**DOI:** https://doi.org/10.53486/escst2023.20
International Conference, December 07-08, 2023, Chişinău, Moldova

# THE IMPACT OF MARTIAL LAW ON THE ORGANIZATION'S INFORMATION SECURITY

**Yuliia SYNYTSINA**
PhD, Associate Professor
Dnepropetrovsk State University of Internal Affairs, Ucraine
ORCID 0000-0002-6447-821X
*E-mail:ysynytsina0@gmail.com*

***Abstract:*** *The article examines the problem of the development of information and analytical activity (IAD) in domestic state and commercial institutions, which leads to the constant improvement of information security issues, which in turn is closely related to issues of economic security. Based on the results of the study, the analysis model was clarified and the practical aspects of the application of neural networks (NN) in the marketing information system (MIS) of the enterprise were clarified with the aim of improving the information system of the enterprise by implementing an intelligent decision support system (IDSS) using a neural network, as well as the concept of modeling the behavior of interacting agents, the basis of which is a three-level structure of modeling subjects and business processes of the contours of the organization's functioning and the security system, based on the modeling of the behavior of antagonistic agents. Modern trends and directions in the field of information security of state and commercial institutions of the present and the near future, which in one form or another use artificial intelligence in their arsenal, are defined, such as EDR / XDR solutions for end hosts, UEBA, SGRC products, Honey Tokens and other developments of the Deception class, IRP (Incident Response), TI- / TH-platforms, etc.*

***Keywords:*** *Artificial Intelligence, Information Technology, informational security, economic security.*

***UDC:*** *004.056:004.8*

***JEL Classification:*** *K24, F52.*

## INTRODUCTION

The rapid development of information and analytical activity (IAA) in domestic state and commercial institutions has become a characteristic trend in recent times. Its implementation is driven by certain objective factors: on the one hand, it is the democratization of social life, the development of market relations, legitimacy, the rapid development of entrepreneurial activity; on the other hand, the increasing importance of the intellectual component in decision-making in the management of social spheres, as well as the growing flow of information necessary for decision-making and the implementation of other types of social activities.

The development of information and analytical activity (IAA) in domestic state and commercial institutions leads to continuous improvement of information security issues, which is closely related to issues of economic security. The specifics of information security issues are also closely linked to the constant development of information technologies. Information technologies that incorporate modern methods of applying artificial intelligence to determine current information and economic threats are of particular importance.

The development of artificial intelligence (AI), data science, and machine learning systems already allows humanity to do what was previously only imaginable: image and speech recognition, personal identification, making complex decisions, predicting human behavior, autonomous vehicle control, and building universal routes, among other things.

Digitization, as the digital transformation of everyday things, has become so ingrained in our lives that in 2001 a new indicator of the level of development of countries in the world was introduced – the Networked Readiness Index (NRI), which is designed to characterize the degree of development of information and communication systems of a country and is an important indicator of its development and investment prospects.

Therefore, the question of the application of artificial intelligence as a tool for information security in state and commercial institutions is currently relevant.

## PAPER BODY

Over the past few years, IT technologies have been actively integrated into the business information security infrastructure. Last year, the global market volume of artificial intelligence technologies in information security reached $8 billion USD. By 2025, the growth of this industry is expected to reach $30 billion USD. This is not surprising, as most solutions in the field of information security are somehow based on artificial intelligence. Virtually any traditional antivirus utilizes some capabilities from the realms of machine learning and big data. It is no longer just local comparison of a suspicious file with the antivirus database of malware signatures. Behavioral analysis is also employed, capable of detecting dangerous objects whose signs are absent in the antivirus database, along with other advanced technologies.

Significant contributions to the study of legal issues related to the application of artificial intelligence have been made by O.A. Baranov, V.M. Bryzhko, K.S. Melnyk, V.G. Pylypchuk, and others. The role and place of artificial intelligence in the field of criminal law relations have been highlighted in the works of V.A. Myslivyi, M.V. Karchevskyi, and N.A. Savinova. However, with each restrained step of scientific research, even greater horizons of boundless reality cognition are revealed.

The principles and tasks of developing artificial intelligence technologies in Ukraine are one of the priority directions in the field of scientific and technological research. The goal of the Concept is to define the priority areas and main tasks for the development of artificial intelligence technologies to satisfy the rights and legitimate interests of individuals and legal entities, build a competitive national economy, and improve the public administration system. Ukraine, being a member of the Special Committee on Artificial Intelligence at the Council of Europe, joined the Organization for Economic Co-operation and Development (OECD) Recommendations on Artificial Intelligence (OECD/LEGAL/0449) in October 2019. The main task in the field of cybersecurity during the implementation of the state policy for the development of the artificial intelligence industry is to protect communication, information, and technological systems, information technologies, especially those used by operators (providers) of key services (including critical infrastructure objects) that are essential for the continuity of the state, society, and the safety of citizens [1]. The application of artificial intelligence technologies in ensuring information security is one of the factors that will contribute to safeguarding national interests. Specifically, monitoring social networks and online media resources using AI technologies allows for the detection of systemic trends and issues, proactive action, and analysis of target audiences.

- To achieve the goal of the Concept in this area, the following tasks should be ensured:
- Formation and use of an information resource, ensuring high rates of its content and specified criteria of quality (accessibility, reliability, timeliness,

completeness).

- Creation of a secure national information space using artificial intelligence technologies.
- Detection, prevention, and neutralization of real and potential threats related to the dissemination through mass media of cultural elements of violence, cruelty, pornography, attempts to manipulate public consciousness, including through the spread of inaccurate, incomplete, or biased information.

The application of neural networks in an intelligent decision support system at an enterprise is described in the work [2, 3]. Based on the research results, a model of analysis was formulated, and practical aspects of applying neural networks (NN) in the marketing information system (MIS) of the enterprise were considered with the aim of improving the enterprise's information system through the implementation of an intelligent decision support system (IDSS) using a neural network [2, 3]. Currently, the foundation of existing DSS lies in artificial intelligence methods. The creation of an intelligent DSS became a natural extension of the widespread use of classical DSS. Intelligent DSS provides information support to all production processes and safety processes in the conditions of state and commercial organizations and institutions.

The authors of the work [4] propose a Concept for modeling the behavior of interacting agents, the basis of which is a three-level structure for modeling the subjects and business processes within the functioning contours of the organization and security system. This concept relies on modeling the behavior of antagonistic agents. The methodology for modeling the behavior of interacting agents, based on the Concept of antagonistic agent behavior, allows for the evaluation and enhancement of security levels by reducing the implementation of hybrid threats by 1.76 times. This results in a reduction of losses by 1.65 times and an increase in the time for selecting resistance tools by reducing the identification time of threats in online mode by 38%.

In summary, all methods and solutions can be divided into external, which analyze user actions and events outside the organization's protective perimeter, and internal, which analyze events and user behavior within the organization. Both external and internal methods currently extensively utilize machine learning, big data processing, and artificial intelligence. Systems similar to those described above are critically important for many industrial enterprises, insurance, banking, and financial companies, as well as numerous critical government institutions.

The use of artificial intelligence and machine learning typically involves connectivity both within a local network and over the Internet. Consequently, these technologies cannot be applied in situations where the probability of external attackers connecting needs to be minimized, such as in critical objects of the energy infrastructure or defense production. Regarding businesses, artificial intelligence technologies are essential for both governmental and commercial institutions dealing with large volumes of data, thousands of transactions, and tens of thousands of users. It's important to note that implementing machine learning and artificial intelligence technologies within small businesses may not always be justified. Also, it's crucial to recognize that artificial intelligence is not a panacea but an additional element in the overall toolkit of information security professionals. Simply connecting an artificial intelligence service to a security system does not solve all problems, and the final decision-making authority still rests with the information security expert.

## CONCLUSIONS

In conclusion, it is worth noting that there are currently numerous trends in the application of artificial intelligence for the protection of information systems, and the relevance of many of them will actively grow in the near future. The significant shift of a vast number of people to remote work during the ongoing pandemic and military actions in Ukraine makes a substantial contribution to the development of artificial intelligence application in optimizing information security in both governmental and commercial institutions. Many organizations find themselves having to restructure information security processes and utilize new tools for the recognition of "friend or foe." The workload on information security departments in various governmental and commercial institutions is gradually increasing, indicating that additional tools, including those based on artificial intelligence, are necessary. The risks in the context of a "blurred perimeter" become significantly higher.

When discussing trends and directions in the field of information security for current and near-future use in governmental and commercial institutions, which incorporate artificial intelligence in one form or another, these include EDR/XDR solutions for end hosts, UEBA, SGRC products, Honey Tokens, and other Deception class developments, IRP (Incident Response), TI/TH platforms, etc. There is a significant variety of solutions and directions, and it is crucial to apply them wisely and consciously.

## BIBLIOGRAPHY

1. ON THE APPROVAL OF THE CONCEPT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN UKRAINE: [online] order of the Cabinet of Ministers of Ukraine dated 02.12.2020 No. 1556-r // Cabinet of Ministers of Ukraine: official. site [viewed 01 december 2023]. Available from: <https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220>
2. SYNYTSINA , Y., ABRAMOV, S., MANOLE A. Improving the information system of the enterprise through the use of neural networks. *Philosophy, economics and law review Dnipropetrovsk State University of Internal Affairs.* [online] 2022. 2(1). 127 – 138. DOI: 10.31733/2786-491X-2022-1-127-138 [viewed 01 december 2023]. Available from: <https://phelr.dduvs.in.ua/wp-content/uploads/files/2_1/Pherl-2%2C%201%202022-127-138.pdf>
3. SYNYTSINA, Y., KAUT, O., FONAREVA, T. Intelligent decision support systems in the enterprise management process. *Infrastruktura rynku*, [online] 2019. 32. [viewed 01 december 2023]. Available from: <http://www.market-infr.od.ua/journals/2019/32_2019_ukr/32.pdf>
4. MILOV, O. et al. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system. *Eastern-European Journal of Enterprise Technologies*. [online] 2020. 6(2). 30-32. DOI: 10.15587/1729-4061.2020.218660 [viewed 01 december 2023]. Available from: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85104142498&origin=resultslist>