UDC 34:004.7:355/359

K. Sporyshev

ANALYSIS OF THE REGULATORY FRAMEWORK FOR INFORMATION AND ANALYTICAL SUPPORT OF THE SECURITY FORCES OF UKRAINE: ASPECTS OF PUBLIC ADMINISTRATION

The article analyzes the current legal framework for information and analytical support of the security forces of Ukraine, as well as foreign experience in legislative approaches to information and analytical support of law enforcement agencies and special services. Improving the regulatory framework for information and analytical support of the security forces of Ukraine is key to increasing the effectiveness of national defense and security, and therefore requires a comprehensive approach, taking into account many factors that affect the security component. This is a comprehensive approach that includes legislative, technical and organizational measures.

The problematic aspects of the regulatory framework for information and analytical support of the security forces of Ukraine and ways to overcome them are identified.

Keywords: *regulatory framework, information and analytical support, security forces of Ukraine, public administration, service and combat activities, state security.*

Statement of the problem. Improving the regulatory framework for information and analytical support of the security forces of Ukraine is an important aspect of strengthening the national security and defense capabilities of the country. Information and analytical support is extremely important for the prompt response of Ukraine's security forces to internal and external threats. The relevance of the topic is due to the increasing number of information operations against Ukraine and the need to adequately counter such challenges. The development and implementation of legislative initiatives to improve the regulatory framework for information and analytical support (IAS) of the security forces of Ukraine is a critical step in ensuring national security and defense capability of the country. Consider some aspects of the impact of the regulatory framework of IAS on the effectiveness of service and combat operations of the security forces.

Legal definition and transparency. Modern, well-structured legislation provides clear rules and procedures for the operation of security forces, promoting transparency and predictability. Legal uncertainty can lead to delays in responding to threats, as well as to abuses and human rights violations.

Adaptation to modern challenges. The effectiveness of the security forces largely depends on their ability to quickly adapt to new threats: cyberattacks, hybrid warfare, terrorism, etc. A regulatory framework that does not reflect current realities significantly limits this ability.

Interagency coordination. Clear legal frameworks facilitate better coordination between different security forces and agencies, avoid duplication of functions and efforts, and optimize resource allocation.

International cooperation. Ukraine's ability to engage in international security cooperation also depends on its legal framework. The compatibility of national legislation with international standards and agreements is crucial for effective international cooperation and support.

Innovation and technology. The legal framework facilitates the introduction of new technologies and techniques into the activities of the security forces. The lack of legal mechanisms for innovation limits the use of modern technological solutions.

Harmonization with international standards. Compliance of national legislation with international norms and standards increases the effectiveness of international cooperation.

Strengthening interagency coordination. It is important to develop and implement mechanisms to strengthen cooperation between different security agencies.

To analyze the current situation of the legal framework for information and analytical support of

the security forces of Ukraine, we will identify the main problems and challenges.

Nowadays, Ukraine has a number of acts and regulations governing the activities of the security forces, including "The National Security of Ukraine Act", "The State Secrets Act", "The Combating Terrorism Act" and others. However, the dynamics of modern threats requires constant updating and supplementation of the existing regulatory framework. Many existing regulations were developed and adopted before the massive development of digital technologies, which makes them not fully adapted to the challenges of modern information security. This applies to the protection of information infrastructure, cybersecurity, and the circulation of information in the digital environment. In some cases, the current legislation contains gaps or uncertainties that make it difficult to effectively apply the state acts in practice: issues of jurisdiction, liability, and coordination between different agencies. Ukraine is actively cooperating with international organizations and integrating into international security standards, but additional efforts are needed to harmonize domestic legislation with international norms, especially in the context of cybersecurity and information space protection.

The main problems of the legal framework are its outdated nature, inconsistency with modern information security requirements, and the lack of an integrated approach to data collection, processing and analysis. Foreign experience shows that effective information and analytical support is achieved through the introduction of advanced data processing technologies, legislative support for the activities of special services and enhanced interagency cooperation. Modern IT solutions for collecting, processing and analyzing data need to be introduced, and there is a need for continuous professional development of specialists in information and analytical units.

Analysis of recent research and publications. The following scientists have made a significant contribution to the analysis of problematic issues of information and analytical support of the security and defense forces of Ukraine: O. Matsko, S. Mykus, V. Solonnikov, H. Drobakha, M. Yermoshyn, E. Smirnov, V. Shemchuk, O. Oleshchenko, O. Iokhov, V. Lisitsyn, S. Horylyshev, and others. S. Belai, O. Bondarenko, V. Yemanov and others have studied the issues of state management of security forces.

However, there has been no comprehensive study of the legal framework for information and analytical support of the security and defense forces of Ukraine.

The purpose of the article is to analyze the current regulatory framework for information and analytical support of the security forces of Ukraine, as well as foreign experience in the field of legislative approaches to information and analytical support of law enforcement agencies and special services.

Summary of the main material. Consider the main legal acts on information and analytical support of the security forces of Ukraine.

1. The Act of Ukraine "The Basic Principles of Ensuring Cybersecurity of Ukraine" [1] created a comprehensive legal framework for the protection of Ukraine's cyberspace, including the protection of critical infrastructure, personal data of citizens, and state information systems. Cybersecurity requirements for critical infrastructure operators have been established. Mechanisms for responding to cyber incidents have been developed. A national infrastructure has been created to detect and prevent cyber threats. The Cyber Security Act regulates the interaction between government agencies, the private sector and international organizations in the field of cyber security.

Ukraine pays considerable attention to strengthening its cybersecurity capabilities in the context of growing global cyber threats. The Cybersecurity Act is a key document that defines the legal and organizational framework for ensuring cybersecurity in the country, including aspects related to information and analytical support of the security forces.

The Act defines the state authorities responsible for cybersecurity, including those that provide information and analytical support to the security forces, such as the Security Service of Ukraine, the State Special Communication and Information Service, the Ministry of Defense, etc.

The Act establishes general rules for ensuring cybersecurity: development and implementation of cybersecurity rules, protection of information systems, and identification and response to cyber threats. It also outlines the mechanisms for collecting, processing and analyzing data on cyber threats, as well as developing strategic and operational analytical materials to support decisions in the field of national security and defense. The importance of international cooperation in the field of cybersecurity is recognized, including the exchange of information on cyber threats, joint exercises and the development of international cybersecurity standards. The legal norms regulating liability for cybersecurity violations were established to protect national interests and ensure the security of the information space.

2. Ensuring the protection of the information space of Ukraine from disinformation, propaganda and other information operations that may threaten national security is the purpose of the Act of Ukraine " The Principles of Information Security of Ukraine Act" [2]. It identifies the main threats to information security and mechanisms to counter them. A system of monitoring and analysis of the information space has been created. Standards have been developed for the media and other information resources for publishing and disseminating information. Responsibility for disseminating false information is established.

The Principles of Information Security of Ukraine Act, while covering the information and analytical support of the security forces, creates a legal basis for a comprehensive approach regarding the protection of Ukraine's information space. This includes not only technical and organizational activities, but also important aspects of interagency coordination, international cooperation, education, and legal regulation.

3. The Act of Ukraine "The Intelligence activity Act" [3] regulates intelligence activities in Ukraine to improve the efficiency of intelligence collection, processing and analysis. It defines the legal basis for intelligence activities, including the collection, analysis and dissemination of intelligence. It regulates the interaction of intelligence services with other state authorities and international partners, and establishes mechanisms for controlling and supervising the activities of intelligence services.

The Intelligence Activity Act defines a clear legal framework for conducting intelligence activities, the main tasks, principles and methods of intelligence, as well as the bodies authorized to conduct intelligence operations. It also regulates the classification, storage, protection and disclosure of information obtained in the course of intelligence activities in order to protect state secrets and other confidential data. It also defines the mechanisms of parliamentary and public control over the activities of the intelligence services, as well as internal procedures for monitoring and evaluating the effectiveness of intelligence work.

The Intelligence Activity Act is a key element of the national security architecture, which provides a legal and organizational framework for the effective work of the intelligence services. The role played by intelligence services in collecting, analyzing and using intelligence makes them an integral part of the information and analytical support of the security forces, thus contributing to the timely detection and neutralization of threats to national security.

4. The Act of Ukraine "The State classified information Act" [4] defines the norms for the protection of state secrets in order to adapt to modern challenges in the field of information security. It regulates the relations associated with the protection of information that constitutes a state secret and establishes the legal, organizational and technical principles of its preservation. As part of the information and analytical support of the security forces of Ukraine, the Act defines the criteria by which information can be recognized as a state secret, including information related to the defense and security of the state: military, technical, scientific intelligence data that is important for national security.

The Act establishes requirements for the protection of information, classified as a state secret, including ensuring its confidentiality, integration and accessibility. This is crucial for the effective management and use of information resources by law enforcement agencies. The Act establishes liability for the unlawful receipt, transfer, disclosure or loss of information constituting a state secret, which creates a legal basis for bringing to justice those who have violated the secrecy regime, thereby ensuring additional protection of information. It outlines the powers and responsibilities of state authorities, institutions and organizations to ensure the regime of state secrets, including the security forces. This includes the development and implementation of security measures, certification of workplaces, personnel training, etc. The Act regulates the procedure for granting access to state classified information, defines the procedures for vetting individuals and their admission to work with classified materials, which is key to the information and analytical activities of the military and special services.

Although The Act of Ukraine "The State classified information Act" is not specifically focused on the information and analytical support of the security forces, it creates a legal framework for the protection and use of information of importance to national security and defense.

5. The Act of Ukraine "The National Security of Ukraine Act" establishes the legal and organisational framework for ensuring national security and defence of the country, as well as sets the main principles of state activity in these areas [5]. Information and analytical support of the security forces of Ukraine in the context of this Act covers the following aspects.

The Act defines information security as an important component of national security, emphasising the need to protect the country's information space from external and internal threats. Specific aspects of intelligence activities are covered by the Act, which is a part of information and analytical support. It highlights the necessity to ensure effective intelligence to identify and counter potential threats to national security. The Act focuses on ensuring cybersecurity as an element of protecting the critical information infrastructure of the state and security forces, establishing the basis for countering cyber threats. The Act provides for the coordination of the activities of various security and defence forces of Ukraine, in particular through the exchange of information and analytical data to improve the efficiency of national security tasks. The Act defines the competences of the President, the Verkhovna Rada, the Cabinet of Ministers, the Ministry of Defence, the Security Service of Ukraine and other bodies in the field of national security, including information and analytical support.

The processes of informatisation of the security forces differ significantly from the market ones and require more rigorous management. Therefore, a regulatory framework should be developed for them, and informatisation should be considered as an organised process of creating optimal conditions for meeting the information needs of personnel and officials of the force management bodies through the formation and rational use of information resources in the new technological environment [6].

The security forces of Ukraine regarding information technology use the regulatory framework of the Armed Forces of Ukraine while performing assigned tasks. These issues are defined by a number of documents, among which the following should be highlighted.

1. The concept of informatisation of the Ministry of Defence of Ukraine is an important part of the strategic development of the country's military infrastructure, focused on increasing its defence capability and efficiency with the help of modern information technologies [7]. It provides a comprehensive approach to the development, integration and use of information systems and technologies in all aspects of the Armed Forces. The concept of informatisation covers the following main aspects.

Integration of information systems: creation of a unified information network that allows for effective management of resources, coordination of units and rapid exchange of data between different levels of command.

Automation of management processes: introduction of modern information and management systems to automate planning, combat management, logistics and other important aspects of the Armed Forces.

Ensuring cyber security: development and implementation of measures to protect military information systems from cyber attacks, spyware and other threats. *Development of the communication system:* modernisation and expansion of communication systems to ensure stable, uninterrupted and secure exchange of information in combat. Pe*rsonnel training:* organisation of training and professional development of military personnel in the use of modern information technologies.

Implementation of the Concept of Informatisation requires an effective legal framework, including state acts and regulations that would regulate the use of information technology in the Armed Forces, cybersecurity, protection of information and personal data, as well as standards and regulations that define technical requirements for information systems, communications, software and equipment. Directives and instructions are needed to regulate the development, implementation and operation of information systems in the military sphere. Important international agreements and cooperation that envisage Ukraine's participation in international projects and programmes for the development of military information technologies, exchange of experience and knowledge with partner countries.

The concept of informatisation of the Ministry of Defence of Ukraine is a key element of the national security and defence strategy aimed at increasing the efficiency and readiness of the military forces to act in the current environment. Its implementation requires a comprehensive approach, including improving the regulatory framework, integrating modern information technologies, ensuring cybersecurity, developing communication systems and training personnel.

2. The concept of creating a unified automated command and control system (UACCS) for the Armed Forces of Ukraine is focused on integrating all levels of command and control and all types of security and defence forces into a single information structure [6]. This should ensure effective management, rapid response to changing conditions and coordinated interaction between different units and agencies. The implementation of such a system requires a comprehensive approach to automating the management of military operations, logistics,

intelligence and other key aspects of the Armed Forces.

The concept consists of the following elements: The UACCS should integrate the various information systems and databases used in the Armed Forces, ensuring their interoperability and a single data exchange format. The main goal of the UACCS is to automate decision-making, planning, troop management and task performing control. A high level of protection against external and internal cyber threats is critical for the reliable operation of the UACCS. The system must be flexible for modification and expansion to adapt to changes in the structure of the Armed Forces and the requirements of modern combat. An important component is the creation of a unified secure communication system that would enable data transfer between all levels of command. The UACCS should ensure interaction not only within the Armed Forces, but also with other agencies, the security and defence forces of Ukraine, and international partners.

The creation of a unified automated control system for the Armed Forces of Ukraine is a strategically important task, the implementation of which will help to increase the country's defence capability, management efficiency and the effectiveness of the tasks performing. Successful implementation of this concept requires not only hardware but also software development.

3. The Regulation on Scientific and Information Activities in the Armed Forces of Ukraine defines the legal, organisational and methodological principles of conducting scientific research, development, implementation and use of scientific knowledge and information technologies in order to increase the defence and security of the state [8]. Its main aspects include: improving the efficiency of the management of the Armed Forces through the introduction of modern scientific achievements and information technologies; development of the scientific base to meet defence and security needs; optimisation of the processes of collecting, processing, storing and transmitting military information; ensuring information security in the face of modern challenges and threats.

4. The Communications and Information Systems Doctrine was developed in accordance with the requirements of the NATO Joint Publication AJP-06 "Allied Joint Doctrine for Communication and Information Systems (Edition A Version 1)" [9]. It provides general strategic guidance on the use of communication and information systems in the Armed Forces of Ukraine and other components of the defence forces during their use and training, including during joint exercises (training), etc. The doctrine introduces terminology in the field of communications and information systems compatible with the terminology adopted by NATO, describes the characteristics of communications and information systems, the concept of information management, architecture of communications and information systems, information protection and cyber defence in information and telecommunication systems, functions and tasks in relation to communications and information systems, defines general provisions for planning and application of communications and information systems, and determines aspects of interoperability of communications systems.

The National Guard, as a security force entity, has the Concept of the State Target Programme for the Development of the National Guard of Ukraine for the period up to 2020 and the Concept of the Development of the Security and Defence Sector of Ukraine, approved by the Decree of the President of Ukraine of 14.03.2016 No. 92/2016 [6, 10]. The Concept for the Development of the National Guard of Ukraine has lost its relevance, the programme has expired, and its implementation was not complete.

The Concept for the Development of the Security and Defence Sector of Ukraine is a strategic document that defines the main directions and priorities in the formation and development of the country's security and defence sector capabilities, including information and analytical support of the security forces.

The regulatory framework for the IAS of the security forces also includes a number of standards and regulations that set requirements for information protection in various areas: public administration, banking, telecommunications, etc.

1. State Standard of Ukraine DSTU 4145-2002 "Information. Information Protection. Basic terms and definitions" establishes basic terms and definitions used in the field of information protection.

2. State Standard of Ukraine DSTU ISO/IEC 27001:2015 "Information Technology. Information security. Information security management systems. Requirements" establishes requirements for information security management systems and provides recommendations for their implementation.

3. State Standard of Ukraine DSTU 3731:2001 "Information Technology. Protection of information. General Provisions" defines general provisions on information protection, in particular, the principles of information protection and basic requirements for it.

4. The Payment Card Industry Data Security Standard (PCI DSS) establishes requirements for the protection of confidential information about payment cards and other data stored and processed in payment systems.

5. ISO/IEC 27001 is an international standard that establishes requirements for an information security management system (ISMS). Although it is an international standard, its principles and practices can be adapted at the national level to ensure the protection of information in law enforcement agencies.

6. The NIST Cybersecurity Framework was developed by the US National Institute of Standards and Technology. This framework offers a structure for managing and mitigating cybersecurity risks. Ukraine could develop a similar national standard or adapt an existing one to the needs of the security sector.

These standards and regulations define the basic requirements and methods of information protection in various fields of activity in Ukraine. State institutions must comply with these requirements to ensure information security and compliance with the state act.

A study of foreign experience in the field of the regulatory framework for information and analytical support of the security forces allows us to identify best practices and innovative approaches that can be adapted and implemented in Ukraine [11]. Here are some examples.

The Patriot Act, a US Act passed after the 11 September 2001 terrorist attacks, significantly expanded the powers of US law enforcement and intelligence agencies to conduct surveillance and gather information to combat terrorism. It includes provisions that allow authorities to conduct surveillance without a court order under certain conditions. This has improved information and analytical support.

The Cybersecurity Information Sharing Act (CISA) 2015 is a act that facilitates the exchange of information on cyber threats between the US government and the private sector. The Act promotes better coordination and efficiency in detecting and responding to cyberattacks.

Israel has developed a comprehensive approach to cybersecurity that includes various legislative and regulatory initiatives. They focus on protecting critical infrastructure and strengthening national cybersecurity through cooperation between the public and private sectors. This ensures effective exchange of information and resources to counter cyber threats.

Estonia is a world leader in e-government and cybersecurity. The country has developed a number of state acts regulating data protection, cybersecurity and electronic services, thus ensuring a high level of information and infrastructure protection. Comprehensive measures are in place to protect personal data, cyber defend public services and introduce digital identifiers.

The Act that establishes the legal framework for cybersecurity in Singapore, including the protection of critical infrastructure from cyberattacks, is the Cybersecurity Act 2018. It provides for the establishment of a national cybersecurity agency to coordinate cybersecurity efforts at the national level and facilitate international cooperation.

The Bundesamt für Sicherheit in der Informationstechnik (BSI) is the German act that regulates the activities of the Federal Office for Security in Information Technology. It establishes a framework for the protection of federal information systems and promotes cybersecurity in the private sector.

These examples confirm that effective information and analytical support for security forces in the modern world requires a comprehensive approach, including updated legislation, cooperation between the public and private sectors, and international coordination.

Conclusions

Improving the regulatory framework for information and analytical support of the security forces of Ukraine is key to improving the effectiveness of national defence and security and requires a comprehensive approach, taking into account many factors that affect the security component. This comprehensive approach includes legislative, technical and organisational measures.

The current challenges facing our country require wider implementation of informatisation and digitalisation of public administration. In recent years, Ukraine has made significant steps towards digitalisation, but the pace of this process for the security forces is slow, and in the context of Russian large-scale aggression, this is one of the critical security factors.

The implementation of software and hardware in the armed forces is already underway, but the process of informatisation is poorly managed in the current environment, which leads to its low efficiency. Informatisation efforts involve large expenditures of forces and resources, so they cannot be carried out at the level of local initiatives and voluntary efforts, but require unified leadership, common conceptual approaches, coordination of efforts within departmental and national

programmes, creation of staff structures responsible for the development and use of software and hardware, and coordination with ongoing reforms and development of the armed forces. Targeted informatisation of the security forces should begin with the training process, thereby solving important tasks: laying the methodological core of the future departmental information system and creating a training base for personnel with experience in implementing information technologies in service and combat activities.

Areas for further research include the adaptation of the regulatory framework of the EU and NATO countries to the realities of the Ukrainian security forces assigned tasks performance.

References

1. *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" № 2163-VIII* [Law of Ukraine about the Basic Principles of Ensuring Cyber Security of Ukraine activity no. 2163-VIII]. (2017, May 10). Retrieved from: http://surl.li/ajfjh (accessed 10 February 2024) [in Ukrainian].

2. *Zakon Ukrainy "Pro zasady informatsiinoi bezpeky Ukrainy" № 4949* [Law of Ukraine about the Principles of Information Security of Ukraine activity no. 4949]. (2014, May 28). Retrieved from: http://surl.li/rngwy (accessed 11 February 2024) [in Ukrainian].

3. *Zakon Ukrainy "Pro rozvidku" № 912-IX* [Law of Ukraine about the Intelligence activity no. 912-IX]. (2020, September 17). Retrieved from: http://surl.li/bvgjz (accessed 11 February 2024) [in Ukrainian].

4. *Zakon Ukrainy "Pro derzhavnu taiemnytsiu" № 3855-XII* [Law of Ukraine about the State classified information activity no. 3855-XII]. (1994, January 21). Retrieved from: http://surl.li/axmgl (accessed 11 February 2024) [in Ukrainian].

5. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 2469-VIII* [Law of Ukraine about the National Security of Ukraine activity no. 2469-VIII]. (2018, June 21). Retrieved from: http://surl.li/tcsi (accessed 12 February 2024) [in Ukrainian].

6. Drobakha H. A., Oleshchenko O. A., Iokhov O. Yu. & Lisitsyn V. E. (2016). *Osnovy informatyzatsii Natsionalnoi hvardii Ukrainy* [Basics of informatization of the National Guard of Ukraine]. Kharkiv : NA NGU [in Ukrainian].

7. *Nakaz Ministerstva oborony Ukrainy "Pro zatverdzhennia Kontseptsii informatyzatsii Ministerstva oborony Ukrainy" № 650* [Order of the Ministry of Defense of Ukraine "On approval of the Concept of informatization of the Ministry of Defense of Ukraine" activity no. 650]. (2014, September 17). Retrieved from: http://surl.li/rngzr (accessed 12 February 2024) [in Ukrainian].

8. *Nakaz Ministerstva oborony Ukrainy "Polozhennia pro naukovo-informatsiinu diialnist u Zbroinykh Sylakh Ukrainy" № 385* [Order of the Ministry of Defense of Ukraine Regulations on scientific and information activities in the Armed Forces of Ukraine activity no. 385]. (2016, July 27). Retrieved from: http://surl.li/baayc (accessed 12 February 2024) [in Ukrainian].

9. *Doktryna "Zviazok ta informatsiini systemy" № 15841* [Doctrine Communication and information systems activity no. 15841/C]. (2020, July 02). *Tsentralne upravlinnia zviazku ta informatsiinykh system Heneralnoho shtabu Zbroinykh Syl Ukrainy.* Kyiv : Heneralnyi shtab Zbroinykh Syl Ukrainy [in Ukrainian].

10. *Ukaz Prezydenta Ukrainy "Kontseptsiia rozvytku sektora bezpeky i oborony Ukrainy" № 92/2016* [Decree of the President of Ukraine "Concept of development of the security and defense sector of Ukraine" activity no. 92/2016]. (2016, March 14). Retrieved from: http://surl.li/rnhbh (accessed 13 February 2024) [in Ukrainian].

11. Yemanov V. V., Sporyshev K. O. (2024). *Dosvid funktsionuvannia systemy informatsiino-analitychnoho zabezpechennia sylovykh struktur providnykh krain svitu* [Experience in the operation of the system of information and analytical support of the power structures of the leading countries of the world]. *Naukovi perspektyvy. Seriia: derzhavne upravlinnia*, vol. 1, no. 43, pp. 132–142 [in Ukrainian].

The article was submitted to the editorial office on 10.03.2024

УДК 34:004.7:355/359

К. О. Споришев

АНАЛІЗ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ УКРАЇНИ: АСПЕКТИ ДЕРЖАВНОГО УПРАВЛІННЯ

Здійснено аналіз сучасного стану нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України, а також проаналізовано закордонний досвід щодо законодавчих підходів у галузі інформаційно-аналітичного забезпечення правоохоронних органів і спецслужб. Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України є ключовим для підвищення ефективності національної оборони та безпеки, тому вимагає комплексного підходу, урахування багатьох чинників, що впливають на безпекову складову. Ідеться про комплексний підхід, який передбачає законодавчі, технічні та організаційні заходи.

Визначено проблемні аспекти нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України та шляхи їх вирішення.

Виклики сучасності, з якими стикнулася наша держава, вимагають ширшого запровадження інформатизації та цифровізації державних органів управління. Останніми роками Україна зробила значні кроки у цифровізації, але темпи цього процесу для сил безпеки замалі, а в умовах широкомасштабної агресії російської федерації це є одним із критичних безпекових чинників.

Щодо насичення військ програмно-апаратними засобами інформатизація вже відбувається, але за теперішніх умов цей процес слабо керований, що й зумовлює його низьку ефективність. Роботи з інформатизації пов'язані з великою витратою сил і засобів, тому не можуть вестися на рівні місцевих ініціатив і громадських засад, а потребують єдиного керівництва, єдиних концептуальних підходів, узгодження зусиль у межах відомчих і загальнодержавних програм, створення штатних структур, відповідальних за розроблення й застосування програмно-апаратних засобів, узгодження з реформами й розвитком військ, що відбуваються. Цілеспрямовану інформатизацію сил безпеки варто розпочинати з процесу навчання, тим самим вирішувати важливі завдання: закласти методологічне ядро майбутньої відомчої інформаційної системи, створити базу підготовки кадрів, які володіють досвідом упровадження інформаційних технологій у службово-бойову діяльність.

Напрямами подальших досліджень є адаптація нормативно-правової бази країн ЄС і НАТО до реалій службово-бойових дій сил безпеки України.

Ключові слова: *нормативно-правововa база, інформаційно-аналітичне забезпечення, сили безпеки України, органи державного управління, службово-бойова діяльність, державна безпека.*

Sporyshev Kostiantyn – Candidate of Technical Sciences, Associate Professor, Doctoral Student of Doctoral Studies and Adjuncts of the National Academy of the National Guard of Ukraine

https://orcid.org/0000-0003-4737-9698