UDC 351.86:004.9(477)

K. Sporyshev **V. Klishyn** **V. Belousov**

THE ROLE OF THE INFORMATION AND ANALYTICAL COMPONENT IN THE FIELD OF STATE SECURITY

The role and significance of information and analytical systems in ensuring the state security of Ukraine in the context of hybrid threats, cyber confrontation and dynamic development of information technologies have been studied, the essence and trends in the development of analytical support in Ukraine have been revealed, the key directions of digital transformation of the security sector have been outlined. A comparative analysis of the practical application of information and analytical systems in the field of state security of Ukraine, the United States of America and the countries of the European Union has been carried out.

A set of measures has been proposed to improve the information and analytical mechanism of public administration in the field of security, in particular, the creation of a single national analytical center, the unification of data exchange formats, the introduction of intelligent algorithms for information processing and the formation of a system for training specialists of a new generation.

Keywords: *state security, information and analytical activities, decision support systems, security forces.*

Statement of the problem. In the current conditions of hybrid threats, information wars and armed aggression against Ukraine, the issue of forming an effective state security system based on operational analysis, assessment and forecasting of situations is of particular importance. At the same time, despite the presence of a significant amount of data, the information and analytical component in the activities of security forces and public administration bodies remains insufficiently integrated, fragmented and technologically uneven [1, 2, 3]. The main problem lies in the lack of a holistic mechanism for the use of information and analytical systems to support the processes of managerial decision-making in the field of state security, which leads to a decrease in the efficiency of response to crisis situations and a decrease in the effectiveness of interaction between the subjects of the security and defense sector [3–6]. Information has become a strategic resource of the XXI century, which determines the level of national security, economic stability and political stability of the state. In the context of the intensive development of information technologies, artificial intelligence, cyber threats and disinformation campaigns, the state needs a new approach to managing security processes – based on modern information and analytical systems [6]. Strengthening the role of the information and analytical component will make it possible to create a single situational space for forecasting, monitoring and managing threats, which is critically important for improving the effectiveness of decisions of state authorities, security and defense forces. Therefore, the development of this component is a necessary condition for ensuring the state's resilience to internal and external challenges.

Analysis of recent research and publications. Problematic issues of state management of the system of information and analytical support of the security forces of Ukraine are considered in the works of such scientists as G. P. Sytnyk, S. V. Belai, K. O. Sporyshev, V. V. Yemanov, G. A. Drobakha, O. A. Oleshchenko, I. O. Kyrychenko, S. A. Gorelyshev, A. A. Poberezhnyi, O. Y. Iokhov, V. E. Lisitsyn and others.

The purpose of the article is to substantiate the role and importance of the information and analytical component in the field of state security, identify the main problems and challenges in its implementation, as well as outline the directions for improving information and analytical mechanisms to support managerial decision-making in the activities of the security forces of Ukraine.

Summary of the main material. Despite significant progress in the implementation of information and analytical technologies in the activities of state security agencies, there remain a

number of systemic problems and challenges that hinder the effective functioning of analytical systems. They can be classified according to technological, organizational, personnel, legal and security aspects.

1. Cyber threats and vulnerabilities of information systems. One of the most serious challenges of our time is the growth of the scale and complexity of cyberattacks. State and military information resources are constantly subjected to attempts of unauthorized access, destruction or modification of data [1, 3].

The main manifestations of cyber threats include:

1) penetration into critical information infrastructures;

2) creation of malware to collect or distort information;

3) DoS and ransomware attacks on analytical servers;

4) use of artificial intelligence to automate cyberattacks.

Combined information and psychological operations that combine technical breakdowns with manipulation of public opinion are especially dangerous. This requires strengthening cyber defenses, developing a national cyber resilience system, and regularly auditing security information platforms.

2. Insufficient data integration and incompatibility of information systems. Despite the active development of analytical technologies, there is still a lack of a unified interdepartmental data exchange system in Ukraine [2, 4]. Information resources belong to different departments [the Ministry of Internal Affairs (MIA), the Security Service of Ukraine (SBU), the Ministry of Defense (MoD), the National Guard of Ukraine (NGU), the State Emergency Service (SESU)], which use their own standards, formats and databases. This leads to the following problems:

– duplication or fragmentation of information;

– difficulties in uniting departmental bases into a single analytical environment;

– lack of centralized interaction protocols.

Without the creation of an interoperable analytical infrastructure with unified data exchange formats, it is impossible to ensure the full functioning of the national system of information and analytical security support.

3. Personnel shortage and uneven level of qualification of specialists. One of the key limitations is the lack of qualified analysts, IT specialists and cybersecurity specialists. Most of the existing training programs do not meet modern requirements for analytical activities, in particular in terms of working with big data, artificial intelligence, automated decision support systems. security and insufficient level of interagency training [7].

To overcome this challenge, it is necessary to create a unified system of professional development of analytical personnel, including training centers, simulation platforms and integrated educational programs in higher education institutions of the security sector.

4. Ethical and legal aspects of data use. Active implementation of analytical systems is accompanied by risks of violation of human rights to confidentiality and privacy. Processing of large amounts of personal data (including biometric, communication and behavioral data) requires clear legal regulation. The main problems in this area are:

– lack of a unified legislative framework for analytical security systems;

– insufficient transparency of information processing algorithms;

– potential for the abuse of analytical tools for political or commercial purposes.

National legislation needs to be improved in terms of regulation of artificial intelligence, cyber intelligence, personal data protection and international exchange of analytical information.

5. Technological fragmentation and lagging behind world standards. Many of the existing information systems of the security agencies of Ukraine were created autonomously, without a single architectural model. As a result, there is a heterogeneity of technical platforms, outdated databases, low server speed and limited scalability. There is also a lag behind international standards, in particular in the field of artificial intelligence, big data processing, blockchain technologies and geographic information analysis [3].

Overcoming these barriers requires a state strategy for the modernization of analytical systems based on unified technical requirements and standards for data exchange (ISO, NATO STANAG, EU INSPIRE, etc.).

6. Lack of a single center for analytical coordination. Information and analytical activities in the security sector are often distributed among different agencies that do not have a common coordination mechanism. This leads to breaks in decision-making chains, duplication of functions and loss of relevance of data.

The solution may be the creation of the National Center for Analytical Security Support, which will

accumulate data from all government agencies, form a unified picture of threats and coordinate information flows between ministries and law enforcement agencies.

7. Financial and infrastructural constraints. Most information and analytical projects in the field of security require significant investments in technical equipment, licensed software, encryption tools and data backup systems. However, limited funding and inconsistent budget support often reduce the pace of digitalization of security processes. Insufficient level of technical equipment of separate units causes uneven access to analytical resources that reduces the efficiency of responding to threats.

Solving this problem requires the creation of public and public-private support programs that will make it possible to attract technological partners, grant resources from the European Union (EU) and international cyber resilience projects.

8. The problem of "trust" and interagency interaction. Another significant obstacle is the low level of trust between individual state institutions in the exchange of sensitive information. The presence of departmental restrictions, bureaucratic procedures and fear of data leakage complicates analytical integration. To overcome it, it is necessary to introduce:

a) uniform standards for the security of information exchange;

b) access control and audit mechanisms;

c) institutional agreements on data exchange based on trust.

The development of a culture of interagency cooperation is a prerequisite for the creation of a holistic system of analytical management of state security.

Let us consider the experience of using information and analytical systems in the world.

I. The national security system of the United States of America (USA) is one of the most complex and technologically advanced in the world. It is based on an extensive network of think tanks, databases, information and communication platforms and decision support systems that cover all levels – from federal to local ones. The USA pioneered the use of information and analytical technologies in the field of defense, counter-terrorism, cybersecurity and crisis management [8].

1. The National Security Agency (NSA) and the SIGINT system. One of the most famous examples of analytical activity in the United States is the work of the National Security Agency, which collects, processes and analyzes intelligence signals (SIGINT – Signals Intelligence). The NSA's information and analytical complexes process billions of units of data received from satellites, Internet channels, telephone networks and open sources. The basis of these processes are Big Data Analyticsthat allow you to identify patterns, relationships, and potential threats. For automated information analysis, the NSA uses specialized machine learning algorithms capable of recognizing suspicious communications, identifying sources of cyberattacks, or identifying new types of malicious influences. In addition, there is an XKeyscore program that provides global search and filtering of information in real time, integrating intelligence streams from dozens of sources.

2. Federal Bureau of Investigation (FBI) and the IAFIS system [8]. In the field of homeland security, one of the key tools is the Integrated Automated Fingerprint Identification System (IAFIS), used by the FBI. It is one of the largest biometric databases in the world, containing more than 70 million records. The system provides the capability for rapid search and automatic matching of biometric data of suspects, stateless persons, or deceased individuals. Later, it was expanded into the NGI (Next Generation Identification) system, which integrates not only fingerprints but also facial images, iris scans, and other biometric identifiers. The NGI system employs artificial intelligence analytical algorithms to recognize individuals in video surveillance streams, detect anomalous behavior, and establish links between members of criminal networks.

Such systems significantly increase the efficiency of law enforcement agencies and provide comprehensive information and analytical support in the field of criminal security.

3. Cyber and Infrastructure Security Agency (CISA). In 2018, the Department of Homeland Security (DHS) created CISA (Cybersecurity and Infrastructure Security Agency), which is responsible for monitoring, analyzing, and protecting critical infrastructure in the United States from cyber threats. A central part of its activities is the National Center for Cybersecurity and Communications, which uses the Einstein 3 Accelerated and Continuous Diagnostics and Mitigation (CDM) analytical platforms. Einstein 3 Accelerated is a system for in-depth analysis of network traffic that automatically detects malicious activity, security breaches, and unauthorized actions in government information networks. The CDM system, in turn, provides constant assessment of cyber risks, collection of metrics from hundreds

of federal systems, and the generation of analytical reports for DHS management. Thanks to these systems, the United States is able to carry out proactive analysis of cyber threats and coordinate actions between public and private entities in real time.

4. Central Intelligence Agency (CIA) and DCGS system. The U.S. Central Intelligence Agency actively uses information and analytics platforms for strategic forecasting, risk analysis, and operational decision support. One of the key tools is the Distributed Common Ground System (DCGS), which is also used by the U.S. military. With the help of DCGS, analysts can create operational situational pictures, conduct in-depth analysis of objects and trends, as well as predict possible scenarios of enemy actions. The system supports the joint work of analysts in different time zones, providing access to up-to-date data in real time [8].

5. Homeland Security Information Network (HSIN) system. The HSIN system is a key information and analytical environment of the US Department of Homeland Security, enabling interaction between federal, regional and local agencies. It is a secure platform for the exchange of analytical information, through which thousands of operational messages, analytical reports and situation reports pass every day. This system allows users to create virtual situational centers, conduct collaborative discussions during crises, and coordinate actions among police, emergency response services, border authorities, and other agencies. In crisis events (e.g. during natural disasters or terrorist threats), HSIN integrates with geographic information analysis (GIS) systems to display risk maps, evacuation routes and rescue resources [8].

6. National Counterterrorism Center (NCTC). After the terrorist attacks of September 11, 2001, the United States created the National Center for Counterterrorism, which combined analytical resources of intelligence, the army, diplomatic and law enforcement agencies. This center functions as a single analytical platform for countering terrorism, aggregating data from more than 20 sources, including from the NSA, CIA, FBI, Pentagon and the State Department. The system uses artificial intelligence tools to build social graphs connections between suspects, analysis of financial transactions and prediction of possible terrorist acts. Thanks to analytical algorithms, NCTC can automatically identify "anomalous behavioral patterns" in large data streams, which makes it possible to prevent crime in the early stages [8].

7. FEMA Crisis Management Systems. The Emergency Management Agency (FEMA) uses a powerful information and analytics platform to predict, respond and recover from natural disasters. The HURREVAC analytical system makes it possible to assess hurricane trajectories, the extent of possible destruction and the need to evacuate the population. EMMA (Emergency Management Mission Area) platform integrates data from local departments, meteorological services, satellite systems, and drones, creating a real-time operational situational picture. These analytical solutions make it possible to effectively coordinate the work of rescuers, predict resource needs, and minimize human losses during disasters.

II. The European Union is one of the most technologically advanced regions of the world in the field of security, analytics and exchange of information between member states. The basis of the European security architecture is integrated information and analytical systems that provide threat monitoring, coordination of operational actions, risk analysis and strategic forecasting in the field of internal and external security.

The European Union is actively forming a single information and analytical security space, which combines the activities of agencies, national intelligence services, police structures and diplomatic institutions. This space was created on the basis of interagency cooperation, cyber resilience and respect for the principles of personal data protection.

1. Europol – European Police Office. One of the key think tanks of the EU is Europol, which is headquartered in The Hague (Netherlands). Its main function is to collect, analyze and disseminate operational information between the national police of the member states. Europol's work is based on the Unified Information and Analytical Platform (EIS – Europol Information System), which provides centralized storage and processing of data on criminal groups, financial flows, cybercrimes, illegal migration and terrorist activities [9, 10].

This platform allows EU countries to carry out joint threat analysis and coordinate actions in real time. Europol analysts use data mining algorithms (link analysis) to identify links between events, personalities and cross-border criminal networks. An important component is also the AP (Analysis Project) analytical platform, within which thematic modules are created (for example, AP Terrorism, AP Cybercrime, AP Fraud, AP Drugs). Each

module provides an opportunity to conduct separate analytical studies, form risk profiles, and support operational decisions at the level of national police.

2. Schengen Information System (SIS II). The Schengen Information System is the largest Europe-wide database that provides security control within the Schengen area. The system contains more than 100 million records of wanted persons, vehicles, weapons, documents, migration violations, etc. It is used by police, border guards, customs and judicial authorities of all EU member states. The SIS II system operates in real time, providing automatic interaction between the national information centers (N.SIS) and the central system (C.SIS) located in Strasbourg [9, 10].

The system is complemented by analytical modules that make it possible to carry out a risk analysis of the movement of persons, determine possible routes of illegal migration, and track the movement of vehicles that may be associated with criminal activity. In practice, SIS II has become a key tool for preventing terrorist acts, investigating cross-border crimes and strengthening control over the EU's external borders.

3. European Border and Coast Guard (Frontex). The Frontex agency, established in 2004, uses a high-tech situational monitoring system EUROSUR (European Border Surveillance System). EUROSUR is a platform that integrates data from satellites, radars, sensors, unmanned aerial vehicles, maritime and terrestrial observation posts. The aim of the system is to provide a holistic view of the situation at the EU's external borders and to contribute to the prevention of illegal migration, smuggling and maritime disasters.

EUROSUR has a multi-level structure [9, 10]:

1) national focal points collect data at the state level;

2) regional hubs carry out comparative analysis and forecasting;

3) the central level of Frontex forms an analytical picture on a pan-European scale.

EUROSUR analytical modules allow you to simulate possible scenarios of migration crises, calculate risks and plan the distribution of response forces.

4. European Center for Combating Cybercrime. Europol has the European Cybercrime Centre, which is the main analytical hub in the field of cybersecurity. This centre monitors cyber incidents in EU member states, conducts forensic analysis of malware, coordinates operations to detect cybercriminals and hacker groups. The system uses the Threat Intelligence Platform, which ensures the exchange of data between police structures, CERT centers, financial institutions and IT companies.

A special role is played by Big Data analysis and automated correlation detection, for example, determining the relationships between cyber incidents, domains, IP addresses, and digital artifacts. This makes it possible not only to investigate crimes, but also to prevent massive cyberattacks on critical infrastructure [9, 10].

5. Integrated Think Tanks in the Field of Terrorism (CTG, INTCEN). After the terrorist attacks in London (2005) and Brussels (2016), the EU intensified the creation of interstate analytical structures, such as the Counter Terrorism Group (CTG) and the EU Intelligence and Situation Centre (INTCEN). These institutions exchange intelligence information between the intelligence services of the member states and conduct joint analytical analysis of terrorist threats.

The INTCEN structure, which operates under the European External Action Service (EEAS), functions as a strategic think tank that processes data from diplomatic missions, military structures, open sources and special services. Its specialists produce analytical reports, risk assessments, warnings, and forecasts for EU leadership. The CTG focuses on the operational analysis of terrorist threats, data exchange between national agencies, and the coordination of joint operations.

Together, these structures create an information and analytical framework of the EU's anti-terrorist policy, based on the principles of shared responsibility and mutual exchange of information.

6. Information and analytical system of the European External Action Service. The European External Action Service uses the EU Open Source Intelligence (EU OSINT) system, a tool for collecting and analyzing open data to monitor geopolitical processes. The system integrates analytics from social networks, media, geolocation services and satellite observations. Based on it, the European Security Analytical Bulletin is compiled, which contains assessments of crisis regions, potential conflicts, and risks to the energy or economic stability of the EU [9, 10].

III. In Ukraine, information and analytical systems are actively used in the activities of security and defense agencies. For example, as part of the fight against cyber threats, modern systems for monitoring and analyzing network traffic are used, which allows detecting and neutralizing cyberattacks in real time. The modern system of state security of Ukraine is at the stage of active digital transformation, when information and analytical technologies are becoming not only an

auxiliary, but also a determining factor in the effectiveness of the activities of security, defense, internal affairs and civil protection agencies. Below are a number of examples of practical use of such systems, demonstrating the diversity of their functions, levels of integration and areas of application [2, 6].

1. National Guard of Ukraine. In recent years, elements of information and analytical support of service and combat activities have been actively introduced in the structure of the National Guard of Ukraine. In particular, there are operational and analytical centers that monitor the current situation in the areas of responsibility, collect data from units, unmanned aerial vehicles, video surveillance systems and open sources (OSINT).

Based on this data, a situational picture is formed, which allows commanders to quickly assess risks, plan the actions of units and predict possible scenarios for the development of events.

Such think tanks are integrated with combat unit management and communication systems, which significantly reduces the time between receiving information and making a decision. Software modules are being developed to automate data analysis using elements of artificial intelligence, for example, to detect suspicious objects in a video stream or determine the likely directions of movement of sabotage groups.

2. The ArmyInform system and the Center for Strategic Communications. Information and analytical tools are used not only in military administration, but also in the field of information countermeasures.

An important role is played by the Center for Strategic Communications and Information Security under the Ministry of Culture and Information Policy of Ukraine. The Center provides monitoring of the information space, detection of disinformation campaigns, formation of analytical reports and forecasts on information influences from the aggressor states [2, 6].

The ArmyInform system, for its part, uses algorithms of content analysis and semantic data processing to identify trends in public discourse about the Armed Forces of Ukraine. This makes it possible to respond to information attacks in a timely manner, coordinate the communication policy of the defense sector and form a positive image of the security forces.

3. The Unified State System of Cyber Defense (State Special Communications Service). An important example is the creation and development of the National Coordination Center for Cybersecurity (NCCC) under the National Security and Defense Council of Ukraine.

This center collects, analyzes and summarizes information about cyber incidents, as well as coordinates interaction between government agencies, military formations and the private sector.

The information and analytical systems of the NCCC contain modules for monitoring network traffic, automatic detection of malicious influences, forecasting potential attacks and assessing the level of cyber resilience of critical infrastructure.

As part of the Cyber Rapid Response Teams initiative, together with EU partners, a Threat Intelligence Sharing platform has been created, which makes it possible to detect and neutralize threats in real time.

4. Analytical system "Situation Center of the Ministry of Internal Affairs". The system of the Ministry of Internal Affairs of Ukraine has a Unified Analytical Platform of the Ministry of Internal Affairs, which combines databases of the National Police, the State Border Guard Service, the National Guard, the State Emergency Service of Ukraine and other structures.

The system allows you to carry out an integrated analysis of the operational situation, predict the occurrence of crisis situations, identify crime "hot spots", and coordinate interagency actions.

A feature of this platform is the use of geographic information technologies that provide spatial display of events, patrol routes, control zones and risk areas. In practice, this makes it possible to respond faster to offenses and more rationally distribute forces and means of security.

In addition, the system supports machine learning algorithms to identify patterns in criminal events and build prediction models.

5. Analytical systems of intelligence and defense analysis. The Defense Forces of Ukraine actively use information and analytical systems of the "Delta" type, developed by the Center for Innovation and Development of Defense Technologies of the Ministry of Defense [2, 6].

This system is an integrated geographic information platform that makes it possible to combine data from unmanned aerial vehicles, satellite images, radar equipment, social networks and open sources.

It provides commanders with up-to-date operational information about the situation on the battlefield, allows you to track the movement of the enemy in real time, analyze and predict the combat situation.

The system has a high level of compatibility with NATO partner platforms, which increases the efficiency of international interaction and data exchange.

In fact, Delta has become an example of a successful combination of national analytical solutions and international technological standards.

6. Use of information and analytical systems in the field of civil protection. The State Emergency Service of Ukraine actively uses emergency monitoring systems that integrate data from meteorological stations, geodata, sensor networks and mobile applications of citizens.

Systems such as "Rescuer" and "Situation Center of the State Emergency Service" provide operational visualization of scenes, coordination of actions of rescue units, assessment of the scale of threats and forecasting the development of emergency situations.

Particular attention is paid to the creation of intelligent analytical models that, based on historical data, make it possible to assess the risks of natural disasters or man-made accidents [2, 6].

7. Integration of analytical solutions into the system of public administration. At the government level, the Unified Information and Analytical System "Safe Country" has been created, which unites the information resources of various ministries and services. This system makes it possible to carry out a comprehensive assessment of the state of national security, model the impact of economic, social and military factors, form analytical reports for government structures and the National Security and Defense Council.

As part of the digital transformation, analytical modules are being introduced in the Diia and Trembita platforms, which create prerequisites for the formation of a unified information environment for state security.

The practical implementation of information and analytical systems in Ukraine demonstrates a gradual transition from disparate information resources to integrated analytical platforms that provide not only data processing, but also support for strategic management in the field of security.

At the same time, interoperability problems of interagency systems, a lack of qualified analysts and the need to create uniform standards for data exchange remain. Further development of these systems should be based on the principles of interagency integration, cyber resilience, the use of artificial intelligence, and international cooperation.

Information and analytical activities in the field of security include a set of processes of collecting, processing, analyzing and disseminating information necessary for making managerial decisions. It contains:

1) collection of information from various sources: open, closed, technical, intelligence;

2) processing and systematization of data for further analysis;

3) analysis of information using modern methods and technologies;

4) forecasting possible threats and scenarios for the development of events;

5) development of recommendations for management and safety bodies.

The information and analytical component in the security system performs the following main functions [2, 6]:

1) monitoring of the situation: constant monitoring of internal and external factors that may affect security;

2) threat forecasting: assessment of the likelihood of crisis situations and their possible consequences;

3) decision support: providing analytical materials for informed management decisions;

4) evaluation of the effectiveness of security measures: analysis of the results of the implemented measures and adjustment of the security strategy.

Modern technologies have significantly improved the efficiency of information and analytical activities. The main methods and technologies include:

– big data: processing large amounts of information to identify patterns and trends;

– artificial intelligence: using machine learning algorithms to automate data analysis;

– geographic information systems: visualization and analysis of spatial information to assess the situation;

– decision support systems: tools for modeling different scenarios and evaluating their consequences.

The directions of further development of the information and analytical component of the state security system can be considered:

1) integration of the latest technologies: the use of blockchain technologies to ensure data integrity, the development of quantum computing to increase the speed of information processing;

2) international cooperation: expanding data exchange and coordination of actions between countries and international organizations;

3) educational programs: training of personnel through specialized training programs and advanced training of existing specialists.

Conclusions

The information and analytical component is an integral part of the modern security system. It ensures timely detection of threats, informed decision-making, and effective coordination of actions between different structures. The successful development of this component requires the integration of the latest technologies, the training of qualified personnel and international cooperation.

The experience of the United States shows that information and analytical systems are the core of national security and a key factor in rapid response to threats of any nature – military, cybernetic, terrorist or natural. They combine big data, artificial intelligence, biometrics, satellite monitoring and network analytics technologies into a single security management system. By adapting this experience, Ukraine can create an integrated multi-level system of analytical support for decisions in the security sector, focused on interagency interaction, cyber defense and operational coordination.

The experience of the European Union shows that an effective security system is based on network interaction and a common analytical environment. The European Union has achieved significant results in creating interoperable information and analytical systems covering law enforcement, border, cyber and foreign policy spheres.

Therefore, the effective functioning of the information and analytical component in the field of state security requires a comprehensive solution of a number of problems – from technological and personnel to legal and coordination. Overcoming these challenges is possible only with institutional integration, innovative renewal, development of analytical culture and interagency cooperation.

We see the prospects for further research in the analysis and development of interagency cooperation between the subjects of the security and defense forces of Ukraine, the study of opportunities for institutional integration of the information and analytical component in the field of state security.

References

1. Sytnyk H. P. (2011). *Derzhavne upravlinnia u sferi natsionalnoi bezpeky (kontseptualni ta orhanizatsiino-pravovi zasady)* [Public Administration in the Field of National Security (Conceptual and Organizational-Legal Foundations)]. Kyiv : NADU [in Ukrainian].

2. Sporyshev K. O. (2024). *Informatsiino-analitychni tekhnolohii syl bezpeky u paradyhmi derzhavnoho upravlinnia* [Information and Analytical Technologies of Security Forces in the Paradigm of Public Administration]. *Naukovi innovatsii ta peredovi tekhnolohii. Seriia: upravlinnia ta administruvannia*, no. 1 (29), pp. 128–136 [in Ukrainian].

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

4. Bielai S. V., & Sporyshev K. O. (2024). *Vplyv stanu systemy informatsiino-analitychnoho zabezpechennia syl bezpeky Ukrainy na derzhavnu bezpeku* [Influence of the State of the Information and Analytical Support System of Ukraine's Security Forces on State Security]. *Naukovi innovatsii ta peredovi tekhnolohii. Seriia: upravlinnia ta administruvannia*, no. 2 (30), pp. 29–37 [in Ukrainian].

5. Kyrychenko I. O., Horielyshev S. A., & Poberezhnyi A. A. (2013). *Tekhnolohichni osnovy informatsiino-analitychnoho zabezpechennia sluzhbovo-boiovoi diialnosti syl okhorony pravoporiadku* [Technological Bases of Information and Analytical Support of Law Enforcement Activities]. Kharkiv : Acad. VV MVS Ukrainy [in Ukrainian].

6. Bielai S. V., & Sporyshev K. O. (2024). *Systemy pidtrymky pryiniattia rishen u derzhavnomu upravlinni sylamy bezpeky Ukrainy* [Decision Support Systems in Public Administration of Ukraine's Security Forces]. *Aktualni pytannia u suchasnii nautsi. Seriia: derzhavne upravlinnia*, no. 2 (20), pp. 320–329 [in Ukrainian].

7. Sporyshev K. O. (2024). *Rozvytok menedzhmentu kadrovykh resursiv v systemi informatsiino-analitychnoho zabezpechennia syl bezpeky Ukrainy* [Development of Human Resource Management in the System of Information and Analytical Support of Ukraine's Security Forces]. *Aktualni pytannia u suchasnii nautsi. Seriia: derzhavne upravlinnia*, no. 3 (21), pp. 410–421 [in Ukrainian].

8. U.S. Department of Homeland Security (CISA) (2023). Cybersecurity Strategic Plan 2023–2027. Washington, D.C. : DHS [in English].

9. European Union Agency for Cybersecurity (ENISA) (2024). Threat Landscape 2024 Report. Brussels : ENISA Publications [in English].

10. Europol (2024). European Union Serious and Organised Crime Threat Assessment (SOCTA 2024). The Hague : Europol Press [in English].

The article was submitted to the editorial office 24.10.2025

УДК 351.86:004.9(477)

К. О. Споришев, В. М. Клішин, В. Л. Белоусов

РОЛЬ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО СКЛАДНИКА У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ

Досліджено роль і значення інформаційно-аналітичних систем у забезпеченні державної безпеки України в умовах гібридних загроз, кібернетичного протистояння та динамічного розвитку інформаційних технологій. Наголошено, що сучасні безпекові процеси неможливі без системного збирання, аналізу, прогнозування та інтерпретації даних, які формують основу для прийняття обґрунтованих управлінських рішень у кризових ситуаціях. Визначено основну проблему – брак цілісного механізму використання інформаційно-аналітичних систем у діяльності сил безпеки, що призводить до фрагментарності даних і зниження ефективності реагування на загрози.

У праці розкрито сутність і тенденції розвитку аналітичного забезпечення в Україні, окреслено ключові напрями цифрової трансформації сектору безпеки. Проведено порівняльний аналіз практичного застосування інформаційно-аналітичних систем у сфері державної безпеки України, Сполучених Штатів Америки та країн Європейського Союзу. Особливу увагу приділено аналізу основних проблем і викликів – кіберзагроз, кадрового дефіциту, технологічної фрагментованості, правових обмежень і недостатньої інтеграції інформаційних ресурсів між відомствами. Підкреслено важливість розвитку систем кіберстійкості, міжвідомчої взаємодії та аналітичної культури прийняття рішень.

У підсумку запропоновано комплекс заходів із удосконалення інформаційно-аналітичного механізму державного управління у сфері безпеки, зокрема створення єдиного національного аналітичного центру, уніфікацію форматів обміну даними, впровадження інтелектуальних алгоритмів оброблення інформації та формування системи підготовки фахівців нового покоління. Отримані результати мають практичне значення для оптимізації управлінських процесів у секторі безпеки та підвищення ефективності державного реагування на сучасні загрози.

Ключові слова: *державна безпека, інформаційно-аналітична діяльність, системи підтримки прийняття рішень, сили безпеки.*

Sporyshev Kostiantyn – Doctor of Science in Public Administration, Associate Professor, Deputy Head of the Educational and Scientific Institute for Training of Management Personnel in Scientific Work – Head of the Scientific and Research Laboratory of Construction and Operational Application of the National State University, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0003-4737-9698

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

Belousov Volodymyr – Adjunct, National Academy of the National Guard of Ukraine
https://orcid.org/0009-0009-8550-2694