitoring and situational analysis*. These operations are used to process information to support a wide range of military operations. Artificial intelligence helps to quickly process large amounts of data simultaneously from multiple servers, summarizes the analyzed information, and offers ready-made conclusions. Such analysis allows the military to identify patterns, generalize conclusions, and in some cases, make their own adjustments. For example, thanks to unmanned systems equipped with AI, the military can monitor large areas for a long time, assess enemy concentrations, enemy equipment, and their movements, and quickly transmit information.

*Simulation and training* is another extremely useful area of application of AI tools, which combines systems engineering, software development and computer science to create computerized models. More and more countries are investing in programs for modeling situations and training the military based on modern experience. Practicing various situations on simulators allows to minimize losses on the battlefield, to take into account human errors (miscalculations) and contributes to the development of safety measures [17].

As we can see, artificial intelligence is an effective tool that can significantly improve the level of many components of Ukraine's state security. However, its use is associated with certain risks, in particular the possibility of abuse and dependence on high technologies. Therefore, an important task is the development and implementation of effective risk management strategies, the creation of ethical norms for the use of artificial intelligence and the provision of cybersecurity systems based on it. The use of AI in law enforcement activities raises the issue of respect for human rights, the possibility of biased approaches and discrimination. Automation of decisions based on AI is dangerous due to the loss of human control and the adoption of biased decisions. It should also be noted that the widespread implementation of AI tools contributes to the automation of labor and can lead to increased unemployment.

Therefore, in parallel with the development of technologies, it is necessary to pay maximum attention to the development of effective legal regulation and control mechanisms to minimize risks and maximize the positive impact of AI on society and the state. Ensuring a balance between the rapid development of technologies and ensuring security is a key task for modern society.

Analysis of the studied sources, domestic and foreign legislation allows us to conclude that currently there is no single approach to the definition of artificial intelligence and the features of the regulatory and legal regulation of its application. However, some steps have already been taken towards solving the above problems both at the national and international levels. In recent years, many states have developed long-term national strategies for the development of artificial intelligence and have taken certain measures to implement them. AI development strategies of

different countries of the world can be conditionally divided into the following main groups [18].

1. Countries (USA, Great Britain, Germany, Saudi Arabia, etc.) that are distinguished by a realistic attitude to the formation of AI strategies, a deep analysis not only of the state of the scope of AI application in the country, but also of the real needs for its development. The strategies of these countries are of a fundamental nature and reflect both general global problems of AI implementation and specific plans for the digitalization of many sectors of the national economy and various spheres of public relations.

2. A group of countries characterized by a thorough and pragmatic approach to goals and stages of their achievement, taking into account the real needs of the state and the formation of individual unique tasks and goals for the development of AI: Grand Duchy of Luxembourg, Malaysia, Lithuania.

3. Countries whose strategies are implemented in a formalized form define the basic goals of the country's development in the direction of implementing AI technologies in certain areas of public life: Australia, the Republic of Austria, the Kingdom of Spain, Qatar, Portugal, the Republic of Israel, the Swiss Confederation, etc. [18].

Ukraine has adopted documents that define the strategy for using artificial intelligence technologies in the field of national security and defense [19–24]. The following are among the main ones.

1. The National Security Strategy of Ukraine, according to which Weapons systems based on AI technologies are being developed, new materials, robotics, and autonomous drones.

2. The Information Security Strategy and the Cybersecurity Strategy of Ukraine, as they provide for the prevention of hybrid threats in the form of disinformation and information operations, the protection of personal data, etc.

3. The Strategy for the Development of the Defense Industrial Complex of Ukraine, which directly mentions the widespread use of the latest technologies in production, in particular with the use of AI.

The Cabinet of Ministers of Ukraine approved May 12, 2021 "Action Plan for the Implementation of the Concept of Artificial Intelligence Development in Ukraine for 2021–2024", according to which a number of measures and legislative initiatives were planned to be developed for the specified period, in particulaя: the introduction of legal regulation on the formation of state policy in the field of AI; the introduction of state support for the use of AI technologies in priority sectors of the economy; the introduction of AI technologies into the national cybersecurity system to analyze and classify threats and choose a strategy for their containment and prevention; the definition of priority areas and main tasks for the development of AI technologies in defense planning documents etc. [25].

Analysis of the current legislation of Ukraine indicates the presence of certain initiatives to regulate the use of artificial intelligence in the sphere of state security and defense, which are based on urgent needs. However, there is no single strategic document, for example, the National Strategy for the Development of AI in the Sphere of Ensuring National Security and Defense. This is precisely what hinders the systematic implementation of these technologies. This situation stimulates active discussion and scientific research on the prospects for the use of AI in the defense complex of Ukraine. The issues of determining promising areas of application of AI, analyzing its impact on the defense-industrial complex and evaluating the experience of other countries in this regard are becoming more urgent.

The United States, the European Union (EU), and China are actively developing their own strategies and regulatory frameworks for regulating AI, while other states may not have the resources or technological readiness to develop and implement effective regulatory mechanisms. This creates the basis for geopolitical and economic differences in attitudes towards the technology, including how to apply ethical principles, protect data privacy, and prevent AI misuse in the areas of security or intellectual property.

The European Union can be considered a leader at the international level in terms of AI regulation. In 2021, the EU presented the draft "AI Act", which envisages the creation of a single legal framework for the application of AI within Europe [26]. This document proposes a systematic approach to the risks associated with the use of AI, in particular defining different categories of risks. Thus, the European regulatory framework provides for stricter control over high-risk applications of AI (systems for automated decisions in judicial proceedings or the use of AI in robotics), while more liberal approaches are proposed for areas with lower risks.

The United States is also actively working on a national AI strategy [27]. However, their approach focuses more on fostering innovation, technology development, and supporting the private sector,

making the United States one of the most innovative countries in the field. However, less attention to regulation and oversight may lead to certain ethical and privacy issues in the future. National Artificial Intelligence Initiative Act of 2020 (National Artificial Intelligence Initiative Act of 2020) encourages and subsidizes innovative AI efforts in key US federal agencies. The AI Bill of Rights, introduced in 2022, contains a set of guiding, non-binding principles for the safe and secure development of AI [28]. Compared to the European Union, the US is less focused on regulating the use of AI, although some states (such as California) have already begun to implement their own laws aimed at protecting privacy and data security.

China is another important player on the international stage, especially in the context of AI development. It is actively investing in research and development in this area, with ambitious plans to become a world leader in the use of artificial intelligence by 2030. At the same time, China has a different approach to regulation (Cyberspace Administration of China – CAC), focusing on strong state control and showing less attention to human rights and ethical issues compared to Europe or the US. This creates challenges for international cooperation, as differences in approaches can cause difficulties in global governance of technologies and their impact on society. The new Chinese rules will apply only to those generative AI services that are available to the general public, and not to those developed, for example, in research institutions. One requirement is that generative AI services will have to obtain a license to operate. If a generative AI service provider detects "illegal" content, it must take measures to stop generating such content, improve the algorithm, and then report it to the relevant authority.

The UN and other international organizations are also addressing the issue of regulating artificial intelligence at the global level. For example, the UN Special Commission on Ethics in the Field of AI is studying the ethical, social and legal aspects of the use of these technologies. In 2021, the "Global Ethics of Artificial Intelligence" was developed and published, which is designed to help governments and other stakeholders define principles for the fair use of AI. It covers issues of ethics, transparency, accountability and the protection of human rights. This document, in particular, states that United Nations structures should ensure that artificial intelligence systems do not override human freedom and autonomy in decision-making, and should guarantee human oversight. All stages of the life cycle of an artificial intelligence system should include human-centric design practices and leave meaningful opportunities for human decision-making [30].

There is also active cooperation between national governments and private technology companies. For example, large technology corporations such as Google, Microsoft, IBM are actively involved in developing policies for regulating AI [31, 32]. They are creating their own codes of ethics and working to improve technologies to ensure their safe use. However, cooperation is hampered by the lack of transparency in the policy development process, as well as the contradiction between the companies' desire to develop technologies for commercial purposes and the need to ensure their safety and ethics.

Global initiatives to regulate AI are still in their infancy. This is one of the main reasons why it is important to create international platforms for sharing experiences and developing common standards. Technical standards that take into account both innovative development and the need for safe and ethical use can become the basis for effective international cooperation. The challenges of international cooperation in regulating AI also include issues of global competition and the risks associated with the technological race. Countries may have different priorities in developing AI – from improving national security to commercial and economic interests. This can lead to unequal access to technologies and the impact of AI on different countries and regions.

Another important problem caused by the lack of a clear definition is that legislative bodies cannot create an appropriate infrastructure for monitoring and evaluating the development of AI technologies. Due to the rapid development of AI technologies, the issue of determining copyright for objects created by artificial intelligence is becoming more relevant. Who is the author of such a work – the person who created the algorithm, or the AI itself? There have already been cases when courts in different countries have considered the issue of copyright for works created by AI. In the USA, for example, copyright cannot be granted to AI, since it is not a natural person [33].

The issue of liability for the actions of artificial intelligence also constitutes one of the most complex and important legal problems in the context of modern technologies. Due to its ability to make autonomous decisions, AI significantly complicates the traditional understanding of liability, which in law is usually assigned to

a specific individual or legal entity. Technologies capable of self-learning and autonomous interaction with the environment pose a question to legal systems that is difficult to answer within the framework of existing norms.

In normal situations, when technologies do not have a high level of autonomy, responsibility for their actions usually lies with their creators – developers or owners. When a system (for example, a robot) makes a mistake, responsibility lies with the company that manufactured it or the owner. However, for more autonomous systems that are able to make decisions and take actions without human intervention, the traditional interpretation of responsibility is not so clear. In particular, when it comes to situations in which AI causes harm. Thus, in the event of an accident involving an autonomous car, it is important to determine who is responsible for the consequences: the software developer, the owner of the system, or the AI itself.

One possible approach is that responsibility for AI actions should remain with the developers and owners of the technology, even if the system operates autonomously. This means that the developers who created the AI algorithm or model should be legally responsible for how these systems work. Technology owners can also be subject to sanctions if they do not provide an adequate level of control over the operation of the system. In this case, this can be seen as liability for negligence or improper use of the technology. It is also considered important to test and check systems for errors before they are released for use. And this should be the responsibility of the developers and owners.

On the other hand, in the case of systems capable of self-learning (for example, neural networks that adapt to new data), it is difficult to predict exactly how the system will behave in a given situation. This creates additional difficulties for legal regulation, since an error may be caused not by a defect in the algorithm, but by unexpected results of the system's self-learning. Since this phenomenon has not yet acquired clear legal definitions, the legal system must adapt to the new challenges posed by such technologies. One idea discussed in legal and technologist circles is to limit the liability of developers in cases of misuse of the system by users at certain stages of the use of AI [34, 35].

One interesting aspect is the proposal for the possible liability of AI itself [18, 36]. Currently, no legal system considers AI as a legal entity capable of being held accountable for its actions. However, with the development of autonomous systems and the possibility of independent decision-making, it is likely that in the future there will be a need to create new legal categories to regulate this aspect. This may be the development of the concept of "digital persons" or the creation of new legal institutions capable of operating in the context of technologies interacting with the world at an autonomous level [37, 38, 39].

Thus, the issue of organizational and legal regulation of AI opens up a whole range of legal, ethical and technical problems that require clear answers from legal systems around the world. Solving these problems requires a comprehensive approach that must take into account both the interests of technological development and the protection of the rights of individuals who may suffer from uncontrolled actions of autonomous systems.

## Conclusions

Artificial intelligence has a significant impact on national security, as it can be used in both positive and negative contexts to strengthen or weaken the security of the state. In the military, intelligence, law enforcement and other state structures, artificial intelligence is already actively used to improve the efficiency of management, data analysis and threat detection. On the one hand, this opens up new opportunities, but on the other hand, it poses new challenges for states and societies related to ethics, control and potential risks.

One of the most obvious areas of application of artificial intelligence in the sphere of state security is defense. Artificial intelligence helps to modernize defense technologies, in particular in the development of such autonomous systems as unmanned aerial vehicles (UAVs), robotic combat units, as well as intelligent systems for managing military operations. They are able to quickly process huge amounts of information and make decisions in real time, which allows for more accurate and effective operations in complex combat situations. Artificial intelligence is also used in the context of cybersecurity to detect and neutralize cyberattacks, as well as to predict possible threats and prevent them at the stage of formation.

The use of artificial intelligence in the context of intelligence and information gathering is another important component. Machine learning algorithms and big data analysis make it possible to recognize patterns that may indicate preparations for terrorist acts, military conflicts, or other threats.

Thus, artificial intelligence has enormous potential to enhance national security, but at the same time, new challenges arise that require a careful and

responsible approach to regulation, ethics, and human rights protection. The use of this technology must be balanced and ensure transparency in processes where it may affect civil liberties and the stability of the state.

Further directions of scientific research are seen as resolving issues of legal support for the functioning of artificial intelligence, taking into account the requirements of national security. Ethical rules and legislative initiatives that would allow for the effective use of artificial intelligence, while maintaining a balance between security and citizens' rights, should be subjected to scientific analysis. This involves establishing clear standards for monitoring and control, data protection, as well as maintaining democratic principles in pr processes where artificial intelligence has a significant impact on state governance.

**References**

1. Turning A. (1950). Computing Machinery and Intelligence. Mind, vol. LIX, is. 236, October, pp. 433–460. DOI: https://doi.org/10.1093/mind/LIX.236.433 [in English].

2. Gigacloud.Ua. (2023). *Dzhon Makkarti – "batko" shtuchnoho intelektu ta khmarnykh obchyslen* [John McCarthy is the "father" of artificial intelligence and cloud computing]. Retrieved from: https://surl.li/hgyusu (accessed 3 November 2024) [in Ukrainian].

3. Dartmouth News Press Release (2006). The Dartmouth Artificial Intelligence Conference: The next 50 years. Retrieved from: https://surli.cc/wfokwr (accessed 2 November 2024) [in English].

4. Fetzer J. H. (1990). What is Artificial Intelligence? Its Scope and Limits. Studies in Cognitive Systems. The Springer, vol. 4 : Dordrecht. DOI: https://doi.org/10.1007/978-94-009-1900-6_1 [in English].

5. Hunt E. B. (1975). Artificial Intelligence. London, New York : Academic press, inc. [in English].

6. Slovo i Dilo (2024). *Derzhkomspetszviazku povidomyv pro zbilshennia kilkosti kiberatak v Ukraini za mynulyi rik* [The State Committee for Special Communications reported an increase in the number of cyberattacks in Ukraine over the past year]. Retrieved from: https://surli.cc/abixgk (accessed 20 October 2024) [in Ukrainian].

7. HYAS Insight (2023). *Platforma rozvidky ta rozsliduvannia kiberzahroz* [Cyber threat intelligence and investigation platform]. Retrieved from: https://stt.llc/hyas#cover-2 (accessed 14 November 2024) [in Ukrainian].

8. i-PRO Expert platform (2022). AI People, Vehicle, Face Detection. Retrieved from: https://surl.li/xiovkm (accessed 2 November 2024) [in English].

9. National Media Literacy Project "Filter" (2023). *Shtuchnyi intelekt i dezinformatsiia: vykryttia tsyfrovoi propahandy* [Artificial Intelligence and Disinformation: Exposing Digital Propaganda]. Retrieved from: https://surl.li/ykqnxp (accessed 2 November 2024) [in Ukrainian].

10. Petriv O. (2024). *Dezinformatsiia ta shtuchnyi intelekt: (ne)vydyma zahroza suchasnosti* [Disinformation and artificial intelligence: the (in)visible threat of our time]. *Tsentr demokratii ta verkhovenstva prava*. Retrieved from: https://surl.gd/oiwpvp (accessed 15 November 2024) [in Ukrainian].

11. Balovsiak N. V. (2023). *Kiberataky z vykorystanniam shtuchnoho intelektu, za otsinkoiu NATO, ye krytychnoiu zahrozoiu* [Cyberattacks using artificial intelligence are a critical threat, according to NATO]. *Internet Svoboda*. Retrieved from: https://surl.li/gbyrlf (accessed 2 February 2025) [in Ukrainian].

12. Khaustova V., Reshetniak O., Khaustov M., Zinchenko V. (2022). *Napriamky rozvytku tekhnolohii shtuchnoho intelektu v zabezpechenni oboronozdatnosti krainy* [Directions of development of artificial intelligence technologies in ensuring the country's defense capability]. *Biznesinform*, no. 3, pp. 17–26 [in Ukrainian].

13. Militarnyi (2024). *Nazemni boiovi platformy: novyi hravets na poli boiu* [Ground combat platforms: a new player on the battlefield]. Retrieved from: https://surl.gd/njmhzc (accessed 12 February 2025) [in Ukrainian].

14. Patsuriia N. (2024). *Vprovadzhennia tekhnolohii shtuchnoho intelektu u zabezpechennia natsionalnoi bezpeky ta oboronozdatnosti Ukrainy: problemy ta perspektyvy povoiennoho periodu* [Implementation of artificial intelligence technologies in ensuring national security and defense capability of Ukraine: problems and prospects of the post-war period]. *Koordynata*. Retrieved from: https://surl.li/nwuqmc (accessed 12 February 2025) [in Ukrainian].

15. Quick D. (2023). Battlefield Extraction-Assist Robot to ferry wounded to safety. *New Atlas*, vol. 2. Retrieved from: https://surl.li/xvdhku (accessed 12 February 2025) [in English].

16. Militarnyi (2024). *V Ukraini vyprobuvaly robotyzovanyi kompleks THeMIS dlia evakuatsii*

*poranenykh* [Ukraine tested the THeMIS robotic complex for evacuating the wounded]. Retrieved from: https://surl.lu/brucud (accessed 12 February 2025) [in Ukrainian].

17. Rademacher T. (2020). Artificial Intelligence and Law Enforcement. Regulating Artificial Intelligence. *The Springer*, vol. 5. DOI: https://doi.org/10.1007/978-3-030-32361-5_10 [in English].

18. Kostenko O. V. (2022). *Analiz natsionalnykh stratehii rozvytku shtuchnoho intelektu* [Analysis of national strategies for the development of artificial intelligence]. *Informatsiia i pravo*, no. 2 (41), pp. 79–76 [in Ukrainian].

19. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu derzhavnoi bezpeky Ukrainy" № 56/2022* [Decree of the President of Ukraine on the decision of State Security and Defense Council of Ukraine "On the Strategy of Military Security of Ukraine" activity no. 56/2022]. (2022, February 2). Retrieved from: https://surl.lu/mpuima (accessed 13 February 2025) [in Ukrainian].

20. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu natsionalnoi bezpeky Ukrainy" № 392/2020* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine "On the Strategy of National Security of Ukraine" activity no. 392/2020]. (2020, September 14). Retrieved from: https://surl.lu/pbsxaa (accessed 13 February 2025) [in Ukrainian].

21. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu informatsiinoi bezpeky Ukrainy" № 685/2021* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine "On the Strategy of Information Security of Ukraine" activity no. 685/2021]. (2021, December 28). Retrieved from: https://surli.cc/qmvwnk (accessed 13 February 2025) [in Ukrainian].

22. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu kiberbezpeky Ukrainy" № 447/2021* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine "On the Strategy of Cyber Security of Ukraine" activity no. 447/2021]. (2021, August 26). Retrieved from: https://surli.cc/ryvkmt (accessed 13 February 2025) [in Ukrainian].

23. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu voiennoi bezpeky Ukrainy" № 121/2021* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine "On the Strategy of Military Security of Ukraine" activity no. 121/2021]. (2021, March 25). Retrieved from: https://surl.li/kkilrr (accessed 13 February 2025) [in Ukrainian].

24. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Stratehiia rozvytku oboronno-promyslovoho kompleksu Ukrainy" № 372/2021* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine " Strategy of development of the defense-industrial complex of Ukraine" activity no. 372/2021]. (2021, August 20). Retrieved from: https://surl.li/ikvfcb (accessed 13 February 2025) [in Ukrainian].

25. *Rozporiadzhennia Kabinetu Ministriv Ukrainy "Pro zatverdzhennia planu zakhodiv z realizatsii Kontseptsii rozvytku shtuchnoho intelektu v Ukraini na 2021–2024 roky" № 438-p* [Resolution of the Cabinet of Ministers of Ukraine "On the approval of the plan for the implementation of the Concept of Artificial Intelligence Development in Ukraine for 2021–2024" activity no. 438-p]. (2021, May 12). Retrieved from: https://surl.li/ikvfcb (accessed 13 February 2025) [in Ukrainian].

26. EUAIAct.com (2020). The EU Act of AI: Directive (EU) 2020/1828 (Artificial Intelligence Act). Retrieved from: https://www.euaiact.com (accessed 12 February 2025) [in English].

27. US Congress summaries (2020). National Artificial Intelligence Initiative Act of 2020. Retrieved from: https://surl.li/txefrv (accessed 12 February 2025) [in English].

28. The White House website (2022). Blueprint for an AI Bill of Rights. Retrieved from: https://surl.li/rquezm (accessed 12 February 2025) [in English].

29. Balovsiak N. *U Kytai zatverdzheni pravyla rehuliuvannia shtuchnoho intelektu* [China has approved rules regulating artificial intelligence]. *Internet Svoboda.* Retrieved from: https://surl.li/snhcig (accessed 12 February 2025) [in Ukrainian].

30. The United Nations Bulletin (2021). UNESCO's Ethics of AI Recommendation. Retrieved from: https://surl.lu/jonfrw (accessed 12 February 2025) [in English].

31. Google inc. (2021). Making AI helpful for everyone. Retrieved from: https://ai.google/ (accessed 12 February 2025) [in English].

32. IBM inc. (2022). Artificial Intelligence (AI) Solutions. Retrieved from: https://surl.li/sdsvqp (accessed 12 February 2025) [in English].

33. Arseniv M. V. (2022). *SShA vyrishyly, shcho shtuchnyi intelekt ne mozhe maty avtorskykh prav na svoi produkty* [The US has decided that artificial intelligence cannot have copyrights for its products]. *Sudovo-yurydychna hazeta*. Retrieved from: https://surl.li/fazoyd (accessed 12 February 2025) [in Ukrainian].

34. Krysovatyi A. I., Sokhatska O. M., Skavronska I. V., Zvarych I. Ia. et al. (2018). *Chetverta promyslova revoliutsiia: zmina napriamiv mizhnarodnykh investytsiinykh potokiv* [The Fourth Industrial Revolution: Changing the Direction of International Investment Flows]. Ternopil : Osadtsa Yu. V. Retrieved from: https://surl.li/lfcuhy (accessed 12 February 2025) [in Ukrainian].

35. Shyshka N. V. (2023). *Shtuchnyi intelekt v ukrainskomu pravosuddi: pravovi peredumovy zaprovadzhennia* [Artificial Intelligence in Ukrainian Justice: Legal Prerequisites for Implementation]. *Yurydychnyi elektronnyi zhurnal*. DOI: https://doi.org/10.32782/2524-0374/2021-3/35 [in Ukrainian].

36. Radutnyi O. E. (2018). *Subiektnist shtuchnoho intelektu u kryminalnomu pravi* [The subjectivity of artificial intelligence in criminal law]. *Pravo Ukrainy*, 2018, no. 1, pp. 123–136 [in Ukrainian].

37. White paper (2020). On Artificial Intelligence – A European approach to excellence and trust. *European Commission*. Brussels, 19.02.2020 COM (2020) 65. Retrieved from: https://surl.li/hxgqhm (accessed 12 February 2025) [in English].

38. Pavlenko Zh. O., Vodoriezova S. R. (2021). *Poniattia elektronnoi osoby v tsyfrovii realnosti* [The concept of an electronic person in digital reality]. *Visnyk NIuU imeni Yaroslava Mudroho. Seriia: philosofiia, filosofiia prava, politolohiia, sotsiolohiia,* vol. 3, no. 50, pp. 59–70 [in Ukrainian].

39. Kolodin D. O., Baitaliuk D. R. (2019). *Shchodo pytannia tsyvilno-pravovoi vidpovidalnosti za shkodu, zavdanu robotyzovanymy mekhanizmamy zi shtuchnym intelektom (robotamy)* [Regarding the issue of civil liability for damage caused by robotic mechanisms with artificial intelligence (robots)]. *Chasopys tsyvilistyky*, no. 33, pp. 87–91 [in Ukrainian].

*The article was submitted to the editorial office on 2 March 2025*

**УДК 342.9, 351, 004.8**

**В. В. Корнієнко, В. П. Гмиря, М. С. Стишук**

## ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

*Штучний інтелект має значний вплив на суспільні процеси і може бути використаний як у позитивному контексті – для зміцнення безпеки держави, так і в негативному – для її ослаблення. У військових, розвідувальних, правоохоронних та інших державних структурах штучний інтелект уже активно застосовується задля поліпшення ефективності управління, аналізу даних і виявлення загроз. З одного боку, це відкриває нові можливості, а з іншого – ставить держави й суспільства перед новими викликами, пов'язаними з етикою, контролем і потенційними ризиками.*

*Сьогодні як в Україні, так і у світі бракує чітко визначеної організаційно-правової бази для використання штучного інтелекту у сфері забезпечення державної безпеки. Саме це й зумовлює актуальність дослідження. Чинне законодавство не цілком ураховує специфіку застосування штучного інтелекту, що створює правову невизначеність та обмежує ефективність його використання.*

*У статті проведено аналіз відкритих джерел і надано пропозиції щодо подальшого нормативного врегулювання використання інструментів штучного інтелекту у сфері державної безпеки, зокрема*

*окреслено межі його застосування, відповідальність власників і користувачів за неналежне або безконтрольне використання інструментарію штучного інтелекту.*

***Ключові слова:*** *штучний інтелект, нейронні мережі, службово-бойова діяльність Національної гвардії України, державна безпека, законодавче забезпечення, кібербезпека.*

**Korniienko Vasyl** – PhD in Law Science, Associate Professor, National Academy of National Guard of Ukraine
https://orcid.org/0000-0002-7682-1281

**Hmyria Viktoriia** – PhD, Associate Professor, Leading Researcher of the Scientific and Organizational Department, State Research Institute for Testing and Certification of Weapons and Military Equipment
https://orcid.org/0000-0003-3070-0158

**Styshuk Mykhailo** – Cadet, National Academy of the National Guard of Ukraine
https://orcid.org/0009-0000-7459-2078