

Міжнародна науково-практична конференція

«Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку»

27 березня 2025 року, м. Харків



Міжнародна науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» / Збірник тез доповідей (м. Харків, 27 березня 2025 р.). – Харків. – 2025. – 256 с.

Організатори конференції: Національна академія Національної гвардії України (м. Харків); Харківський національний університет радіоелектроніки (м. Харків).

Організаційний комітет конференції:

Голова – Іохов О.Ю., начальник Центру імітаційного моделювання Національної академії Національної гвардії України, доктор технічних наук, професор.

Заступник голови – Малюк В.Г., доцент кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України, кандидат технічних наук, доцент.

Відповідальний секретар – Новикова О.О., професор кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України, кандидат технічних наук, доцент.

Члени організаційного комітету:

Споришев К.О. – заступник начальника Центру імітаційного моделювання Національної академії Національної гвардії України, доктор технічних наук, доцент;

Яковлєв С.В. (Yakovlev S.) – професор Institute of Information Technology, Lodz University of Technology (м. Лодзь, Польща), заступник директора навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету ім. В.Н. Каразіна, член-кореспондент НАН України, доктор фізико-математичних наук, професор;

Безкоровайний В.В. – професор кафедри системотехніки Харківського національного університету радіоелектроніки, доктор технічних наук, професор;

Смеляков К.С. – завідувач кафедри програмної інженерії Харківського національного університету радіоелектроніки, доктор технічних наук, професор;

Дудар З.В. – професор кафедри програмної інженерії Харківського національного університету радіоелектроніки, кандидат технічних наук, професор;

Кобзєв В.Г. – професор кафедри програмної інженерії Харківського національного університету радіоелектроніки, кандидат технічних наук, с.н.с.

Адреса організаційного комітету: 61001, м. Харків, майдан Захисників України, 3, Національна академія Національної гвардії України, науково-організаційний відділ.
Телефон: +38097-69-81-250. **Електронна адреса**: nanguki@ukr.net.

Тези доповідей опубліковано в авторській редакції, мовою оригіналу: **http://kinf.nangu.edu.ua**

Відповідальність за фактичні помилки, зміст і достовірність інформації та точність викладених фактів несуть автори.

© Національна академія Національної гвардії України, 2025



Ministry of Internal Affairs of Ukraine
National Academy of the National Guard of Ukraine

Ministry of Education and Science of Ukraine
Kharkiv National University of Radio electronics



International scientific and practical conference

«Application of information technologies in the preparation and operation of law enforcement forces»

March 27, 2025

Kharkiv

International scientific and practical conference «Application of information technologies in the preparation and operation of law enforcement forces» / Collection of theses of reports (Kharkiv, March 27, 2025). – Kharkiv. – 2025. – 256 p.

Conference organizers: National Academy of the National Guard of Ukraine (Kharkiv), Kharkiv National University of Radio Electronics (Kharkiv).

Organizing committee of the conference:

Chairman – Iokhov O.Yu., Head of the Simulation Modeling Center of the National Academy of the National Guard of Ukraine, Doctor of Technical Sciences, Professor.

Deputy Chairman – Malyuk V.G., Associate Professor of the Department of Military Communications and Informatization of the National Academy of the National Guard of Ukraine, Candidate of Technical Sciences, Associate Professor.

Executive secretary – Novykova O.O., Professor of the Department of Military Communications and Informatization of the National Academy of the National Guard of Ukraine, Candidate of Technical Sciences, Associate Professor.

Organizing Committee Members:

Sporyshev K.O. – Deputy Head of the Center for Simulation Modeling of the National Academy of the National Guard of Ukraine, Doctor of Technical Sciences, Associate Professor;

Yakovlev S.V. – Professor of the Institute of Information Technology, Lodz University of Technology (Lodz, Poland), Deputy Director of the Educational and Scientific Institute of Computer Sciences and Artificial Intelligence of the V.N. Karazin Kharkiv National University, Corresponding Member of the NAS of Ukraine, Doctor of Physical and Mathematical Sciences, Professor;

Bezkorovaynyi V.V. – Professor of the Department of Systems Engineering of the Kharkiv National University of Radio Electronics, Doctor of Technical Sciences, Professor;

Smelyakov K.S. – Head of the Department of Software Engineering of the Kharkiv National University of Radio Electronics, Doctor of Technical Sciences, Professor;

Dudar Z.V. – Professor of the Department of Software Engineering of the Kharkiv National University of Radio Electronics, Candidate of Technical Sciences, Professor;

Kobzev V.G. – Professor of the Department of Software Engineering of the Kharkiv National University of Radio Electronics, Candidate of Technical Sciences, Senior Researcher.

Organizing committee address: 61001, Kharkiv, Maidan Defenders of Ukraine, 3, National Academy of the National Guard of Ukraine, scientific and organizational department.
Phone: +38097-69-81-250 (Iokhov O.Yu.). **Email:** nanguki@ukr.net.

Theses of reports are published in the author's edition, in the original language: **http://kinf.nangu.edu.ua**

The responsibility for factual errors, the content and reliability of information and the accuracy of the facts presented are carried by the authors.

© National Academy of the National Guard of Ukraine, 2025

UDC 621.396

Bordunova K.

PROBLEMS OF USING FREQUENCY HOPPING SPREAD SPECTRUM (FHSS) SIGNALS IN UAV CONTROL CHANNELS

The use of FHSS signals (Frequency Hopping Spread Spectrum based on pseudorandom frequency sequences) in the data transmission channels of unmanned aerial vehicles (UAVs) offers several advantages such as enhanced protection against interception, resistance to interference, and resilience against electronic warfare (EW). However, in practice, a number of issues arise that limit the effectiveness of this method in combat or complex environments.

Key Problems of FHSS Use in UAVs:

1. Synchronization Complexity. Effective FHSS operation requires that the transmitter and receiver synchronously switch frequencies according to the same pseudorandom sequence. This creates difficulties during rapid UAV deployment, changes in environmental conditions, or loss of connection (e.g., under EW impact). In mobile conditions (changing altitude, antenna orientation, latency), synchronization can be lost.

2. Transmission Delays. Due to constant switching between frequencies, FHSS systems may experience packet delays and losses—especially when the hopping intervals are short (2–10 ms). This is critical for real-time UAV control or live video streaming.

3. Limited Bandwidth. FHSS reduces the effective channel width due to the necessity of frequent hops and packet repetitions. In high data rate scenarios (HD video, telemetry, sensors), the FHSS channel may become overloaded. Alternatives like DSSS (Direct Sequence Spread Spectrum) or OFDM offer higher throughput.

4. Implementation Complexity in Compact UAVs. Reliable FHSS implementation requires sophisticated radio hardware, high-frequency oscillators, and precise synchronization. For small/portable UAVs, this may be too energy-consuming or physically impractical.

5. Pattern Detection Risk (in case of poor implementation). If the pseudorandom sequence is poorly generated, an adversary may spectrally identify frequency patterns and jam or intercept the channel. Inadequate PRNGs (e.g., not based on Galois fields) create spectral repetitions detectable by SDR analysis tools.

6. Vulnerability to Electronic Warfare (EW). While FHSS resists wideband interference, modern EW systems can analyze the spectrum in real-time (e.g., using SDRs) and begin frequency-following jamming. Under conditions of high jamming power, FHSS may prove ineffective without additional protective measures.

Potential Solutions:

– use of quantum-safe or cryptographically secure PRNGs to improve hopping entropy;

– implementation of adaptive frequency hopping based on interference levels, allowing UAVs to dynamically change hopping strategies;

– combining FHSS with DSSS or AES encryption to increase channel protection;

– transition to software-defined radios (SDRs) for flexible protocol switching during flight;

– use of laser communication or MIMO OFDM (e.g., Starlink or 5G NR) in complex or long-range operations.

While FHSS provides a basic level of protection for UAV data links, its effectiveness largely depends on implementation methods, system parameters, and the operating environment. In the context of modern warfare, especially as seen in Ukraine, the efficient use of FHSS requires integration with other communication security methods and the application of intelligent frequency management protocols.

UDC 681.5.015

Dyadun S.

INFORMATION SYSTEM FOR MODELING AND CONTROL OF THE FUNCTIONING OF THE CITY'S GAS SUPPLY NETWORK

The current state of the gas industry requires guarantees of operational safety and improvement of control of gas supply processes by minimizing energy and raw material costs while adhering to the supply plan. To achieve these goals, an automated technological process control system is being developed and put into operation, which requires the development of effective mathematical models.

The city gas supply system is designed to transport and distribute gas between consumers. This system is a hierarchical structure and at each level of the hierarchy has a distribution network of appropriate complexity. To determine the control object, it is necessary to identify one or more control objectives. Qualitative and quantitative objectives are distinguished.

The qualitative objective of control city gas supply systems is characterized by their functional purpose and consists in providing consumers with gas in the required quantities and in a given pressure range.

The quantitative goal of control the city's gas supply systems is achieved at different values of technical indicators that determine the state of the system and depend on the values of the controlled variables. Quantitative control goals are designed to reduce (or increase) the values of some parameters (optimization criteria) that characterize the operating modes of the city's gas supply system.

Control is considered in normal conditions, control in the conditions of gas shortage, control in emergency situations.

Control under normal conditions occurs when the amount of gas needed by the city for a given period of time does not exceed the supply. The qualitative goal of management is achieved in this case. Such implementation of control allows reducing gas leaks in the network, its overconsumption by consumers, and the likelihood of emergency situations in the network.

Control under gas shortage conditions occurs when the amount of gas needed by the city for a planned period of time exceeds the amount that its supplier can allocate. The qualitative goal of control is not achieved in this case. In this case, the control task is divided into two stages:

– the task of optimal selection of the gas restriction for consumers with minimization of national economic damage, which is an optimization criterion;

– the task of planning (for the remaining consumers) flow distribution of gas in the network according to the criterion of minimum total excess pressures at the inputs of consumers.

Control in emergency situations occurs in the event of a failure (accident) of a linear section of the gas network, which leads to significant losses due to direct gas losses, changes in the operating modes of gas supply systems, the occurrence of a gas shortage in the system and, in the worst case, an explosion of the gas-air mixture. In this case, the qualitative goal can in some cases be achieved after the localization of the emergency section in the presence of a known structural redundancy of the network. In this case, the control task is divided into three stages:

1) the task of identifying the location of the emergency situation according to the control criterion, which is the minimum time for detecting the emergency situation;

2) the task of rational localization of the emergency section;

3) the task of planning (for the network structure resulting from the solution of the problem of the previous stage) flow distribution in the network according to the criterion of minimum total excess pressure at the inputs of consumers.

The existence of a reliable comprehensive tool for assessing and predicting the technical condition of gas supply systems, which takes into account qualitative and quantitative management objectives, increases the reliability of such systems.

The capabilities of modern software and mathematics allow significantly simplifying and accelerating decision-making procedures in the process of rational operation and development of gas supply systems. Solving such a problem requires the use of various mathematical models of gas distribution networks, various volumes of static (normative and reference) and dynamic (operational) data and is carried out in different time intervals.

The information system for modeling and operational control the functioning of the city's gas supply system in normal conditions, in conditions of gas shortage and in emergency situations is considered. This information system allows for calculations of optimal flow distribution and efficiency indicators for comparing options, simulation of various emergency situations, modeling different operating modes and parallel calculation of integral indicators of the quality of functioning of the city's gas distribution network.

Iokhov O., Ishchuk O.

PROPOSALS FOR THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE INTO THE JCATS SIMULATION SYSTEM

The integration of artificial intelligence (AI) into simulation systems such as JCATS (Joint Conflict and Tactical Simulation) opens new opportunities for enhancing realism, automation, analytical value, and adaptability in military exercises, research, and commander training.

What does AI bring to JCATS?

Intelligent agents AI allows replacing scripted unit behavior with autonomous agents that can:

– make decisions based on the current tactical situation;
– assess threats;
– choose targets and routes;
– coordinate actions within a group.

For example, an AI-controlled infantry platoon can independently select firing positions, maneuver under fire, and request support.

Adaptive enemy behavior AI modules make it possible to create a dynamic and unpredictable adversary that:

– responds to user actions;
– learns (e.g., via reinforcement learning);
– simulates the tactics of a specific army or doctrine.

Prediction and optimization AI can analyze large volumes of JCATS data in real time to:

– suggest optimal movement routes and force distribution;
– estimate the probability of success of tactical decisions;
– identify weaknesses in the user’s strategy.

Adaptive scenario (dynamic scripting) AI can dynamically alter scenario conditions (e.g., deploy unexpected maneuvers or reinforcements), which is useful for stress-testing commanders and adaptive training.

How to implement AI in JCATS.

Integration via interfaces (API / HLA) JCATS supports the HLA (High Level Architecture) protocol, allowing external AI systems to be connected as federates:

– develop an AI agent (in Python, C++, Java);

– integrate it into the HLA simulation environment;
– the agent receives JCATS data and issues commands (e.g., move, fire).

This is the most flexible approach, supporting integration with TensorFlow, PyTorch, OpenAI Gym, etc.

Use of behavior logic (Behavior Trees / Finite State Machines) For tactical models without machine learning, behavior trees or FSMs can be embedded to define decision logic, e.g., «If enemy detected → seek cover → call artillery support.»

Can use JCATS XML scripts or external logic modules. Preprocessing / postprocessing modules are:

– apply AI to analyze scenario results;
– train ML models on simulation archives (e.g., to assess operational risks).

Perspectives for AI in JCATS are:

– military training – intelligent scenarios for commander education;
– weapon systems assessment – AI agents enable modeling of hundreds of tactical applications of new systems;
– robotic warfare – JCATS + AI enables simulation of human-machine collaboration (e.g., drones, MLRS, logistics);
– decision analysis – use of Explainable AI (XAI) to understand why specific decisions led to success or failure;
– tactics development – AI can propose novel strategies that human planners might overlook.

Iokhov O., Liwång H., Krahn U.

MODERN SIMULATION TECHNOLOGIES FOR TACTICAL-LEVEL OFFICER TRAINING: THE CASE OF STEEL BEASTS USAGE

Modern military training increasingly relies on simulation technologies to enhance the preparedness of officers at the tactical level. One of the most advanced simulation systems available today is Steel Beasts, a comprehensive armored warfare simulation used for training military personnel in various combat scenarios.

Traditional live training exercises, while effective, are costly, logistically demanding, and pose safety risks. To address these challenges, military academies and training institutions have adopted advanced simulation tools such as Steel Beasts. This simulation system provides a realistic and interactive training environment where officers can develop their decision-making skills, improve battlefield awareness, and practice tactical maneuvers.

Steel Beasts is a professional military-grade simulation system designed to train armored units and tactical commanders. It offers a variety of battlefield scenarios, allowing officers to engage in both offensive and defensive operations, reconnaissance missions, and coordination with other units. Key features of Steel Beasts include:

– Realistic Combat Scenarios: the system simulates a wide range of combat situations, including urban warfare, mechanized assaults, and defensive operations.
– Advanced Command and Control Functions: officers can practice issuing orders, maneuvering units, and responding to enemy actions in a dynamic environment.
– After-Action Review (AAR): detailed performance analysis helps officers identify strengths and areas for improvement.
– Multiplayer Capability: enables collaborative training with multiple participants, simulating joint and multinational operations.

The integration of Steel Beasts into military training offers several advantages: cost-effectiveness, safety and risk reduction, flexibility and scalability, enhanced tactical decision-

making.

Despite its advantages, the use of Steel Beasts and other simulation technologies presents certain challenges:

– Technical Limitations: while the system offers a high degree of realism, it cannot fully replicate the psychological and physiological stress of real combat.

– Infrastructure and Resources: effective use of simulation systems requires specialized hardware, software, and trained personnel to operate and maintain them.

– Complementarity with Live Training: simulation training should not entirely replace live exercises but rather complement them to ensure a well-rounded training experience.

The use of simulation technologies such as Steel Beasts has revolutionized tactical-level officer training by providing a cost-effective, safe, and flexible alternative to traditional exercises. While there are challenges in implementation, the benefits far outweigh the drawbacks, making simulation training an essential component of modern military education. With continued technological advancements, simulation-based training is expected to play an even greater role in preparing officers for the complexities of modern warfare.

The implementation of Steel Beasts will provide the opportunity to conduct command and staff exercises using combat simulations for the military command and control units of the National Guard of Ukraine and students of higher military education in various specialties (specializations).

Furthermore, the application of Steel Beasts in the educational process will enhance the practical command skills of cadets in managing troops within a dynamic combat environment. Therefore, the integration of Steel Beasts into the educational framework is a priority task for the Academy's simulation center.

Kharchenko I., Lysechko V.

FIXED REALLOCATION METHOD OF FREQUENCY POSITIONS AMONG CHANNELS IN QOFDM

The increasing demand for efficient spectrum utilization in modern communication systems, particularly in cognitive radio environments, necessitates advanced techniques to mitigate intra-system interference. A critical issue in this context is the occurrence of frequency collisions among subcarriers. The Quasi-Orthogonal Frequency Division Multiplexing (QOFDM) method offers a partial solution by assigning individually spaced subcarrier frequencies to each frequency plan. Nevertheless, conventional QOFDM assigns fixed frequency positions to channels, which can result in periodic conflicts and non-uniform energy distribution across the spectrum.

This paper introduces an enhancement to the QOFDM method by enabling fixed-frequency reallocation of channels within a frequency plan ensemble. The approach preserves the constant frequency spacing (Δf) between subcarriers in each plan while introducing controlled variability in channel positioning through predetermined permutation schemes.

In contrast to standard QOFDM – where channels are statically allocated to specific frequency positions – the proposed method employs a predefined permutation table that redistributes frequency positions across channels for each plan. Although the frequency offset Δf remains unchanged, the order of channels is periodically altered according to a fixed rule, which promotes spectral diversity.

The key advantages of the proposed method are as follows:

1. Improved spectral uniformity, which reduces the likelihood of local interference concentrations.

2. Decreased persistence of interference zones, due to variation in channel frequency positions across plans.

3. Low implementation complexity, as the permutation logic is fixed and does not require real-time adaptation mechanisms.

This technique allows for more balanced spectral energy distribution without altering the overall structure of subcarrier spacing, thus enhancing the operational performance of QOFDM in high-density network conditions.

Future development directions include:

1. Integration of adaptive algorithms for real-time permutation adjustments based on measured interference levels.
2. Implementation of dynamic reallocation protocols suitable for time-varying environments.
3. Fusion with pseudorandom frequency hopping (FHSS) techniques, aiming to further improve robustness against interference.

The proposed method represents a promising advancement in the optimization of frequency resource allocation in QOFDM systems, contributing to more reliable and interference-resilient wireless communications.

Kubiavka M., Pyrogov K.

APPLICATION OF REFLEXIVE INTELLIGENT SYSTEMS FOR PROCESSING NATURAL LANGUAGE INFORMATION IN INFORMATION SYSTEMS EDUCATION QUALITY MANAGEMENT

A characteristic feature of today is the processes of informatization, which are intensively developing and implemented in almost all spheres of human activity. They have led to the formation of a new information infrastructure, which is associated with a new type of social relations and the use of information and communication technologies (ICT). For our country, the effective provision and organization of education of pupils/students in the transforming education system, the formation of a new information mentality of all stakeholders is an urgent task. Solving this task requires constant monitoring and assessment of the state of the education system, which is based on the collection, processing of information and analysis of educational data necessary for making informed management decisions. Such information provision makes it possible to implement modern education management information systems (EMIS).

Informatization of education is closely related to the widespread introduction of methods and means of information and communication systems and technologies into the education system, the creation on this basis of a computer-oriented information and communication environment, with the filling of this environment with electronic scientific, educational and management information resources, with the provision of opportunities for subjects of the educational process to access the resources of the environment, use its tools and services when solving various tasks. At the same time, without the use of modern means of processing natural language information, it is impossible to count on the convenience and effectiveness of using such systems in the conditions of education quality management. It is clear that in such a complex area as education quality management, where the activities of managers and specialists are associated with the processing of a significant amount of data, it is impossible to do without the use of natural language information processing tools. But the modern Ukrainian market of information technologies (IT) does not offer educators a wide choice of instrumental intellectual systems that could be used at the lowest cost for processing natural language texts in education quality management. Therefore, there is a need to create problem-oriented intellectual systems that are capable of «selecting» the information necessary for education managers and specialists from the natural language representation of various categories of projects in education and applying it to solve the problems of planning

educational activities, managing the quality of education, managing the cost of education, managing risks, etc.

It is proposed to take the theory of information (non-force) interaction as the scientific and methodological basis for solving this problem. Within the framework of this theory, not only an apparatus for predicting the development of systems based on human interaction has been created, but also a mathematical apparatus has been provided for formalizing the soft component, also generated by human activity.

The concept of building this reflexive intellectual system implements the principles of universal modeling of patterns in a given subject area that manifest themselves statistically. The methodology for developing an intelligent system response adequate to all external influences provides for the selection of the most probable response of the intelligent system to a set of input influences with known probabilities of choosing a response to each input influence, as well as to some combinations of input influences.

In the course of this study, it was shown that the mathematical apparatus of the theory of non-force interaction is quite simple and convenient for building natural language text processing systems. The mathematical apparatus used will be the basis of a system for discrete text semantics processing in education quality management and educational management. In further work, it is planned to develop the structure and algorithms of the specified system and conduct its experimental verification in production conditions for managing educational processes. The use of the developed new ICT will affect the development of the formed ICT environment, which is dynamic and open, which will allow improving the process of managing educational institutions, improving and maximally directing their activities to improving the quality of education. The proposed model differs from existing ones by identifying differences in the conditional probabilities of the appearance of message addressees as the magnitude of the information impact of natural language text fragments, which allowed automatically determining the most likely addressees of this text. The developed technology meets the requirements of simplicity, informativeness and clarity, and minimal cost. It is based on the models and methods of managing the processes of influence developed by the authors, and the results obtained bring our state closer to creating competitive ICT for managing the quality of education and education management and bring us closer to creating full-fledged artificial intelligence. Currently, reflexive intelligent systems are already solving various tasks in the areas of human intellectual activity.

Shevchenko O., Perets K., Lysechko V.

EXPANDING APPROACHES TO THE EVALUATION OF SIGNAL CORRELATION PROPERTIES IN COGNITIVE NETWORKS

The efficient operation of wireless cognitive networks largely depends on the system's ability to accurately assess the correlation properties of the transmitted signals. Traditional approaches to such analysis – based primarily on autocorrelation and cross-correlation functions – often prove insufficient under dynamic spectral environments and conditions of multiple access.

The objective of this work is to improve the methodology for analyzing the correlation characteristics of complex signals with consideration for the specific requirements of cognitive networks. New approaches are proposed, based on the use of modified correlation functions, frequency-domain analysis, and adaptive smoothing algorithms.

The improvements include:

1) the use of generalized cross-correlation metrics that are sensitive to phase shifts and temporal deformations of signals;

2) application of frequency masks for selective evaluation of correlation properties within specific spectral subbands;

3) use of interval segmentation of signals to account for variable user activity over time;

4) construction of correlation matrices for signal ensembles under varying transmission conditions.

Computer modeling has shown that the use of these extended methods allows for a 20–25% average reduction in error when assessing mutual interference, compared to standard techniques. This significantly improves the quality of adaptive resource allocation in cognitive networks and reduces the likelihood of user conflicts.

The proposed approaches lay the groundwork for the development of new spectrum access optimization algorithms that take into account not only signal energy levels but also their correlation structure. Future research will focus on integrating these methods with machine learning techniques for dynamic prediction of spectral conflicts.

Shubina H., Komar O., Lysechko V.

ANALYSIS OF THE IMPACT OF TIME SEGMENTATION ON THE EFFICIENCY OF TELECOMMUNICATION SYSTEMS

Modern telecommunication systems operate under dynamic interference conditions, high traffic density, and limited spectral resources. In such an environment, signal segmentation methods become particularly important, as they enable optimization of information transmission, enhancement of interference immunity, and reduction of energy consumption.

Time segmentation involves dividing the signal into discrete time intervals for further processing, analysis, or transmission. The effectiveness of segmentation depends on parameters such as segment width, overlap, and processing approach. These parameters determine the system’s ability to adapt to external interference and rapidly changing conditions of the electromagnetic environment.

This paper presents the results of an analysis of how time segmentation parameters affect key performance indicators of telecommunication systems, including:

1. Interference immunity under varying channel conditions;
2. Stability of data transmission in multi-user environments;
3. Impact on system throughput and signal-to-noise ratio (SNR);
4. Influence on the efficiency of adaptive algorithms in telecommunication systems.

Particular attention is given to the comparison between uniform and variable (adaptive) segmentation methods. It was found that adaptive segmentation provides an improvement in interference immunity by approximately 20–28% compared to classical approaches and offers better performance in scenarios with high signal dynamics.

The obtained results can be applied in the design of wireless intelligent communication systems, particularly for tasks involving cognitive spectrum management, complex signal processing, and efficient multiple access implementation.

Sovhar O.

DIGITAL TOOLS FOR DEFENSE: LEVERAGING TECHNOLOGY FOR LANGUAGE PROFICIENCY IN UKRAINE

In the contemporary geopolitical landscape, marked by the ongoing Russian armed aggression against Ukraine, foreign language proficiency has emerged as a critical competency for defense forces personnel. The complexities of international military

cooperation, participation in joint exercises, and the adoption of advanced foreign-manufactured weaponry necessitate seamless communication and interoperability. This imperative has catalyzed a paradigm shift in language training methodologies within the Armed Forces of Ukraine, with a pronounced emphasis on the integration of information technologies and distance learning platforms.

The traditional pedagogical approaches to language acquisition are increasingly being supplanted by innovative, technology-driven solutions. Interactive online platforms, video conferencing, and mobile applications have revolutionized the learning experience, offering unprecedented flexibility and accessibility. This is particularly crucial for military personnel who often operate under demanding schedules and in geographically dispersed locations.

Distance learning systems provide both synchronous and asynchronous learning modalities, enabling personnel to engage with educational content at their convenience. Multimedia technologies enhance the learning process by facilitating the integration of language training into the daily routines of service members. Mobile applications, equipped with vocabulary builders, grammar exercises, and interactive tasks for developing listening and speaking skills, further augment the learning experience.

The integration of adaptive learning technologies allows for the personalization of the educational process, tailoring it to the individual needs and learning styles of military personnel. This dynamic approach ensures that training remains relevant and effective, fostering a more engaging and productive learning environment. The utilization of these innovative solutions is essential for preparing the Armed Forces of Ukraine for international missions and fostering effective collaboration with allied forces.

The contemporary educational landscape is characterized by the ascendancy of lifelong learning, a philosophy that underscores the importance of continuous professional development. This is particularly relevant in the military context, where personnel must continually adapt to evolving operational requirements and technological advancements. The system of continuous language training within the Armed Forces of Ukraine is integral to this lifelong learning paradigm, ensuring that personnel maintain and enhance their language proficiency throughout their careers.

The adoption of distance learning technologies aligns seamlessly with the principles of lifelong learning, providing flexible, accessible, and efficient educational opportunities. This approach is particularly advantageous in the context of military operations, where personnel may be deployed in remote locations or subject to unpredictable schedules.

The development of foreign language training within the Armed Forces of Ukraine is underpinned by a robust policy framework, including the Order of the Ministry of Defense of Ukraine «Basic Principles of Language Training of Personnel in the System of the Ministry of Defense of Ukraine,» the Concept of Distance Learning in the Armed Forces of Ukraine, and the Roadmap for Improving Language Training in the Armed Forces of Ukraine. These strategic documents articulate a clear vision for enhancing language training capabilities and fostering a culture of continuous learning.

The attainment of NATO partner status with enhanced capabilities has further underscored the importance of language proficiency, necessitating the development of interoperable communication systems and the adoption of standardized language training programs.

Traditional language training methodologies often struggle to meet the evolving needs of military personnel, particularly in terms of flexibility and accessibility. Distance learning technologies offer a viable solution to these challenges, providing a dynamic and adaptable learning environment.

The integration of BigBlueButton (BBB) into the Moodle distance learning platform has emerged as a pivotal development in the modernization of language training within the Armed Forces of Ukraine. BBB, an open-source web conferencing system, provides a comprehensive suite of digital tools for conducting online classes, including interactive whiteboards, presentation capabilities, video conferencing, and chat functionalities.

The platform's ability to facilitate real-time interaction and collaboration creates a virtual classroom environment that closely replicates traditional face-to-face instruction. Features such as screen sharing, polling, and session recording further enhance the learning experience.

H5P (HTML5 Package) is another valuable tool for creating interactive educational content. This open-source platform enables instructors to develop engaging multimedia resources, including presentations, videos, quizzes, and games, without requiring advanced programming skills.

H5P's versatility and ease of use make it an ideal solution for creating customized learning materials that cater to the specific needs of military personnel. The platform's compatibility with various learning management systems, including Moodle, further enhances its accessibility and usability.

The continued integration of information technologies and distance learning platforms is essential for ensuring the effectiveness of language training within the Armed Forces of Ukraine. By embracing these innovative solutions, the military can cultivate a cadre of linguistically proficient personnel who are well-equipped to meet the challenges of modern military operations.

The focus on continuous improvement, adaptive learning, and personalized education will be paramount in shaping the future of language training within the Armed Forces of Ukraine. The goal is to create a dynamic and responsive learning environment that empowers personnel to achieve and maintain a high level of language proficiency.

UDC 351.74:355/359

Sporyshev K.

PROBLEMATIC ASPECTS OF INFORMATION AND ANALYTICAL ACTIVITIES OF UKRAINE'S SECURITY FORCES

Among the key challenges faced by the information and analytical activities within Ukraine’s security forces, the following aspects can be highlighted:

– **Limited technological resources**: Despite significant progress in digitalization, there are still gaps in the technological infrastructure, which limits the ability to conduct in-depth analysis of big data;

– **Rising cyber threats**: Ukraine’s security forces face the urgent need to enhance cybersecurity and information protection. According to forecasts by Cybersecurity Ventures, global damages caused by cybercrime are expected to grow by 15% annually from 2021 to 2025, potentially reaching $10.5 trillion per year. This growth is driven by the increased activity of cybercriminal groups, many of which receive state support. The number of attacks has also risen due to ongoing digital transformation processes;

– **Lack of highly qualified specialists**: Effective operation of modern information and analytical systems requires highly skilled professionals. In light of the growing demand for cybersecurity experts, there remains a significant shortage of qualified personnel. According to the (ISC)² Cybersecurity Workforce Study, the global workforce gap in this sector is 3.4 million, with 70% of organizations reporting unfilled positions. Governments and major corporations such as Google, Microsoft, and IBM are actively working to close this gap by implementing various training and upskilling programs in the field of cybersecurity;

– **Insufficient efficiency of state governance**: Certain issues exist in the management of information and analytical activities within Ukraine’s security sector, which limits overall effectiveness.

Despite these challenges, Ukraine has shown success in certain aspects of information and analytical activity. Firstly, international cooperation – active engagement in international

partnerships for information exchange and sharing best practices – provides Ukraine with access to the latest analytical and intelligence methods. Secondly, the development of specialized training programs – the implementation of educational and professional development initiatives for analysts – contributes to the enhancement of expertise in the field of information and analytical activity (IAA).

In conclusion, while challenges remain, Ukraine demonstrates measurable progress in selected areas of its information and analytical operations. Notably, international collaboration facilitates the integration of advanced practices and methodologies, giving Ukraine strategic access to state-of-the-art analysis tools and intelligence resources. Equally important is the advancement of tailored training programs, which elevate the analytical competencies of professionals involved in IAA.

UDC 621.327:681.5

Tupitsya I., Kryvonos V.

METHODOLOGY FOR RESTRUCTURING AIRCRAFT INTELLIGENCE DATA FOR UNMANNED AIRCRAFT INFO COMMUNICATION SYSTEMS

The growing role of unmanned systems as a key tool for the successful performance of combat missions has led to increased activity of domestic manufacturers (enterprises, factories, volunteer organizations) and partner countries. It should be noted that the characteristic features of the national manufacturer include an attempt to balance the quality indicators of unmanned aircraft systems (UAS) samples and the high dynamics of the development of enemy weapons and military equipment (the dynamics of the introduction of modern information technologies into the software and hardware of the UAS is quite significant). In turn, the main goal of the international manufacturer (partner countries) is to conduct tests of already created samples in combat conditions. In this regard, today, the Defense Forces of Ukraine actively use various UAS [1]. In turn, the active integration of UAVs, provided as part of international logistical assistance by partner countries, into combat operations on the territory of Ukraine has led to the widespread implementation of NATO standard requirements in the production and operation of unmanned aerial vehicles.

It should be noted that today, digital optical-electronic aerial reconnaissance systems use the JPEG graphic format to generate aerial reconnaissance data (images, streaming video) [2].

Using this graphic format has the following advantages:

1. Allows the provision of high compression characteristics of data generated by onboard sensors of digital optoelectronic aerial reconnaissance systems of UAVs [3]. This, in turn, allows us to provide the necessary efficiency level of aerial reconnaissance data delivery over video data transmission lines.

2. Compliance of the aerial reconnaissance data format with the requirements of NATO standards (Stanag 7023 and others) [4].

However, the main disadvantage of using this graphic format for encoding aerial reconnaissance data is its low resistance to interference in video data transmission lines [5]. Therefore, the phased implementation of the specified compression algorithm should be investigated in more detail.

Practical implementation of the algorithm JPEG involves external restructuring methods of encoded data's alphabet, which transforms the original data [6]. These methods are used before statistical encoding at the data preparation stage. Thus, at the stage of data preparation for encoding, the following methods of external restructuring are used:

1. Color model transformation (transition from additive RGB to YCbCr color model) and subsampling. These external restructuring methods allow for reducing the dynamic range of

encoded elements.

2. Transition from spatial to frequency representation of coded elements (discrete cosine transform) and their subsequent quantization. Using these external restructuring methods leads to a significant loss of information.

3. Linearization of coded data – transition from matrix to vector representation using zigzag scanning (stage of preparation for using statistical coding methods).

Thus, when preparing data for coding, external restructuring methods are used to present the coded data more advantageously.

In turn, at the encoding stage, the external restructuring method is used to group the vector elements by a common feature (the number of zero elements for the JPEG format). Accordingly, the final stage of forming the original encoded sequence is the use of a lossless encoding method - the Huffman statistical encoding method, the result of which is the formation of a sequence of uneven code structures that have the prefix property, the problematic aspect of which is the avalanche effect of errors on the process of reconstructing digital images [6].

To solve the above-mentioned problematic aspect, a fundamentally new approach to restructuring the alphabet of encoded data was proposed in the article [7]. A distinctive feature of the proposed approach is the transformation of the alphabet by structural features without data loss [8]. In turn, using the specified approach in the statistical coding scheme proposed in the article [9] indicates that conditions are created to increase the noise immunity of the original code sequence.

Today, the primary transformation in UAV info-communication systems is the integration of artificial intelligence technologies into the process of processing aerial reconnaissance data, which leads to increased requirements for the integrity of data generated by onboard sensors of digital optoelectronic aerial reconnaissance systems; it is proposed to integrate the specified approach into the model of automated data processing.

Further scientific research will be aimed at creating a model for automated detection of aerial reconnaissance objects using pre-processing of aerial reconnaissance data based on the proposed approach.

References

1. Ukrainian Unmanned Aerial System Tactics. Oe.tradoc.army.mil: web site. URL: https://oe.tradoc.army.mil/2024/10/08/ukrainian-unmanned-aerial-system-tactics. (Accessed 11 January 2025).
2. Why Ukraine is Establishing Unmanned Forces Across Its Defense Sector and What the United States Can Learn from It. Csis: web site. URL: https://www.csis.org/analysis/why-ukraine-establishing-unmanned-forces. (Accessed 11 January 2025).
3. Image formats (RAW, JPEG, HEIF) and compression. Canon: web site. URL: https://www.canon.ge/pro/infobank/image-file-types. (Accessed 11 January 2025).
4. STANAG 7023, Edition 5. Air reconnaissance primary imagery data standard - AEDP-7023 Edition A. NATO Standardization Office : web site. URL: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/9556/EN. (Accessed 7 January 2025).
5. Khmelevskyi S., Tupitsya I., Kibitkin S., Korolyuk N., Romanyuk A., Dziuba I. Creation of a video data reliability assessment model for compression coding technology in the conditions of errors in the data transmission channel. Information Processing Systems. 2022. № 2 (169). P. 72-86. https://doi.org/10.30748/soi.2022.169.09.
6. S. Khmelevskiy, I. Tupitsya, Q.A. Mahdi, O. Musienko, M. Parkhomenko, and Y. Borovensky, «Development of the external restructuring method to increase the efficiency of information resource data encoding,» Information Processing Systems, 3(166), pp. 52-61, 2021. https://doi.org/10.30748/soi.2021.166.06.
7. S. Khmelevsky, I. Tupitsya, M. Parkhomenko, and Y. Borovensky, «Model of

Transformation of the Alphabet of the Encoded Data as a Tool to Provide the Necessary Level of Video Image Quality in Aeromonitoring Systems,» IT&I Workshops, 2021, pp. 311-319. [Electronic resource]. Available: http://ceur-ws.org/Vol-3179/Short_4.pdf.
8. Karlov D., Tupitsya I., Parkhomenko M. Methodology of increasing the reliability of video information in infocommunication networks aerosegment. Radio Electronics, Computer Science, Control. 2022. No. 3. P. 120−132. https://doi.org/10.15588/1607−3274−2022−3−12.
9. Karlov D., Tupitsya I., Parkhomenko M., Musienko O., Lekakh A. Compression Coding Method Using Internal Restructuring of Information Space. International Journal of Computing. 2022. Vol. 21. No. 3. P. 360−368. https://doi.org/10.47839/ijc.21.3.2692.

UBC 621.391

Vasylyshyn V.

SPECTRUM MONITORING METHOD FOR COMMUNICATION SYSTEMS BASED ON COGNITIVE RADIO

Nowadays, the efficiency of communication systems (means of communication) is increased by the use of modern communication technologies, including cognitive radio (CR) technology, the implementation of not only time, but also space-time signal processing. In addition, methods of signal spectrum spreading are used such as pseudo-random frequency hopping (i.e. FHSS), direct sequence spreading spectrum (DSSS), their combinations, adaptive modulation and coding methods, and some other approaches. In modern conditions, improving the efficiency of a communication system can be associated with increasing stability (to a greater extent, noise immunity as its component), capacity, and intelligence protection.

The important task that can be solved on the basis of the CR is the effective use of the radio frequency resource for both military and civilian users, coordination of joint operation of radio communications and own electronic warfare equipment. Increasing the efficiency of spectrum use is achieved by scanning (monitoring) the spectrum in order to identify temporarily free spectrum areas and their use. The CR system assumes that some users are primary (i.e. have advantages in the use of frequency bands), and other users are secondary (who are granted the right to use free spectrum bands).

The implementation of the CR is associated with a certain set of actions, which include signal detection, frequency scanning and determination of the boundaries of free spectrum areas (spectrum holes), determination of the direction of signal arrival from noise sources, the state of the communication channel, etc.

There are already known IEEE standards that regulate the use of CR, the samples of communication equipment that assume implementation of CR or elements of CR (for example, the radio manufactured by L3 Harris, Silvus and others). In addition, certain functions of cognitive radio are implemented by spectrum analyzers based on software defined radio (SDR) technology.

The advantages of cognitive radio can be enhanced by spatio-temporal signal processing, which can be implemented in modern communications equipment that uses MIMO technology or its modifications (MN-MIMO, MU-MIMO, etc.).

In order to determine the boundaries of free spectral regions, the so-called spectrograms can be used, which are implemented using the windowed Fourier transform, periodograms, the methods based on the spectral decomposition of the correlation matrix (CM) of observations (MUSIC, ESPRIT), methods of spectral analysis with windowed processing based on the use of spheroidal wave functions. In the process of signal detection, it is

important to estimate the noise variance, the accuracy of which affects the accuracy of determining the detection threshold. Estimation of noise variance usually involves the use of classical approaches (periodogram, etc.) based on available samples of input data.

The periodogram method (Bartlett or Welch) for detection and spectrum holes estimation is used. The noise variance estimate used for detection is improved using the spectral decomposition of the CM. The threshold is obtained using the variance estimate and probability of false alarm. Simulation in Matlab for OFDM communication system confirms the effectiveness of the proposed approach. The situation with fading channels was also analysed.

Areas for further research include the use of methods based on the spectral decomposition of the CM of observations, and an analysis of the application of the proposed approach to MANETs. Furthermore, it is of interest to extend the presented approach for the case of jammer influence when combined application of CR and FHSS is of interest.

Vlasov K.

THE ROLE OF IoM/BT TECHNOLOGIES IN ENSURING COMBAT EFFECTIVENESS OF MILITARY UNITS

One of the most significant aspects of modern military confrontation is that information has become the most powerful tool of influence. Operational awareness, formed based on collected data, has become the foundation of any military strategy. The synergy of information operations, an integrated system of sensors, weaponry, and platforms significantly enhances combat effectiveness.

The Internet of Military/Battlefield Things (IoM/BT) is gaining increasing importance in the military sphere, ensuring continuous connectivity between various systems, platforms, and devices. Thanks to IoM/BT, military units can monitor equipment, control logistics, and respond promptly to changes on the battlefield. This improves coordination, reduces risks, and enhances the efficient use of resources.

IoM/BT technologies represent a network of interconnected devices equipped with sensors, data transmission systems, and automated analysis tools. They enable tracking the condition of equipment, monitoring soldiers' health, coordinating unit actions, and ensuring object security in real time. The integration of IoM/BT into military operations significantly improves management and response to threats, increasing the effectiveness of modern combat systems.

The main components of IoM/BT include:

– sensors and detectors – used to collect data on the environment, the condition of equipment, and the location of enemy forces;

– combat information systems – platforms that integrate data from various sources and provide command with real-time intelligence;

– automated control systems – allow real-time management of troops, equipment, and logistics;

– secure communication networks – ensure data exchange between devices without the risk of cyberattacks.

IoM/BT technologies provide real-time battlefield intelligence. For example, sensors mounted on armored vehicles can transmit data on their technical condition, while drones can detect enemy movements. The main areas of IoM/BT application in situational awareness include environmental monitoring, target recognition, and troop movement tracking. For instance, NATO utilizes the JISR (Joint Intelligence, Surveillance, and Reconnaissance) system, which integrates IoM/BT sensors to enhance troops' situational awareness.

Automated supply systems based on IoM/BT ensure timely delivery of ammunition, fuel, and provisions according to real-time needs. The use of smart warehouses minimizes the risk of resource shortages. Key advantages of IoM/BT technologies in logistics and supply include: real-time inventory monitoring; – optimization of supply routes to the frontlines using GPS trackers and AI-based algorithms; – automated supply chain systems. For example, the U.S. Armed Forces use the RFID (Radio Frequency Identification) system to track logistics chains, enabling more efficient resource management.

One of the key areas of military technology development is unmanned combat systems, where IoM/BT plays a crucial role. Drones and autonomous combat vehicles utilize sensors, artificial intelligence, and cloud computing to enhance combat effectiveness. Reconnaissance drones equipped with cameras, infrared sensors, and image recognition systems can conduct aerial reconnaissance, identify enemy positions, and transmit data in real time.

Autonomous ground combat vehicles equipped with IoM/BT systems, such as unmanned tanks or mobile combat robots, can perform patrolling and enemy engagement tasks without involving personnel. Additionally, IoM/BT enables the creation of drone swarms that can coordinate actions to execute complex missions such as simultaneous attacks or reconnaissance. For example, Israel uses Harop loitering munitions, which autonomously detect and engage targets while exchanging data with other combat systems through IoM/BT.

IoM/BT facilitates integrating various military units into a single network, ensuring operational communication and data exchange. This networked interaction allows real-time information sharing between soldiers, vehicles, drones, and command centers. Military personnel can use smart devices to report changes on the battlefield, enabling faster threat response. For example, the U.S. Army employs the Nett Warrior system, which equips soldiers with wearable IoM/BT devices to improve coordination and situational awareness.

At the same time, the widespread implementation of IoM/BT technologies requires addressing cybersecurity issues, ensuring reliable communication, and securing adequate funding.

Despite challenges, Ukraine has already integrated several IoM/BT solutions, including:

1. Ukrainian forces actively deploy both commercial and specially modified unmanned aerial vehicles. These drones are equipped with high-resolution cameras, infrared, and thermal sensors, allowing real-time data collection on enemy positions, terrain changes, and potential threats. The collected data is integrated into command systems, providing an up-to-date battlefield picture;

2. IoM/BT devices collect data from multiple sources, including drones, stationary sensors, combat vehicle systems, and soldiers' wearable devices. This creates a unified system that provides real-time situational awareness, enabling rapid tactical adjustments, optimal force deployment, and accelerated decision-making;

3. IoM/BT sensors deployed at strategic locations and critical facilities detect movement, sound anomalies, or temperature changes that may indicate enemy activity. The information is instantly transmitted to command centers, allowing proactive threat response;

4. Ukraine's military has implemented RFID- and GPS-based systems to monitor the movement of supplies, ammunition, fuel, and critical equipment. These solutions enable real-time tracking of resources, route planning, and prompt responses to logistical changes, significantly reducing the risk of shortages or delays.

This demonstrates that IoM/BT technologies are becoming a crucial tool for modernizing Ukraine's armed forces, enhancing intelligence capabilities, improving battlefield management, and optimizing logistics. By integrating advanced technologies, Ukraine is strengthening its ability to adapt to dynamic combat conditions and improve its overall defense capabilities.

Yakovlev S., Uzlov D., Strukov V., Kobziev V.

HANDLING OUTLIERS IN DATA PROCESSING AND SWARM ALGORITHMS

Modern intelligent technologies for processing data of various origins must take into account the possibility of unknown (fully or partially) stochastic properties of the processed data sets or processes that determine them. Some values that do not correspond to formal or convenient prior ideas about the internal regularities of numerical sets or developing processes are most often characterized as outliers or anomalous values. At the same time, it is precisely in such features that important internal patterns are manifested, which are not captured by the data models used or the situations associated with their origin.

Procedures for detecting and processing anomalies are used in a large number of application areas, some of them are described in [1, 2]. Processing of single or group anomalies is performed taking into account the features of their manifestation.

To solve the problem of optimizing complex systems, where traditional methods are often ineffective, swarm optimization algorithms inspired by the collective behavior of biological swarms are a promising tool [3]. At the same time, the presence of outliers can significantly affect the process of finding the optimal solution. In particular, these algorithms often suffer from early convergence, where particles get stuck in local optima due to outliers.

Therefore, the study of methods for detecting and processing outliers in swarm algorithms, such as the particle swarm optimization (PSO), is an urgent task that has significant potential to improve the efficiency and reliability of these algorithms in various practical applications, for example, drone control systems. Outliers in swarm systems can be represented as particles in the swarm that do not follow the expected swarm behavior, such as particles that move much faster or slower than other ones in the swarm. Such particles have all the characteristics inherent in the standard definition of an outlier: they can deviate significantly from the swarm trajectory, interfere with other particles, and prevent them from moving to their destination. There is no universal solution for handling outliers in swarm systems, as hyperparameters in swarm algorithms greatly impact their efficiency and stability. Tailoring strategies to specific problems and exploring alternative outlier control methods are key priorities for practical tasks.

Recent studies incluse a wide range of variations of the PSO algorithm with adaptive approaches, where hyperparameters dynamically change during the optimization process, considering the current state of the swarm and the characteristics of the problem. There are also methods using swarm topologies that affect the exchange of information between particles to avoid early convergence, hybrid algorithms that combine PSO with genetic algorithms or bee swarm methods to combine the advantages of different approaches.

The adaptive particle swarm method balances exploration and fast convergence but is more complex than standard PSO. Cooperative PSO aids particle cooperation but can get stuck in local optima, while binary PSO handles both continuous and discrete parameters but may be less efficient than specialized algorithms. It has been determined that none of the existing variations of PSO is a universal solution; each comes with its own limitations.

Article [3] concludes that the use of hybrid approaches that combine PSO with neural networks and reinforcement learning provides new opportunities for solving complex optimization problems and improving the efficiency of existing solutions. Unlike algorithmic solutions, the use of neural networks in combination with the particle swarm optimization method (its variations) will be appropriate for obtaining a positive practical result when applied to drone control systems.

References

1. Kirichenko L., Kobziev V., Fedorenko Y. Data Mining methods for detection of collective anomalies in time series // Міжн. наук.-практ. конф. “Застосування інформаційних

технологій у підготовці та діяльності сил охорони правопорядку" / Збірник тез доповідей. - Харків, 2021, - с. 106.
2. Кобзєв В.Г., Яковлєв С.В., Назаров О.С., Назарова Н.В., Горішня К.О. Модифікації методу опорних векторів для класифікації та виявлення аномалій у задачах обробки зображень // Міжн. наук.-практ. конф. "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" / Збірник тез доповідей. - Харків, 2024, - с. 149-151.
3. Uzlov D., Havryliuk Y., Hushchyn I., Strukov V. and Yakovlev S. Handling outliers in swarm algorithms: a review. Proceedings of the 4th International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2024). Cambridge, MA, USA. CEUR Workshop Proceedings, 2024, 3777, pp. 430-437.

УДК 004.942

Адаменко А.А., Антонов Д.В., Порохончук О.М.

ІМІТАЦІЙНО-ТРЕНАЖНІ ТА МОДЕЛЮЮЧІ СИСТЕМИ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ ПРОТИПОВІТРЯНОЇ ОБОРОНИ

З перших часів російської агресії проти України гострою проблемою стала протидія пілотованим та непілотованим засобам повітряного нападу противника, вирішення якої потребує постійну забезпеченість усіх складових Сил оборони України достатньою кількістю засобів протиповітряної оборони (ППО) та військових фахівців, здатними на професійному рівні здійснювати їх бойове застосування та технічне обслуговування.

В умовах ведення активних бойових дій, особливу актуальність набуває проблема підготовки військових фахівців ППО з числа молодого поповнення, що повинна здійснюватися в зжаті терміни як в навчальних центрах, так і безпосередньо в бойових частинах. Зрозумілими є об'єктивні причини, що негативно впливають на якість підготовки військових фахівців в таких умовах, що, в свою чергу, здійснює негативний вплив на стан бойової готовності та ефективність ведення бойових дій військовими підрозділами Сил оборони [1].

Імітаційно-тренажні та моделюючі комп'ютерні комплекси стали невід'ємною складовою систем підготовки сучасних армій світу. У найбільш розвинутих у військовому відношенні країнах та військових альянсах ці комплекси здобули найбільшого розвитку і на сьогоднішній день їх можливості не обмежуються ні чисельністю та різноманітністю угруповань військ (сил), що навчаються, ні їх територіальним рознесенням.

Їх висока ефективність, економічність, гнучкість та багато інших позитивних якостей обґрунтовують їх довгострокову перспективність, зокрема, для підготовки органів військового управління (ОВУ) та бойових розрахунків (обслуг) озброєння та військової техніки (ОВТ) різних складових Сил оборони.

Аналіз нагальних потреб в підготовці військових фахівців для заміщення посад бойових розрахунків (обслуг) ОВТ ППО дозволив сформувати перелік зразків ОВТ та їх елементів, для яких доцільним є розробка відповідних імітаційно-тренажних та моделюючих систем. Це, перш за все, ОВТ ППО радянських розробок, яких на озброєнні Сил оборони України перебуває в найбільшій кількості.

В доповіді представлені основні групи імітаційно-тренажних та моделюючих систем ОВТ ППО, що розроблені Харківським національним університетом Повітряних Сил імені Івана Кожедуба та успішно використовуються в підготовці військових фахівців військ ППО Сухопутних військ Збройних Сил (ЗС) України.

Першу групу складають програмні моделі панелей блоків зразків ОВТ, що надають можливість набуття практичних навичок щодо проведення функціонального контролю бойових машин «Тунгуска», «Оса-АКМ» та «Шилка». Ці моделі функціонують автономно без використання локальної обчислювальної мережі.

Друга група – це імітаційно-тренажні системи для індивідуальної та групової підготовки бойових розрахунків (обслуг) зенітних ракетних комплексів «Оса-АКМ», «Стріла-10» та «Шилка». Ці імітаційно-тренажні системи можуть функціонувати як автономно, так і в складі локальної обчислювальної мережі, що об'єднує програмні моделі різних робочих місць екіпажу певної бойової машини та відповідні моделі інших бойових машин, у тому числі, різнотипних. Для створення єдиної моделі повітряної обстановки використовується спеціальне програмне забезпечення (СПЗ) для проведення оперативно-тактичних розрахунків та імітаційного моделювання бойових дій Повітряних Сил ЗС України «Віраж-РД» [2–4].

З використанням імітованої повітряної обстановки, що створюється та керується за допомогою СПЗ «Віраж-РД», працює також програмна імітаційна модель переносного зенітного ракетного комплексу «Ігла» («Ігла-1»).

Використання СПЗ «Віраж-РД» дозволяє здійснювати індивідуальну та групову підготовку бойових розрахунків декількох екіпажів (операторів) в єдиному інформаційному полі з використанням імітованої повітряної обстановки, що, за потреби, може нарощуватися чи корегуватися. Зокрема, СПЗ «Віраж-РД» має інформаційну модель та інтерфейс, споріднений з СПЗ «Віраж-Планшет» [5], що, у тому числі, формує практичні навички у курсантів щодо використання цього СПЗ в своїй майбутній бойовій роботі.

Список використаних джерел

1. Оцінювання впливу системи підготовки військовослужбовців у навчальних центрах на стан бойової готовності Збройних Сил України / М.Ф. Пічугін, Д.В. Карлов, А.С. Воловодюк, О.О. Клімішен // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2016. – № 2(47). – С. 226-229.
2. Створення, впровадження, досвід використання та перспективи розвитку комплексу оперативно-тактичних розрахунків та імітаційного моделювання «Віраж» / С.П. Лещенко, С.І. Бурковський, М.П. Батуринський, Л.В. Польшина, А.А. Адаменко, І.А. Кулініч, Д.Ю. Свистунов // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2017. – № 5(54). – С. 80-84.
3. Використання можливостей тренажно-імітаційного комплексу «Віраж-РД» для виконання розрахунків та моделювання польоту транспортної авіації при виконанні бойового завдання / М.Ю. Романченко, М.С. Соломон // Наука і техніка Повітряних Сил Збройних Сил України. – 2016. – № 2. – С. 81-84. – Режим доступу: http://nbuv.gov.ua/UJRN/Nitps_2016_2_23.
4. Імітатор повітряно-завадової обстановки з використанням системи «Віраж-РД» для оглядових аналогових радіолокаційних станцій / О.А. Малишев, М.Р. Арасланов, С.В. Бєлай, В.В. Сидоров, І.С. Бабенко, А.О. Астахов // Наука і техніка Повітряних Сил Збройних Сил України. – 2020. – № 4(41). – С. 112-124. https://doi.org/10.30748/nitps.2020.41.14.
5. Застосування допоміжної автоматизованої підсистеми збору, обробки, відображення та аналізу інформації про повітряну обстановку «Віраж-Планшет»: навч.-метод. посіб. / С.П. Лещенко, О.М. Колеснік, А.А. Адаменко, Д.В. Антонов та ін. – Х. : ХНУПС, 2020. – 80 с.

Бабенко О.І., Сізон Д.О., Калачова В.В.

ПРОЕКТУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВОЇ ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ

Задача побудови системи інформаційно-аналітичного забезпечення військової організаційної структури є багатофакторною, а з досвіду побудови систем – такою, що належить до класу маловизначених. На практиці це призводить до формування реальної системи, виходячи з розуміння сильних та слабких сторін відомих попередніх реалізацій з подальшим процесом уточнення такої системи на основі досвіду її функціонування. Крім того, вирішення подібних задач передбачає її декомпозицію (розбиття) на окремі етапи, з застосуванням підходів ітераційного наближення до необхідного стану за кожним етапом.

В залежності від призначення військової організаційної структури, виділяють наступні етапи проектування системи інформаційно-аналітичного забезпечення:

- етап формування онтологічної моделі (словника проектування),
- етап системного проектування,
- етап проектування (оцінювання) спроможностей,
- етап організаційного проектування,
- етап ергономічного проектування,
- етап технічного проектування,
- етап функціонального проектування.

На етапі формування онтологічної моделі формують перелік основних концептів діяльності та зв’язки між ними. На основі онтологічної моделі формують необхідні словники та глосарії, базові візуальні моделі.

На етапі системного проектування часто визначають всі елементи цілевизначення, та встановлюється схема відповідності між цілями та задачами.

На етапі проектування (оцінювання) спроможностей визначають перелік ключових умов здійснення діяльності та показники успішності виконання завдань, а також напрямки заходів з покращення за факторами, наприклад: DOTMLPFI (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Interoperability). Особливістю цього етапу є уточнення вимог до діяльності, а саме: умов виконання завдань та показників успішності.

На етапі організаційного проектування обирають структуру системи, склад та кількість підсистем, порядок організації взаємодії.

На етапі ергономічного проектування – уточнюють чисельність персоналу в підрозділі інформаційно-аналітичного забезпечення військової організаційної структури на основі оцінки можливостей людини щодо управління (норми керованості), а також елементи стандартизації діяльності: алгоритми, стандартизовані операційні процедури, технологічні карти тощо.

Технічне проектування передбачає врахування питань технічного забезпечення, іноді окремим питанням оцінюють елементи системи C4ISR (Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), включно з питаннями отримання та доступу до різного виду інформації, зв’язку, управління тощо.

Всі етапи проектування є взаємопов’язаними в ітераційному циклі наближення до бажаного рівня. З врахуванням прийнятої в ЗС України моделі оборонного планування на основі спроможностей, етапи проектування можуть бути і відмінними від зазначених вище, а саме повторювати (корелювати) напрямки визначені факторами DOTMLPFI.

УДК 681.3

Балабуха О.С., Качуровський Г.М., Максимов М.О., Споришев К.О.

ПРОПОЗИЦІЇ ЩОДО РОЗРОБКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ КОМАНДИРА МОБІЛЬНОГО КОМПЛЕКСУ ОЗБРОЄННЯ У СКЛАДІ ПІДРОЗДІЛУ (ЧАСТИНИ) РАКЕТНИХ ВІЙСЬК І АРТИЛЕРІЇ СУХОПУТНИХ ВІЙСЬК

Автоматизована система підтримки прийняття рішень (АСППР) командира мобільного комплексу озброєння (МКО) у складі підрозділу (частини) ракетних військ і артилерії (РВ і А) сухопутних військ (СВ) призначена для вироблення обґрунтованих рішень, які приймаються командиром на організацію та ведення бойових дій, як у складі підрозділу (частини) РВ і А СВ, так і при умові, що МКО діє автономно, як окремий вогневий модуль. Головною особливістю інформаційної технології підтримки прийняття рішень є якісно новий метод організації взаємодії джерел інформації, обчислювальної системи та людини, яка приймає рішення [1-7].

Вироблення рішення, яке є основною метою такої взаємодії, здійснюється в результаті ітераційного процесу, у якому приймають участь:

– система підтримки прийняття рішень у ролі обчислювального комплексу;

– людина, яка приймає рішення, як управляючий орган, що задає вхідні дані та оцінює отриманий від обчислювального комплексу результат.

Центральними вимогами до АСППР – є достовірність отриманих результатів, оперативність розрахунків (актуальність проведених розрахунків у динаміці бою) та контрольованість впливів (АСППР лише рекомендує, а людина – приймає рішення та повністю за нього відповідає) [4]. Закінчення даного процесу проходить за рішенням людини при прогнозованому досягненні заданих критеріїв ефективності ведення бойових дій підрозділом (частиною) РВ і А або за відсутністю часу (часовий критерій прийняття рішення) за умови вибору раціонального варіанту ведення бойових дій.

Слід визначити особливості структури та умов функціонування АСППР командира МКО підрозділу (частини) РВ і А СВ [4]:

– орієнтація на рішення погано структурованих (формалізованих) задач, використання у алгоритмах АСППР методів нечітких множин, нечітких мір, інтелектуального аналізу даних;

– використання у складі алгоритмічного (математичного) забезпечення методів прийняття рішень в умовах невизначеності;

– сполучення традиційних методів доступу та обробки даних з можливостями математичних моделей та методами рішення задач на їх основі;

– урахування системи переваг людини, яка приймає рішення (командира підрозділу (частини) РВ і А);

– висока адаптивність, яка забезпечує можливість пристосовуватися до особливостей технічного та програмного забезпечення, а також до вимог користувача.

Слід зауважити, що АСППР може використовуватися на будь-якому рівні управління [1-6], що характерно для ієрархічної та мережецентричної структури побудови системи управління РВ і А СВ. Тобто, рішення (пропозиції до рішення, замисел), які приймаються на різних рівнях системи управління повинні бути координовані. Тому, важливою функцією системи підтримки прийняття рішень є координація (на програмному рівні) дії командирів, які приймають рішення на різних рівнях управління, а також на одному рівні управління (організація взаємодії).

До складу АСППР можливо виділити чотири головних компоненти [4]:

– база даних (БД);

– база моделей (знань);

– геоінформаційні системи;

– програмна система, яка складається з системи управління базами даних, системою управління базою моделей та системи управління інтерфейсом між командиром (користувачем) та обчислювальним комплексом.

БД грає важливу роль у структурі АСППР, оскільки дані є основою для прийняття рішення, вони використовуються для розрахунків за допомогою математичних моделей [4]. Важливо відмітити джерела даних та їх особливості. Інформація від власних джерел. До цієї інформації належить інформація про повітряного (наземного) противника, характер його дій, отримана від власних розвідувальних джерел інформації. Особливістю такої інформації є її достовірність, оперативність та безперервність отримання.

Бойові документи (розпорядження, директиви). До цієї інформації відносяться директивні документи, отримані командиром частини (підрозділу) РВ і А СВ від безпосередніх (прямих) начальників. Особливістю даного виду інформації є безумовне виконання (врахування) отриманих розпоряджень при виробленні рішення на ведення бойових дій.

Інформація від автоматизованої системи управління вищого (взаємодіючого) рівня управління. Особливістю застосування даного виду інформації є робота АСППР командира МКО РВ і А СВ у єдиному інформаційному просторі для забезпечення отримання повної картини операції (бою).

Список використаних джерел

1. Смірнов Є.Б. Метод вибору раціональної за ефективністю стратегії управління в ході збройної боротьби в умовах її нечіткого інформаційного ресурсу / Є.Б. Смірнов, В.І. Ткаченко, В.М.Більчук // Системи обробки інформації. - 2007. - Вип. 9(67). - С. 2 - 10.
2. Ткаченко В.І. Застосування геоінформаційних і космічних навігаційних систем для підвищення ефективності дій зенітних ракетних підрозділів / В.І. Ткаченко, М.О. Єрмошин // Системи озброєння і військова техніка. — 2007. — № 4 (12). — С. 48 - 52.
3. Чеченков М.М. Особливості забезпечення процедур обробки та обміну інформацією в інтегрованій системі автоматизованого управління і зв’язку ракетних комплексів Сухопутних військ / М.М.Чеченков, С.В.Малахов, А.Г.Снисаренко, В.М.Шлокин, А.Л.Гостев // Системи озброєння і військова техніка. – Х.: ХУПС. – 2010. – Вип. 4(24). – С.80-87.
4. Піскунов С.М. Вимоги до системи підтримки прийняття рішення командира частини (підрозділу) військ протиповітряної оборони Сухопутних військ / І.М. Тіхонов, С.М. Піскунов, А.В. Тристан // Системи озброєння і військова техніка. — 2011. — № 1(25). — С. 214 — 217.
5. Звигляныч С.М. Оцінка якості функціонування автоматизованих систем управління / С.М. Звигляныч, М.П. Ізюмський, О.С. Балабуха // Системи обробки інформації. — 2017. Вип. 3(149) — С. 115 — 117. DOI: 10.30748/soi.2017.149.22
6. Аналіз напрямків розвитку військової техносфери країн НАТО / О. Коломійцев та ін. InterConf. 2023. № 37(171). С. 379–397. URL: https://doi.org/10.51582/interconf.19-20.09.2023.033 (дата звернення: 03.03.2025).
7. Особливості застосування безпілотних літальних апаратів коптерного типу / О. Коломійцев та ін. Collection of Scientific Papers «ΛΌГОΣ». 2024. С. 188–198. URL: https://doi.org/10.36074/logos-16.08.2024.038 (дата звернення: 03.03.2025).

Баранов Ю.М., Баранов А.М., Каршень А.М.

ОБҐРУНТУВАННЯ ВИМОГ ДО ЗАСТОСУВАННЯ РОБОТИЗОВАНИХ КОМПЛЕКСІВ ПОДОЛАННЯ ІНЖЕНЕРНИХ ЗАГОРОДЖЕНЬ

Сучасні зразки роботизованих комплексів (РК) подолання інженерних загороджень (ІЗ), які стоять на озброєнні збройних сил різних країн, за своїм можливостями застосовуються такими підрозділами:

– розвідки (в складі загальновійськових та інженерних груп розвідки);

– інженерно-саперними, у складі груп протидії та знешкодження при масовому застосуванні противником вибухонебезпечних предметів (ВНП) на місцевості та об’єктах у районах виконання частинами та підрозділами бойових (спеціальних) завдань;

– розмінування, у складі груп та загонів розмінування об’єктів і районів місцевості розташування та перебування військ;

– розгородження, у складі штурмових груп при веденні військами тактичних дій на складній та урбанізованій місцевості.

Виконання завдань щодо подолання ІЗ здійснюють на підставі бойового розпорядження командира.

В основу пріоритетності дій розрахунків РК подолання ВНП повинні покладатись вимоги, а саме:

– збереження життя та здоров’я особового складу (принцип збереження людського життя домінує понад усіма іншими);

– повернення місцевості до нормального функціонування;

– збереження інфраструктури та обладнання (які мають значення для основної операції чи місцевого населення).

Принципи, яких необхідно дотримуватись в операціях зі знешкодження ВНП для досягнення поставленої мети:

– для знешкодження ВНП оператор повинен максимально застосовувати дистанційні засоби;

– спосіб нейтралізації ВНП шляхом розбивання пристрою за допомогою дистанційних засобів завжди повинен розглядатись як перший варіант знешкодження;

– наскільки можливо, оператор повинен повертатися до дистанційних та напівдистанційних дій з метою мінімізації часу проведеного біля ВНП;

– застосовувати і чітко дотримуватись часу очікування (час очікування передбачає період, коли оператор не може покидати пункт управління). Часи очікування необхідні для того, щоб після здійснення будь-яких дій над ВНП, пристрій стабілізувався і оператор міг здійснити безпосередній підхід;

– подальший пошук на вторинні вибухові пристрої здійснювати тільки після знешкодження основного вибухового пристрою;

– використовувати місцевість у районі знешкодженого вибухового пристрою тільки після перевірки на наявність вторинного саморобного вибухового пристрою (СВП);

– якщо дозволяє час, операції зі знешкодження повинні плануватись до їх безпосереднього проведення (краще передбачити будь-які загрози та їх наслідки, ніж протистояти обставинам у процесі роботи);

– командири повинні розставляти пріоритети при виконанні завдань із метою успішного проведення операції.

При виборі місця пункту управління (ПУ) для знешкодження ВНП старший розрахунку (оператор) повинен обрати:

– безпечну робочу зону для своєї групи та впевнитись у відсутності вторинних СВП, можливостей розльоту осколків (уламків) від ВНП;

– забезпечити визначене місце достатнім захистом від наслідків спрацювання ВНП

та його осколків (уламків).

Уточнити та перевірити:

– визначене місце для ПУ зразка РК, провести його ретельну перевірку перед початком виконання завдання;

– існування можливих загроз розрахунку (оператору) зразка РК зі знешкодження ВНП на місцевості;

– існування загрози ураження противником вибраного місця ПУ зразком РК при знешкодженні ВНП, наявність сил та засобів у групі охорони для забезпечення захисту розрахунку (оператора) РК під час виконання завдання;

– достатність місця для маневрування роботизованою системою при висуванні до місця виявлення ВНП з ПУ та при його поверненні у вихідне положення;

– забезпечення ПУ достатнім рівнем захисту від можливих розвідувальних дій противника та його засобів ураження.

Пошук та виявлення ВНП включає:

– визначення демаскуючих ознак встановлених ВНП (сліди свіжої землі, залишені на місцевості упаковки від ВНП і підривників, паперові етикетки, кинутий інструмент і знаряддя тощо), підтвердження небезпеки вибухової загрози, маркування місця встановлення ВНП;

– очищення місцевості та виставлення оточення із дотриманням безпечних відстаней;

– визначення та встановлення пункту контролю;

– здійснення доповіді про випадок або інцидент рапортом по команді;

– виклик групи знешкодження ВНП, здійснення контролю на місцевості до прибуття групи знешкодження.

При ідентифікації в процесі роботи групи знешкодження ВНП визначаються:

– загальні дані про вибуховий пристрій і його конструкцію;

– фіксація місця виявлення і стан ВНП, положення рухомих деталей і частин з урахуванням їх стану;

– вражаюча дія (фугасна, осколкова, запалювальна, комбінована);

– тип механізму приведення в дію (механічний, вогневий, електричний, радіокерований або хімічний);

– принцип спрацьовування: миттєвої дії (при відкритті кришки, нахилі корпусу, зняття з місця встановлення, після закінчення часу сповільнення) або при якому-небудь впливі (механічному, світловому, зміні параметрів зовнішнього середовища, тощо);

– наявність систем та елементів протидії спробам вилучення або знешкодження;

– перелік виробів, матеріалів і речовин, використаних як основний заряд вибухової речовини, корпус заряду, засоби ініціювання, механізму приведення в дію, камуфляж, осколкові елементи та інші складові ВНП;

– можливість переміщення ВНП.

Під час виконання завдань інженерної підтримки зразки РК подолання ІЗ можуть застосовуватися у складі підрозділів інженерної розвідки, інженерно-саперних, розмінування, розгородження (штурму) та елементах бойового порядку:

– групах розгородження (штурму);

– загонах забезпечення руху;

– групах (загонах) розмінування.

Науково-технічний прогрес інноваційних технологій розширює можливості застосування НРК в умовах ведення бойових дій. З урахуванням досвіду ведення бойових дій та досягнутого рівня розвитку озброєння та військової техніки і технологій визначено основні завдання, які доцільно покласти на РК, принципи та умови їх застосування, у тому числі з метою подолання ІЗ.

Реалізація ідеї застосування РК з метою проведення подолання ІЗ дозволить зменшити втрати особового складу та досягнути рівня спроможностей підрозділів Сил

підтримки ЗС України, якого неможливо досягнути існуючими екіпажами під час подолання ІЗ.

Крім того, визначений вище перелік покладених на РК завдань інженерної підтримки не є вичерпним і може бути доповнений у зв'язку з постійним розвитком науки, озброєння та військової техніки та інноваційних технологій.

УДК 629.735:623.746.7

Басараб О.К., Мішенюк Р.М.

ЩОДО ЗБІЛЬШЕННЯ ДАЛЬНОСТІ ПОЛЬОТУ FPV-ДРОНІВ

Сучасні збройні конфлікти вимагають застосування сучасних інноваційних рішень та методів ведення війни. Так, в російсько-українській війні з 2022 року активно використовуються малі безпілотні літальні апарати (БпЛА) і на даний час можна впевнено стверджувати, що сучасна війна – це війна дронів [1]. Отже, одним з основних пріоритетів у війні з агресором є перевага у застосуванні БпЛА [2].

На сьогодні існує велике різноманіття БпЛА які суттєво відрізняються між собою як за формою та габаритами так і за призначенням та тактикою застосування тощо. Серед основних напрямків бойового застосування дронів можна окреслити наступні:

– ведення розвідки, моніторингу як наземної (надводної) обстановки так і повітряної;

– нанесення вогневого ураження;

– здійснення дистанційного мінування;

– здійснення логістичного забезпечення – доставка вантажів в небезпечні для іншої логістики місця;

– проведення радіоелектронної боротьби – радіоелектронна підтримка, радіоелектронне подавлення та радіоелектронний захист тощо.

Нанесення вогневого ураження може здійснюватись двома основними способами:

– доставка та скидання боєприпасу з поверненням дрону – типу «бомбер» ;

– ураження цілі дроном з боєприпасом – типу «камікадзе».

Найкращим видом БпЛА для ураження цілі за типом «камікадзе» є FPV-дрони. FPV-дрони – вид безпілотників, керування якими здійснюється за допомогою функції «вигляд від першої особи» (англійською абревіатура означає FPV – First Person View).

Одною з основних проблем застосування FPV-дронів є обмежена дальність їх польоту. При чому, дальність обмежуються різними факторами, а саме:

– особливості місцевості (рельєф, рослинність, забудова) – управління FPV-дронів здійснюється здебільшого на радіочастотах УКХ діапазону та вище, і суттєво залежить від прямої видимості між передавачем та приймачем;

– ємність акумуляторної батареї – на більшість FPV-дронів встановлюють акумуляторні батареї, що дозволяють перебувати в польоті від 20 до 40 хвилин в залежності від ємності самого акумулятора, ваги корисного навантаження, погодних умов, стилю управління дроном тощо;

– наявна радіоелектронна обстановка – завантаженість робочого діапазону радіочастот сторонніми випромінюваннями, радіоелектронна протидія противника.

Зазначені фактори значно обмежують тактику застосування FPV-дронів та вимагають шукати шляхи збільшення дальності польоту.

Серед можливих методів збільшення дальності польоту FPV-дрону варто зазначити наступні:

1. Підвищення ефективності антен – підняття антени вище на щоглах, закріплення на будівлях, деревах; використання направлених антен, з варіативністю поляризації; застосування нових прогресивних метаматеріалів;
2. Збільшення потужності передавача – застосування передавачів більшої потужності, здійснення примусового активного охолодження передавачів;
3. Правильний підбір радіочастот – частоти нижчого діапазону з більшою довжиною хвилі краще огинають перешкоди та проникають через матеріали;
4. Застосування більш ефективних протоколів дистанційного керування – TBS Crossfire, ExpressLRS, TBS Tracer – з дальністю дії до 40 км [3];
5. Збільшення ємності акумулятору та підвищення енергоефективності – застосування акумуляторних батарей з найкращим співвідношенням енергоємність/вага, зниження споживання електроенергії за рахунок застосування більш енергоефективних електродвигунів;
6. Використання ретрансляторів – застосування ретрансляційного обладнання як наземного базування, що не завжди можливо в бойових умовах, так і повітряного базування на інших дронах.

Таким чином, окреслено можливі шляхи для збільшення дальності польоту FPV-дронів, та можливі варіанти реалізації зазначених шляхів. Збільшення дальності польоту FPV-дронів, в свою чергу, збільшить варіативність тактики їх застосування. В подальших дослідженнях буде більш детально розглянуто найбільш перспективні методи.

Список використаних джерел

1. Басараб О.К. Радіон Н.В. Акустична пеленгація безпілотних авіаційних комплексів методом порівняння сигналів. Міжнародна науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» / Збірник тез доповідей (м. Харків, 14 березня 2024 р.). – Харків. – 2024. – 400 с.
2. The Commander-in-Chief of Ukraine’s Armed Forces on How to Win the War. The Economist. URL: https://Www.Economist.Com/By-Invitation/2023/11/01/The-Commander-In-Chief-Of-Ukraines-Armed-Forces-On-How-To-Win-The-War (дата звернення 13.03.2025)
3. Що таке ExpressLRS? Це найкраща система FPV на великі відстані? Чи краще за Crossfire? URL: https://www.gsmsota.ua/blog/stati/expresslrs/?srsltid=AfmBOooL5PTLwDsqgOnCczMbYsqjjpF59Gat9kCA8pjebw-MlLdpAOv7 (дата звернення 13.03.2025)

УДК 004.9: 519.81

Безкоровайний В.В.

ОПТИМІЗАЦІЯ ТОПОЛОГІЧНИХ СТРУКТУР МЕРЕЖ ВЕЛИКОМАСШТАБНОГО МОНІТОРИНГУ

Основною метою створення систем великомасштабного моніторингу є отримання, реєстрація та оперативна передача для аналізу даних про стан об’єктів, що розташовані на значній території. Залежно від особливостей об'єктів моніторингу для передачі даних використовуються мережі з різними структурами та мережевими технологіями [1-2]. Зміна території (множини об’єктів, точок чи засобів) контролю, вимог до оперативності та точності спостережень на певному етапі призводить до необхідності проведення реінжинірингу існуючих мереж моніторингу. Зважаючи на значні витрати, необхідні для створення й експлуатації мереж великомасштабного моніторингу,

нераціональність варіантів їхньої побудови, може призводити до значних економічних втрат. Реінжиніринг таких мереж передбачає вирішення комплексу задач оптимізації їх структури, параметрів її елементів та каналів передачі інформації, їх топології, технологій збору, передачі та обробки інформації. Задачі їхньої оптимізації розв'язуються за множиною показників (локальних критеріїв) оперативності, надійності, живучості, економічності $k_j(s)$, $j=\overline{1,m}$, які адекватно характеризують варіанти їхньої побудови на множині допустимих $s \in S$, з урахуванням специфічних обмежень та мають суттєві відмінності від традиційних задач проектування технічних об'єктів [3]. Недостатньо формалізованими до теперішнього часу вважаються задачі ранжування множини ефективних варіантів $s \in S^E$ й вибору найкращого серед них $s^o \in S^E$.

Одним із шляхів підвищення ефективності проектів великомасштабного моніторингу є удосконалення математичних моделей і методів підтримки прийняття проєктних рішень, які повніше враховують: специфіку задач реінжинірингу; неповну визначеність вхідних даних; знання та досвід проєктувальників (особи, що приймає рішення – ОПР), на основі яких визначаються співвідношення між функціональними $k_j(s) \in Q(s)$ і витратними $k_j(s) \in C(s)$ показниками якості проєктних рішень.

За результатами аналізу взаємозв'язків комплексу задач реінжинірингу мережі моделі кожної з них $ModTask_i$, $i=\overline{1,N}$ пропонується подавати у вигляді відображень:

$$ModTask_i : \{ InDat_{iE}, InDat_{iI}, Res_i \} \to DesDec_i, \; i=\overline{1,N}, \qquad (1)$$

де $InDat_{iE}, InDat_{iI}, Res_i, DesDec_i, i=\overline{1,N}$ – відповідно множина зовнішніх, внутрішніх вхідних даних, обмежень і розв'язок i-ї задачі комплексу; N – кількість задач, виділених у проблемі реінжинірингу мережі.

У запропонованій технології реінжинірингу мереж великомасштабного моніторингу пропонується використовувати ітераційну логічну схему оптимізації, що реалізує цикли процедур генерації варіантів структури, параметрів її елементів, каналів передачі інформації, їх топології, що чергуються з процедурами аналізу варіантів і вибору кращого з них [3]:

$$CirDes = < Tasks, In, Res, DesDec, ProcDec >, \qquad (2)$$

де $Tasks = \{ Task_i \}$ – упорядкована множина комплексу задач реінжинірингу мережі; $Task_i$ – i-та задача комплексу; In – множина вхідних даних задач комплексу; Res – множина обмежень для задач комплексу; $DesDec$ – множина розв'язків задач; $ProcDec$ – множина відображень (вирішувальних процедур), що ставлять у відповідність кожній парі $< InDat, Res >$ непусту підмножину розв'язків задач $DesDec$.

Для ранжування варіантів і остаточного вибору найкращого серед них пропонується використовувати критерій загальної ефективності $P(s)$, побудований на основі полінома Колмогорова-Габора [4]:

$$P(s) = \sum_{i=1}^{m} \lambda_i \xi_i(s) + \sum_{i=1}^{m} \sum_{j=i}^{m} \lambda_{ij} \xi_i(s) \xi_j(s) + \sum_{i=1}^{m} \sum_{j=i}^{m} \sum_{l=j}^{m} \lambda_{ijl} \xi_i(s) \xi_j(s) \xi_l(s) + \ldots \to \max_{s \in S^E}, \qquad (3)$$

де λ_j, λ_{ij}, λ_{ijl}, $i,j,l=\overline{1,m}$ – значення вагових коефіцієнтів локальних критеріїв та їх добутків; $\xi_i(s)$ – значення функції корисності варіанта s по i-му локальному критерію.

Для оцінки корисності значень локальних критеріїв $\xi_i(s)$, $i=\overline{1,m}$ пропонується використовувати функції, які мають найкраще значення комплексного показника «точність-складність», і дозволяють реалізувати лінійні, нелінійні опуклі, ввігнуті, S - і

Z -подібні залежності.

Встановлення значень вагових коефіцієнтів λ_j, λ_{ij}, λ_{ijl}, $i,j,l=\overline{1,m}$ в моделі (3) здійснюється з використанням експертних методів чи методу компараторної ідентифікації. Врахування похибки визначення вагових коефіцієнтів δ в адитивних згортках локальних критеріїв, як часткового випадку моделі (3), може бути здійснено з використанням співвідношення [3]:

$$P(s)=\left\{\frac{1}{m}\sum_{j=1}^{m}\left[\lambda_j\,\xi_j(s)\right]^{\beta}\right\}^{1/\beta},\quad \beta=-\log m/\log(1+\delta). \tag{4}$$

Для оптимізації мереж, у залежності від кількості їх елементів, пропонується використовувати методи спрямованого перебору та еволюційного синтезу, побудовані на основі генетичних алгоритмів [3].

Отримані результати можуть бути використані для підтримки прийняття рішень у технологіях оптимізації мереж екологічного, радіаційного, частотного моніторингу, моніторингу повітряного простору тощо. Їх використання за рахунок оптимізації топологічних структур дозволяє скорочувати витрати на створення та експлуатацію мереж. Напрямком для подальших досліджень може бути врахування множини локальних критеріїв та неповної визначеності вхідних даних задач [5].

Список використаних джерел

1. Wang Y. Network Monitoring and Performance Optimization of Large-scale Distributed System Based on Big Data Algorithm // 2024 Asia-Pacific Conference on Software Engineering, Social Network Analysis and Intelligent Computing (SSAIC), 2024. P. 281-287. https://doi: 10.1109/SSAIC61213.2024.00059.
2. Environmental Monitoring Systems: Review and Future Development / I. Šećerov, D. Dolinaj, D. Pavić and others // Wireless Engineering and Technology, 2019. Vol.10. No.1. P. 1-18.
3. Beskorovainyi V.V., Petryshyn L.B., Honcharenko V.O. Mathematical models of a multi-criteria problem of reengineering topological structures of ecological monitoring networks // Applied Aspects of Information Technology. 2022. Vol. 5 No.1. P. 11–24. https://doi.org/10.15276/aait.05.2022.1.
4. Beskorovainyi V. Combined method of ranking options in project decision support systems // Innovative Technologies and Scientific Solutions for Industries, 2020. No 4 (14). P. 13–20.
5. Bezkorovainyi V., Kolesnyk L., Gopejenko V., Kosenko V. The method of ranking effective project solutions in conditions of incomplete certainty // Advanced Information Systems, 2024. v. 8, no 2. P 27–38. https://doi.org/10.20998/2522-9052.2024.2.04.

УДК 004.9

Безкоровайний В.В., Драз О.М.

АДАПТАЦІЯ ЛОГІСТИЧНИХ МЕРЕЖ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

В умовах надзвичайних ситуацій (пандемії, військового стану, бойових дій тощо) в логістичних мережах порушуються існуючі ланцюги постачання. Це породжує проблеми та ризики, які суттєво впливають на якість логістичних процесів. За таких умов поряд з традиційними завданнями управління мережами виникають нові завдання, пов’язані з мінімізацією часу відновлення постачання, забезпечення необхідних рівнів

їх надійності, живучості тощо. Це може призводити до суттєвих змінам у структурах, топології, параметрах та технологіях функціонування мереж. Проєкти адаптації логістичних мереж у надзвичайних ситуаціях передбачають розробку планів дій, спрямованих на швидку реструктуризацію ланцюгів постачання для зниження залежності від зміни постачальників, мережі хабів чи окремих маршрутів [1]. Завдання оптимізації варіантів побудови мереж розв'язуються за множиною показників якості з урахуванням обмежень існуючих мереж та мають відмінності від традиційних задач їхнього проєктування [2–3].

Об'єктом дослідження є трирівнева централізована логістична мережа, яка зазнала ушкоджень внаслідок надзвичайної ситуації. Задача її адаптації розглядається у такій постановці. Задані: множина елементів мережі (елемент центр-відправник, елементи-вузли, елементи-споживачі), що залишилась після настання надзвичайної ситуації $I = \{ i : i = \overline{1,n} \}$; її топологічна структура s', що задається місцями розташування споживачів, терміналів (співпадають з місцями розміщення елементів), центру $i = 1$, а також зв'язками між центром, вузлами і споживачами $[s'_{ij}]$, $i, j = \overline{1,n}$ ($s'_{ij} = 1$, якщо між елементами мережі i та j існує безпосередній зв'язок та $s'_{ij} = 0$ – за відсутності безпосереднього зв'язку); наведені витрати на створення $[c_i]$, $i = \overline{1,n}$, адаптацію $[d_i]$, $i = \overline{1,n}$ вузлів, реалізацію перевезень $[e_{ij}]$, $i, j = \overline{1,n}$; вартість ресурсів, які можуть бути повторно використані у новій мережі $[g_i]$, $i = \overline{1,n}$. При цьому без втрати загальності можна вважати, що вузли мережі розміщуються у безпосередній близькості від споживачів.

Необхідно визначити найкращі варіанти топологічної структури логістичної мережі $[s_{ij}]$, $i, j = \overline{1,n'}$ для максимально швидкого відновлення постачання $s_0^o \in S^*$ (де S^* – множина допустимих варіантів), для постачання з мінімальними наведеними витратами $s_z^o \in S^*$ і ефективну траєкторію адаптації варіанту побудови мережі від s_0^o до s_z^o.

Множина допустимих варіантів побудови централізованої трирівневої логістичної мережі визначається умовами [3–4]:

$$S^* = \{s\} = \begin{cases} [s_{ij}],\ s_{ij} \in \{0,1\},\ i, j = \overline{1,n},\ s_{11} = 1; \sum_{i=j}^{n} s_{ij} \geq 1\ \forall j = \overline{1,n}; \\ \sum_{j=1}^{n} \sum_{i=j}^{n} s_{ij} = n + \sum_{i=1}^{n} s_{ii},\ s_{ii} = 1 \rightarrow s_{i1} = 1\ \forall i = \overline{1,n}; \\ s_{ii} \wedge s_{ij} = 1 \rightarrow ij = \arg \min\limits_{1 \leq i, j \leq n} c_{ij}\ \forall i, j = \overline{1,n}. \end{cases} \quad (1)$$

Варіанти адаптації топологічної структури мережі задаються кількістю вузлів u, місцями їх розміщення $s_{ii} = 1$, $i = \overline{1,n}$ та схемою зв'язків між елементами $[s_{ij}]$, $i, j = \overline{1,n}$.

При розв'язанні задачі оптимізації топологічної структури за показником максимально швидкого відновлення постачання $s_0^o \in S^*$ необхідно визначити варіант під'єднання споживачів до уцілілих вузлів за мінімальними витратами на перевезення:

$$s_{ii} \wedge s_{ij} = 1 \rightarrow ij = \arg \min\limits_{1 \leq i, j \leq n} c_{ij}\ \forall i, j = \overline{1,n}.$$

Для розв'язання цієї задачі можна використовувати алгоритм повного перебору, який має лінійну часову складність $O[u \cdot n]$.

Цільова функція для задачі постачання з мінімальними наведеними витратами

$s_z^o \in S^*$ матиме такий вигляд:

$$C(s', s) = \sum_{i=1}^{n} [c_i(1 - s'_{ii})\, s_{ii} + d_i s'_{ii} s_{ii} - g_i(1 - s_{ii}) s'_{ii}] + \sum_{j=1}^{n} \sum_{i=j}^{n} [e_{ij}(1 - s'_{ij})\, s_{ij}] \to \min_{s \in S^*}. \qquad (2)$$

Загальна кількість можливих варіантів топологічних структур у цій задачі для кількості терміналів $1 < u \le n/2$ становить порядку $2^n / 2$. Для оптимізації мереж з відносно невеликою кількістю елементів n доцільно використовувати методи спрямованого перебору, а для мереж з великою кількістю елементів – методи еволюційного синтезу, побудовані на основі генетичних алгоритмів [3].

При плануванні траєкторії трансформації мережі в рамках еволюційної стратегії від s_0^o до s_z^o здійснюється розв'язання множини задач (1) - (2). При цьому варіанти побудови мережі на кінцевому s_z^o і поточному етапі s_k^o слугують додатковим обмеженням для вибору варіанту на наступному етапі s_{k+1}^o.

Отримані результати можуть бути використані для підтримки прийняття рішень у технологіях адаптації логістичних мереж різного призначення до нових умов за наслідками надзвичайних ситуацій. Їх використання дозволить з мінімальними витратами скорочувати час відновлення постачання та оптимізувати постачання після стабілізації ситуації. Напрямком подальших досліджень у цій галузі можуть бути врахування у моделях оцінок побудови мереж за множиною локальних критеріїв, неповної визначеності вхідних даних щодо попиту, функціональних та вартісних характеристик обладнання вузлів і транспортних засобів [5].

Список використаних джерел

1. Морозов О. О. Методика розв'язання задачі синтезу топологічної та функціональної структур систем ремонту озброєння і військової техніки // Науковий вісник Київського інституту національної гвардії України, 2023. №1. С. 6–10.
2. Beskorovainyi V., Kuropatenko O., Gobov D. Optimization of transportation routes in a closed logistics system // Innovative Technologies and Scientific Solutions for Industries, 2019. No. 4 (10). P. 24-32.
3. Beskorovainyi V., Sudik A. Optimization of topological structures of centralized logistics networks in the process of reengineering // Innovative Technologies and Scientific Solutions for Industries, 2021. No. 1 (15). P. 23–31.
4. Безкоровайний В.В., Нефьодов Л.І., Русскін В.М. Математична модель структурно-топологічної оптимізації логістичних мереж // Вісник Харківського національного автомобільно-дорожнього університету, 2021. № 95. С. 178–184.
5. Безкоровайний В.В., Русскін В.М., Тітов С.В. Математична модель задачі оптимізації логістичних мереж в умовах інтервальної визначеності вхідних даних // Вісник Харківського національного автомобільно-дорожнього університету, 2023. №103. С. 95–103.

Бєрнік Є. В., Худов Г. В.

МЕТОД ВИЗНАЧЕННЯ КООРДИНАТ РОЗВІДУВАЛЬНИХ БПЛА МЕРЕЖЕЮ ДВОХ SDR ПРИЙМАЧІВ

Сучасні умови ведення російсько-української війни показали, що безпілотні літальні апарати (БпЛА) відіграють критичну роль у розвідці та веденні бойових дій. Тому, одну із найбільших загроз для підрозділів Збройних Сил України та цивільного населення становлять розвідувальні БпЛА, головна мета яких – це збір інформації, коригування

артилерії та навіть нанесення кібератак. Складність виявлення та визначення координат таких БпЛА обумовлена малими висотами їх застосування та низькими значеннями ефективної поверхні розсіювання (ЕПР). Це, в свою чергу, ускладнює виявлення таких повітряних об'єктів існуючим радіолокаційними станціями радіотехнічних військ.

З метою вирішення даної проблеми є розробка методів виявлення і визначення координат БпЛА в мережі пасивної локації. Елементом мережі прийнято Software Defined Radio (SDR) приймач.

Відомо, що в розвідувальних БпЛА є декілька основних каналів зв'язку (командний канал, телеметричний канал, канал видачі цільової інформації, канал ручного управління, канал супутникової навігації). Встановлено, що основними джерелами інформації для SDR приймачів є сигнали від вищевказаних каналів БпЛА.

Проведений аналіз дозволив обґрунтувати можливість використання таких сигналів для підвищення відношення «сигнал/шум» за рахунок використання системи пасивних приймачів. Саме система пасивних приймачів є споживачами сигналів бортових систем БпЛА. Це, в свою чергу, призводить до підвищення точності визначення координат розвідувальних БпЛА.

Таким чином, запропоновано удосконалений метод визначення координат безпілотного літального апарату (БпЛА) мережею двох SDR приймачів. Враховуючи те, що в мережі SDR приймачів методи визначення координат повітряного об'єкту повинні бути простими, використано тріангуляційний метод. Місцеположення БпЛА визначається по кутовим напрямам на джерело випромінювання, що виміряні двома SDR приймачами (SDR1, SDR2), шляхом вирішення тріангуляційної задачі.

Удосконалений метод визначення координат безпілотного літального апарату (БпЛА) мережею двох SDR приймачів передбачає: введення вхідних даних; вимірювання пеленгів повітряного об'єкта; визначення координати X повітряного об'єкта; визначення координати Y повітряного об'єкта; визначення дальності до повітряного об'єкта; перевірка знаходження БпЛА в зоні дії мережі SDR приймачів; при знаходженні БпЛА в зоні дії мережі SDR приймачів координати БпЛА оновлюються; в іншому випадку – проводиться визначення траєкторії польоту БпЛА.

Встановлено, що найменшу помилку вимірювання координат можна забезпечити при знаходження БпЛА на траверсі до середини бази (кут спостереження від середини бази дорівнює 90º) і коли відстань до БпЛА близька до величини бази.

Проведено оцінювання точності визначення координат БпЛА мережею двох SDR приймачів. Встановлено, що похибки вимірювання координат БпЛА складають (250–350) м у достатньо широкому діапазоні напрямів (кут спостереження від середини бази (30º–60º)). При зменшенні величини бази похибки швидко зростають (досягають величину більше 1000 м) при відхиленні кута спостереження від напрямку 90º.

Таким чином, удосконалено метод визначення координат БпЛА мережею двох SDR приймачів, який, на відміну від відомих, передбачає:

- використання сигналів бортових систем БпЛА;
- у якості елементів мережі використання SDR приймачів;
- використання тріангуляційного методу визначення координат БпЛА.

УДК 355.424.3

Биков О.М., Пришляк І.В., Дидюк В.Г.

РОЗРОБКА НАВЧАЛЬНО-ЛАБОРАТОРНОГО СТЕНДУ ДЛЯ ДОСЛІДЖЕННЯ СИСТЕМ УПРАВЛІННЯ ДВИГУНАМИ ЗРАЗКІВ ВІЙСЬКОВОЇ ТЕХНІКИ

Сьогодні більша частина зразків військової техніки закордонного виробництва

обладнана електронною системою управління двигуна [1, 2]. Це дає змогу максимально оптимізувати роботу двигуна для підвищити його коефіцієнт корисної дії, збільшити ресурс та міжремонтні інтервали, застосувати внутрішні алгоритми самодіагностики для попередження випадків виходу з ладу, зменшити температуру вихлопних газів для забезпечення малопомітності [3]. Обслуговування цих системи потребує спеціальних навичок, досвіду роботи та глибоких теоретичних знань. Для здобуття таких навичок слухачі під час навчання на практичних заняттях повинні наочно вивчати не тільки будову та функціонування таких систем, а досліджувати алгоритми роботи, форми та рівні сигналів з датчиків та сигнали управління виконавчими механізмами системи управління двигуном за допомогою спеціалізованих вимірювальних приборах [4]. Після засвоєння алгоритмів роботи електронних систем управління двигуном повинні вивчити особливості ремонту та обслуговування конкретних систем на зразках військової техніки за фахом підготовки [5].

Одним з основних критеріїв при створенні подібного обладнання є його універсальність і мобільність [6, 7]. На ринку України представлено продукцію, яка призначена для вивчення роботи електронних систем управління автомобіля. Наприклад, у роздрібній торгівлі можна придбати лабораторний стенд «Система живлення інжекторного двигуна з автоматичним управлінням» НТЦ-1540. Стенд являє собою зібрану систему управління двигуна в корпусі вагою 85 кілограм. У ньому виведені основні виконавчі пристрої, де наочно імітується їхня робота. Цей стенд дає можливість вивчати всі елементи системи подачі пального двигуна та імітувати основні його несправності. Вартість такого стенда становить близько 150000 грн. Переваги цього стенда в тому, що слухач може вивчати роботу електронної системи подачі пального двигуна, як за їх напругою живлення, так і візуально за факелом розпилення палива. На жаль, його призначення проглядається тільки в закріпленні теоретичних знань з будови системи подачі пального двигуна. Основні недоліки – це відсутність візуального розташування всіх елементів техніки, до того ж немає реальної роботи двигуна, а тільки його імітація, що не дає змоги привести процес вивчення тонкощів ремонту та обслуговування до реальних умов.

Пропонується створити навчально-лабораторного стенд, який буде інтегровано в наявну матеріальну базу (зразок військової техніки) та збереже розташування всіх елементів системи управління двигуна на своїх місцях та матиме мінімальну собівартість. Таке рішення забезпечить швидкий доступ до діагностичних параметрів загальнодоступними засобами вимірювання з можливістю імітації несправності, пов’язаних з відмовою елементів системи управління. Дана розробка спрямована на мінімізацію часу підготовки до лабораторних або практичних робіт з можливістю більш глибокого вивчення симптомів несправності та способів їх усунення. Так само дасть змогу проводити вивчення впливу несправності на функціонування системи управління та енергетичні характеристики двигуна. Такого рівня підготовка дасть змогу слухачам одержати величезний досвід роботи з такими системами, а так само підвищити свою кваліфікацію.

Електронна система управління двигуном (ЕСУД) складається з кількох частин: електронного блока, що дає змогу обробляти інформацію та видавати сигнал управління на виконавчі пристрої, системи датчиків для вимірювання фізичних параметрів з подальшим перетворюванням в інформацію у вигляді сигнал визначеного рівня та форми, виконавчих пристроїв роботою яких керує електронний блок управління. Основна мета проведення досліджень роботи електронного блоку управління за допомогою навчально-лабораторного стенду полягає в тому, щоб здійснювати спостереження та контроль за вимірювальною та виконавчою частиною системи управління двигуном безпосередньо на зразку техніки під час роботи двигуна. Звідси усі вимірювальні та керівні сигнали повинні проходити через даний стенд, де можна бути провести вимірювання та зняти їх характеристики (форми сигналів, рівень

напруги, тощо) за допомогою осцилографу та мультиметру. Запропонований навчально-лабораторний стенд інтегрується в кола електроживлення в місцях з'єднання роз'ємів та шин передачі даних.

Кожен елемент ЕСУД у процесі експлуатації може вийти з ладу, що може впливати на стабільність роботи двигуна або його відмову. Причиною цього може бути тривала експлуатація, вплив зовнішніх чинників, несправність кола живлення, несвоєчасне планове обслуговування, якість електронних елементів та комплектуючих системи. Тому для повноти проведення досліджень системи управління двигуна необхідно імітувати несправності для спостереження їх впливу на роботу двигуна. Імітувати обрив або замикання кола живлення пропонується за допомогою перемикачів. Імітувати несправності датчиків та виконавчих пристроїв у своїх колах живлення за допомогою змінних опорів для штучного створення похибок у вимірах або падіння напруги в колах живлення додаткових пристроїв.

Застосування даної елементної бази визначає низьку собівартість стенду, оскільки це завдання на сьогоднішній день можна виконати програмно на мікроконтролері, але такий спосіб потребуватиме додаткових коштів і часу.

Запропонований навчально-лабораторний стенд не обмежується застосуванням до одного зразка техніки, він може використовуватися й на іншому зразку техніки з аналогічною системою управління, оскільки він не є стаціонарним. Для його під'єднання до разка техніки знадобиться переобладнання електропроводки, що полягає в додаванні в її кола живлення кількох роз'ємів, які приєднуватимуться до стенду. Таким чином, операція підключення до ЕСУД становить лише кілька кроків і займає мінімум часу.

Додатково до стенду можуть бути виведені індикатори, для контролю викладачем за діями слухачів при пошуку несправності ЕСУД, а також діагностична колодка, для зручності підключення діагностичних приладів. Так само є можливість за допомогою генератора сигналів і осцилографа здійснювати дослідження та принцип роботи виконавчих пристроїв без запуску двигуна, що дозволяє проводити роботи в боксах і лабораторіях без системи вентиляції відпрацьованих газів і зберігати ресурс двигуна.

Впровадження запропонованого навчально-лабораторного стенду в освітній процес і підготовки фахівців обслуговування та ремонту зразків військової техніки дає змогу значно підвищити рівень підготовки у сфері обслуговування, ремонту та проектування систем управління. Так само, подібні методи підготовки можуть використовуватися не тільки на військовій техніці, а й на бронетехніці, тракторах, дорожньо-будівельній та спецтехніці. Вони дадуть змогу набувати практичних знань в роботі системи управління двигунів, трансмісій, керованої підвіски, системам безпеки, систем управління озброєнням, а також спеціальними приводами і пристроями.

Список використаних джерел

1. O. Daki, S. Herasimov and H. Zubrytskyi, **Digital Correlation Method For Power Measurement**, *Information Processing Systems*, № 4 (163), 2020, p.p. 15-26, https://doi.org/10.30748/soi.2020.163.02.
2. S. Herasimov, M. Pavlenko, E. Roshchupkin and etc. **Aircraft flight route search method with the use of cellular automata**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, is. 4, 2020, p.p. 5077-5082, https://doi.org/10.30534/ijatcse/2020/129942020.
3. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.
4. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022,

p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.
5. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference «Application of information technologies in the preparation and operation of law enforcement forces»*, March 15, 2022, p.p. 31-32.
6. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference «Scientific Trends and Trends in The Context of Globalization»*, UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.
7. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

Бокачов С.В., Чаган Ю.А., Марцінко Н.М., Варванець Ю.В.

ПОТРЕБА РОЗВИТКУ СИСТЕМИ УПРАВЛІННЯ ЛОГІСТИЧНИМ ЗАБЕЗПЕЧЕННЯМ ВІЙСЬКОВИХ ФОРМУВАНЬ ЗСУ ТА ПРАВООХОРОННИХ ОРГАНІВ ПІД ЧАС ВИКОНАННЯ НИМИ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ В СУЧАСНИХ УМОВАХ

Світовий досвід застосування військових формувань у збройних конфліктах і досвід ведення бойових дій Збройними Силами України у взаємодії з військовими формування ми інших сил оборони і безпеки держави (СО і БД) у війні з рф свідчить про домінуючу роль процесів управління. При цьому вирішальне значення має інформаційно-аналітична перевага, за рахунок якої досягається підвищення оперативності процесів управління, скорочення циклів управління і як наслідок - підвищення ефективності виконання визначених завдань об'єднаними угрупуваннями військ, до складу яких входять сили та засоби ЗСУ та інших складових сектору СО і БД.

У зв'язку з насиченістю підрозділів і частин СО і БД великою кількістю різноманітної бойової та спеціальної техніки і озброєння як вітчизняного, так і іноземного виробництва, а також її застосування і тактики ведення бойових дій, значно ускладнюється і відповідно зростає роль системи логістичного забезпечення (ЛЗ), виникає потреба удосконалення системи управління нею, що передбачає впровадження в її роботу сучасних алгоритмів і методів роботи, удосконалення наявних і створення сумісних пунктів управління ЛЗ, створення єдиної системи автоматизованого управління ЛЗ під час виконання завдань із захисту держави. Сучасні умови ведення бойових дій диктують свої правила: якщо ще не так давно була можливість підвозити засоби матеріального забезпечення (МЗ) за 2-3 км до передових позицій, то у зв'язку з масовим застосуванням противником різноманітних ударних БпЛА ця відстань збільшилась до 5-7 км, а інколи і більше. Тенденція збільшення дальності дії БпЛА продовжує зберігатись, що в свою чергу відсуває безпечну лінію підвозу МЗ. В багатьох випадках доставка МЗ військовослужбовцями здійснюється навіть у пішому порядку, що значно зменшує його обсяги та збільшує час виконання. Такий стан забезпечення підрозділів вимагає застосування нових засобів доставки МЗ, якими можуть бути легкові автомобілі, квадроцикли, а також спеціальні вантажні БпЛА і роботизовані наземні комплекси (РНК). Таким чином процес МЗ ускладнюється, що, в свою чергу, вимагає додаткових зусиль на реалізацію завдань ЛЗ.

Ступінь реалізації усіх завдань ЛЗ в сучасних умовах знаходиться у безпосередній залежності від ефективності управління під час їх підготовки та у ході виконання. Тому

одним з основних напрямків удосконалення управління системою ЛЗ є автоматизація найбільш трудомістких інформаційних процесів.

Інтенсивність ведення бойових дій висуває необхідність підвищення ефективності дій підрозділів (частин), процес управління якими найбільш динамічний, і цьому мають відповідати завдання ЛЗ, щодо їх забезпечення. В АСУ бригади інтегрована АСУ ЛЗ, тому автоматизація процесів управління нею сьогодні є особливо актуальною. При цьому необхідно зосередитись на таких її складових як системи зв`язку, інформаційного забезпечення і захисту інформації. Щодо аналітичної системи, її інформаційно-розрахункових задач і моделей, то ця складова повинна нарощуватись постійно в ході подальшого удосконалення ЄАСУ, при цьому особливу увагу необхідно звернути на надійний захист (закриття каналів) комутаційної складової АСУ, функціонування системи в умовах РЕБ, підвищення функціонування АСУ в ланці бригада-батальйон-рота під час ведення активних дій. Система управління ЛЗ має бути на такій функціональній основі, яка б включала управління підрозділами і частинами ЛЗ з новітніми засобами ЛЗ, які відповідають вимогам сьогодення в системі логістичного забезпечення ЗСУ, а також спрягалася із системами ЛЗ підрозділів і частин інших СО і БД.

АСУ ЛЗ повинна надати можливість службовим особам, командирам тилових підрозділів різних рівнів управління відповідного доступу до загальної інформаційної бази для отримання і передачі інформації, замовлення необхідних матеріальних засобів; огляду району дій, збору і аналізу інформації про розташування техніки і озброєння бойових підрозділів, а також їх потреб, розташування підлеглих підрозділів (органів) матеріального забезпечення, їх стану і можливостей, а також сил і засобів матеріального забезпечення всіх інших силових структур в районі дій. Наявність доступу до системи АСУ ЛЗ сприяє також отриманню своєчасної інформації про забезпеченість бойових підрозділів і частин матеріальними засобами, дозволяє проводити аналіз і оцінку їх стану та приймати в стислі терміни обґрунтовані рішення, щодо їх забезпечення, виходячи з можливих варіантів ведення бою (дій), що визначені старшим командиром, якісно готувати підлеглих до виконання завдань.

Виходячи з практичного досвіду, командири тактичного рівня сьогодні приділяють ЛЗ досить велику увагу як при підготовці, так і в ході виконання завдань, що напряму пов’язано з умовами ведення бойових дій. Наприклад, планування заходів щодо матеріального забезпечення підрозділів першого ешелону може здійснюватися лише в періоди ранкових або вечірніх сутінок («по-сірому»), коли застосування противником БпЛА без тепловізорів малоефективно, застосування на техніці забезпечення засобів РЕБ для їх захисту, використання маршрутів постачання, де вже діють системи РЕБ старшого командира та багато інших нюансів. Крім того, у зв’язку з неможливістю доставки безпосередньо в підрозділи, що діють розосереджено, призначаються додаткові точки розвантаження МЗ звідки здійснюється постачання до підрозділів різними способами і засобами. Таким чином обсяг інформації, що підлягає обробці, постійно збільшується.

Обсяг інформації, який обробляється і передається до органів ЛЗ вручну, має затримку по часу, що збільшує цикл управління. Наявність же доступу до АСУ ЛЗ невеликих підрозділів тактичного рівня надасть можливість всім органам ЛЗ оперативно одержувати інформацію, самостійно планувати виконання замовлень і свої дії відповідно обраного командиром варіанту дій ще до отримання розпорядження старшого органу управління. У критичні моменти бою (дій) частина сил ЛЗ або весь орган, що пересувається для забезпечення одного з підрозділів, може бути спрямований в стислі терміни для забезпечення іншого. Все це дозволить командирам більше зосереджувати свою увагу на підготовку та виконання основного завдання.

Наявність АСУ ЛЗ, яка інтегрована в загальну систему бойового управління і суміщається з іншими системами управління, в тому числі й інших підрозділів і частин

СО і БД, є вирішальним фактором здійснення якісного та ефективного ЛЗ об'єднаного угрупування військ, яке виконує сьогодні одне завдання із захисту держави незалежно від приналежності його складових до різних силових структур. Вона дозволить спостерігати за переміщенням всіх без винятку сил і засобів в системі ЛЗ, оперативно відстежувати проблеми, які виникають з питань ЛЗ, і своєчасно реагувати на них.

Створення і розгортання інтегрованої інформаційної системи ЛЗ частин Збройних Сил України виходячи з умов ведення бойових дій і отриманого досвіду на всіх рівнях управління має суміщуватись з подібними системами частин інших складових СО і БД, що значно спрощує управлінські процеси в системі ЛЗ. Вона забезпечує здійснення управління в реальному масштабі часу, оптимізацію процесів обробки і обміну даними в усіх ланках управління, надасть вільний доступ користувачам за своїм рівнем до ресурсів системи, що в кінцевому результаті сприятиме ефективному виконанню завдань об'єднаному угрупуванню військ.

УДК 623.437.4-047.58:007.5

Бриженюк Ю.Д., Братченко Г.Д., Лукаш Р.В.

НАПРЯМИ ПІДВИЩЕННЯ ЖИВУЧОСТІ БЕЗПІЛОТНИХ НАЗЕМНИХ КОМПЛЕКСІВ В УМОВАХ БОЙОВИХ ДІЙ

Стрімкий розвиток та впровадження інтелектуальних технологій та сучасних засобів телекомунікації значно підвищив роль застосування безпілотних авіаційних комплексів (БпАК), а останнім часом також безпілотних наземних комплексів (БпНК) в російсько-українській війни. Досвід повномасштабної збройної агресії російської федерації дозволяє визначити переваги та недоліки бойового застосування БпНК. Основною перевагою, безумовно, є можливість збереження життя людей на лінії бойового зіткнення. Вже зараз, завдяки масованому застосуванню БпАК, втрати важкої техніки стають надто великими. Значно ускладнюються можливості переміщення особового складу, постачання боєприпасів та інших матеріально-технічних засобів.

В умовах постійної загрози ураження артилерією у комплексі з розвідувальними БпАК, БпАК камікадзе або зі скидом мін застосування БпНК для виконання найбільш небезпечних бойових завдань є перспективним досягнення для успіху в бою з мінімальними втратами особового складу. При цьому важливою проблемою застосування БпНК є забезпечення такої їх живучості в бойових умовах, яка б дозволяла виконувати бойові завдання з допустимим рівнем втрат БпНК.

Для прогнозування допустимого рівня втрат БпНК в районі бойових дій пропонується застосовувати ймовірнісні моделі масового обслуговування, а за умов одночасного застосування дуже великої кількості БпНК – динаміки середніх [1]. При розробці моделі потрібно ураховувати ймовірності: виявлення та викриття БпНК наявними у противника розвідувальними засобами; ураження БпНК різноманітними вогневими засобами противника у разі його викриття; втрати стійкості під дією зовнішнього середовища (метеорологічних умов, рельєфу і перепон на місцевості, впливу радіоперешкод та інших факторів); виходу з ладу критичних складових БпНК в процесі виконання завдання. Для оцінки цих ймовірностей потрібно ураховувати значну кількість факторів впливу, що потребує розробки окремих математичних моделей. Кожна з таких моделей дозволить обґрунтовувати вимоги до характеристик БпНК, які визначають його живучість.

Перевірка адекватності моделей можлива шляхом відтворення умов застосування БпНК з урахуванням реального досвіду бойового застосування.

Успішність застосування БпНК суттєво залежить від його є живучості, тобто здатності зберігати та відновлювати свою працездатність в умовах впливу негативних зовнішніх факторів (радіоелектронного та вогневого впливу противника, складних погодних умов тощо).

Моделювання варіантів застосування БпНК в типових умовах сучасного бою має дозволити оцінювати вплив різних технічних рішень для підвищення їх живучості. За результатами моделювання можуть обиратись рішення, реалізація яких є доцільною за критерієм ефективність/вартість. Успішність БпНК також змінюється в залежності від способів їх застосування. Наприклад, масованість застосування дешевих БпНК, частина з яких виконує завдання з відволікання або введення в оману противника, може виявитись доцільнішою за розробку більш захищених, але дорогих зразків.

Процес застосування БпНК за призначенням може бути представлений переходом комплексу в різноманітні ймовірнісні стани, як наприклад показано на рис. 1. Для розрахунку ймовірностей перебування БпНК у певному стані пропонується застосовувати ймовірнісні математичні моделі теорії пошуку, теорії стрільби і теорії надійності.

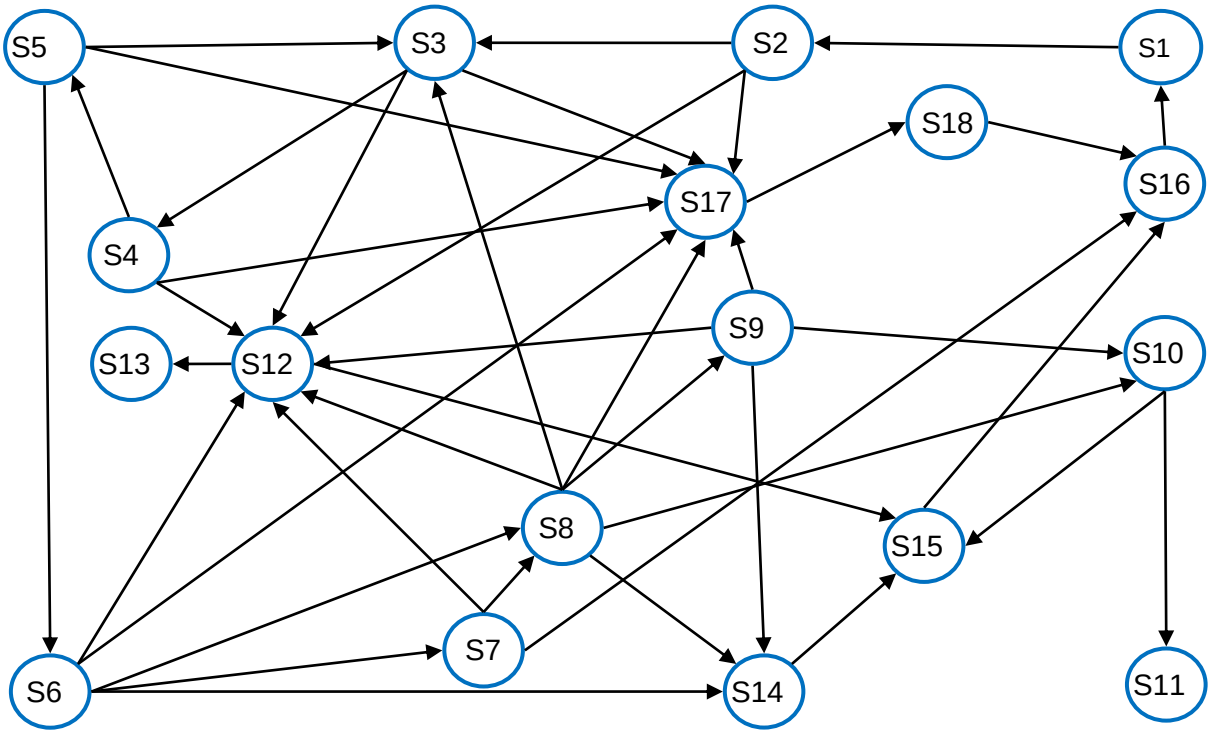


Рисунок 1 – Варіант графу станів перебування БпНК

Стани БпНК:
S1 – справний, готовий до застосування;
S2 – справний, застосовується, не розвіданий противником;
S3 – справний, застосовується, але розвіданий противником;
S4 – справний, застосовується, впливають засоби РЕБ противника;
S5 – втрата зовнішнього керування внаслідок впливу засобів РЕБ противника;
S6 – справний, застосовується з переходом в автономний режим;
S7 – справний, в автономному режимі повертається у визначене програмою місце;
S8 – справний, застосовується/ перебуває під впливом засобів вогневого ураження;
S9 – має пошкодження, знижені характеристики/застосовується за призначенням;
S10 – несправний в результаті вогневого ураження/не здатен виконувати завдання;
S11 – знищений противником в результаті вогневого ураження;
S12 – несправний в результаті підриву на міні/не здатен виконувати завдання;
S13 – знищений в результаті підриву на міні;

S14 – відмова/несправний/не здатен виконувати завдання;
S15 –доставка для ремонту;
S16 – обслуговування/ремонт для повернення в стрій;
S17 – виконав завдання за призначенням;
S18 – повертається у вихідне положення.

Наприклад, у припущенні закону експоненціального розподілу ймовірностей часу виявлення для кожного з технічних засобів розвідки (ТзР), ймовірність виявлення $P_{\text{вияв}}$ мобільної платформи зразка БпНК сукупністю з n ТзР противника хоча б один раз в процесі його спостереження на маршруті переміщення за час t [2]:

$$P_{\text{вияв}}(t) = 1 - \exp\left[-U(t)\right], \tag{1}$$

де $U(t)$ – розвідувальний потенціал сукупності з n ТзР, який є сумою потенціалів,

$$U(t) = \sum_{i=1}^{n} U_i(t), \tag{2}$$

в якому $U_i(t)$ для випадку неперервного пошуку з нестаціонарним пуасонівським потоком виявлень у проміжок часу (t_0, $t_0 + t$) обчислюється за співвідношенням [2]

$$U_i(t) = \int_{t_0}^{t_0+t} \gamma_i(t)dt, \tag{3}$$

де $\gamma_i(t)$ – змінна у часі інтенсивність потоку виявлень.

При проєктуванні зразка БпНК потрібно ураховувати необхідність зменшення ймовірності з його виявлення противником. Тобто, в конструкцію БпНК мають втілюватись технічні рішення спрямовані на зниження розвідувального потенціалу наявних у противника засобів ТзР.

В процесі виконання завдання БпНК може бути ціллю для N видів засобів ураження. Тому ймовірність бути не ураженим при виконанні завдання

$$P_{\text{неур}} = \prod_{i=1}^{N} (1 - P_{\text{ур}i}), \tag{4}$$

де $P_{\text{ур}i}$ – ймовірність ураження НРК i-м засобом ураження за результатами його розвідки на маршруті руху;

N – кількість різних типів засобів ураження БпНК у противника.

Кожна з ймовірностей $P_{\text{ур}i}$ оцінюється з урахуванням типових умов застосування та характеристик систем ураження.

Окрім можливості ураження вогневими засобами, БпНК може бути тимчасово виведений з ладу засобами радіоелектронного придушення (РЕП). У разі застосування засобів РЕБ важливою властивістю БпНК є здатність до автономного виконання завдання. Тому ймовірність придушення $P_{\text{РЕП}}$ має враховувати стійкість БпНК до впливу навмисних та ненавмисних радіозавад.

Для успішного виконання БпНК завдання він має бути технічно надійним, а також здатним оминати на своєму шляху невідомі перепони. Надійність зазвичай характеризується ймовірністю безвідмовної роботи P_c, тобто ймовірністю того, що протягом заданого проміжку часу Δt відмова не виникне. Ці фактори можуть впливати також і одночасно з вогневим впливом та в умовах впливу радіозавад [3].

Таким чином, підвищення живучості БпНК є одним з важливих напрямів їх удосконалення, оскільки, разом із зменшенням загрози життю людини, необхідною є їх здатність успішно виконувати завдання за призначенням у складних бойових умовах.

Математичне моделювання процесу бойового застосування БпНК з урахуванням особливостей сучасного бою є доцільним для обґрунтування оперативно-тактичних і окремих технічних вимог при їх проектуванні. Досвід бойового застосування БпНК може бути використаний при визначенні вихідних даних для моделювання.

Запропонований варіант графу станів перебування БпНК в процесі виконання завдання за призначенням є наближеним представленням процесу його застосування. Подальше удосконалення такої моделі передбачає обчислення часових залежностей ймовірностей переходу із стану в стан, що потребує розробки додаткових математичних моделей, подібних (1)-(4). Ймовірності перебування у певному стані в системі масового обслуговування (рис. 1) також будуть змінними у часі, і їх обчислення потребуватиме застосування методів чисельного моделювання.

Список використаних джерел

1. Вентцель Е.С. Исследование операцій. Москва. Сов. радио, 1972. 552 с.
2. Абчук В.А., Суздаль В.Г. Поиск объектов. М.: Сов. радио, 1977. 336 с.
3. Братченко Г.Д., Гончарук А.А., Абрамов С.В., Лукаш Р.В., Яструбенко О.В. Методика обґрунтування кількісного складу безпілотних систем для доставки вантажів. *Збірник наукових праць Військової академії (м. Одеса)*. 2023. № 2 (20). С. 73-86.

Бричинський О.В., Малюк В.М., Контуров В.М.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ПІДГОТОВКИ САПЕРНИХ ГРУП

Підготовка саперних груп під час дії воєного стану стала набагато складнішою через розвиток новітніх технологій, використання противником заборонених мін, саморобних вибухових пристроїв (СВП), а також необхідність гуманітарного розмінування після бойових дій.

Інформаційні технології (ІТ) відіграють важливу роль у підготовці саперів, сприяючи підвищенню ефективності, безпеки та точності їхньої роботи. Розглядається кілька основних напрямків, у яких ефективно застосовуються в навчанні та в підготовці саперів: моделювання вибухових ситуацій, геоінформаційні системи (ГІС), безпілотні літальні апарати (БПЛА), автоматизовані системи пошуку і знешкодження вибухонебезпечних предметів (ВНП), віртуальні тренажери та навчальні платформи, інформаційні системи для моніторингу та керування.

Моделювання вибухових ситуацій є важливим елементом підготовки саперів, оскільки дозволяє максимально наблизити навчання до реальних умов зберігаючи при цьому безпеку. Це дає змогу саперам розвивати необхідні навички для розпізнавання, знешкодження та безпечного поводження з вибуховими пристроями (ВП) в різноманітних умовах. Віртуальні тренажери створюють безпечне середовище для навчання саперів, де можна моделювати різні вибухові ситуації без ризику для життя. Такі системи дозволяють: моделювати різні типи вибухонебезпечних предметів (вибухові речовини, міни, снаряди, боєприпаси, саморобні вибухові пристрої), тренувати саперів у розпізнаванні типів ВП і обрані правильних методів для їх знешкодження, створювати реалістичні сценарії, де сапери повинні працювати в обмежених умовах часу або в складних погодних умовах. При моделювання поведінки ВП використовують симулятори. Вони імітують реальні дії вибухового пристрою, такі як: наявність або відсутність детонатора, чутливість до механічних пошкоджень, магнітність, зміни в умовах середовища, які можуть вплинути на вибух (погодні умови, вологість, температура). Симулятори можуть забезпечувати інтерактивне навчання, де сапер отримує зворотній зв'язок після кожної дії, а саме: якщо сапер обирає неправильний спосіб для знешкодження пристрою, симулятор може показати негативний результат і пояснити, чому вибір був помилковим також система може надати підказки та рекомендації щодо безпечного виконання завдання. Моделювання

вибухових ситуацій дозволяє створювати тренування в нічних умовах, пошук та знешкодження ВП у зонах з підвищеним рівнем радіації, хімічного чи біологічного забруднення, виконання завдання в міських умовах або в будівлі. Моделювання вибухових ситуацій дає змогу не лише тренувати саперів, а й аналізувати їхні дії , щоб покращити ефективність навчання, а саме: визначення часу, який необхідний для розпізнавання та знешкодження вибухового пристрою, оцінка точності прийнятих рішень і способів, створення звітів для подальшого аналізу і корекції навчальних програм. Симуляція реальних вибухових ситуацій дозволяє саперам тренуватися в умовах стресу та напруги, що є важливим для розвитку психологічної витривалості. Це допоможе саперам бути готовим до реальних бойових умов і зменшує ризик помилок у критичній ситуації. Прикладом програм для моделювання вибухових ситуацій: EOD Simulation Systems, Virtual Reality(VR) Training Simulators. Отже моделювання вибухових ситуацій – це важлива складова підготовки саперів, що дозволяє покращити їхню підготовленість до реальних завдань, знижуючи ризик та підвищуючи ефективність виконання завдань.

ГІС відіграють важливу роль у підготовці саперів, оскільки вони дозволяють зібрати, аналізувати та візуалізувати просторову інформацію для ефективного планування та проведення операції з розмінування. Завдяки використання ГІС сапери можуть точніше планувати свої дії, оцінювати небезпечні ділянки місцевості, а також підвищити рівень своєї безпеки. Система допомагає саперам створювати карти зон з підвищеною небезпекою, таких територій, де ймовірно можуть бути вибухонебезпечні предмети. Це дозволяє визначити небезпечні території за допомогою точних карт і супутникових знімків, враховувати історичні дані про можливе мінування територій, дані розвідки, а також розташування вибухонебезпечних об’єктів. ГІС дозволяє ефективно здійснювати моніторинг та планувати операції з розмінування, а саме: створювати детальні карти мінних полів та позначати місця знешкодження чи знищення ВП,проводити розрахунок безпечних маршрутів пересування саперів, аналіз рельєфу місцевості для оцінки доступності місцевості, вести облік виконання операцій.

Застосування БПЛА значно покращує процес підготовки саперів і підвищує ефективність розмінування. Вони дозволяють мінімізувати ризик для особового складу, покращують картографування мінних полів і прискорюють ідентифікацію ВНП. Дрони обладнані камерами високої роздільної здатності (оптичним, інфрачервоним та мультиспектральними), що дозволяє виявляти підозрілі об’єкти без фізичного наближення сапера, створювати 3D-моделі мінних полів для подальшого аналізу, використовувати тепловізори для знаходження металевих предметів під ґрунтом.

Під час навчань та реальних операцій дрони дозволяють командуванню та інструкторам відстежувати дії саперів в режимі реального часу, оцінити ефективність розмінування на великих територіях, фіксувати знайдені загрози для подальшого аналізу. Також деякі вантажні дрони можуть транспортувати спеціальні заряди для знищення ВНП або доставляти допоміжне обладнання сапера у важкодоступні місця. Використовують такі дрони: DJI Matrice 300 RTK, Parrot Anafi USA, Flyability Elios3, БПЛА»Лелека-100».

Сучасна підготовка саперів передбачає використання автоматизованих систем для підвищення ефективності пошуку, ідентифікації та знешкодження ВНП. Це зменшує ризик для сапера і дозволяє швидше розміновувати території, особливо у великих масштабах. Роботи-сапери використовуються для дистанційного знешкодження мін та інших ВНП, а саме: TALON, Mine Kafon Drone, UGV Cobra Mk2, M160. В підготовці використовуються для тренування операторів дистанційного керування, відпрацювання тактик розмінування у складних умовах та інтеграції роботів у спільному виконанні завдання з саперами.

Віртуальні тренажери та навчальні платформи дозволяють саперам тренуватися у безпечному середовищі, імітуючи реальні бойові умови. Ці платформи допомагають

підтримувати навички в роботі та знайомитись з новими ВНП та технологіями. Також застосовуються мобільні додатки для вивчення техніки знешкодження ВП, отримувати інформацію про мінні поля та небезпечні території, надавати важливі матеріали в реальному часі, що допомогає саперав в бойових умовах.

Інформаційні системи для моніторингу та керування забезпечують координацію між саперами, командуванням та іншими підрозділами. Використовуються такі системи: C4ISR Systems (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance), NATO EOD Command & Control System, SKIF Tactical Management System. Інформаційні системи значно покращують підготовку саперів, роблячи процес безпечнішим, ефективним і технологічно просунутим. Вони дозволяють моніторити ситуацію, аналізувати дані, координувати дії та покращувати освітню діяльність.

Застосування інформаційних технологій значно полегшують і підвищують безпеку роботи саперів, дозволяючи їм швидше та точніше використовувати завдання в умовах сучасності.

УДК 355.424.3

Бурак А.В., Воловоденко Ю.М., Мосійчук М.В.

ІМІТАЦІЙНА МОДЕЛЬ ДІАГНОСТУВАННЯ ТЕХНІЧНОГО СТАНУ ДВИГУНІВ БРОНЕТАНКОВОЇ ТЕХНІКИ

Працездатність і ефективність функціонування бронетанкової техніки залежить від своєчасного виявлення відмов у моторному відділенні, основою якого є двигун внутрішнього згоряння. На сьогодні переважна більшість рухомих об’єктів укомплектовується дизельними двигунами з урахуванням їх переваг [1, 2]. Тому, визначення технічного стану дизельних двигунів для своєчасного виявлення можливих відмов забезпечує потрібну ефективність функціонування рухомого об’єкту [3].

Сучасні дизельні двигуни потребують безперервного контролю за багатьма параметрами технологічного процесу при виготовленні та, особливо, при експлуатації [4, 5]. Враховуючи особливості роботи дизельних двигунів, основними характеристиками, які характеризують технічний стан двигунів, є параметри механічного руху. До таких параметрів необхідно віднести параметри періодичних переміщень двигуна під час функціонування – переміщення двигуна в просторі, тобто вібрації [3, 6]. Основними параметрами вібрації є амплітуда та частота [1, 2]. Підвищення достовірності вимірювання вібрацій при роботі дизельних двигунів є одним з основним напрямків забезпечення їх надійності за рахунок своєчасного виявлення відмов [1]. Тому пропонується розробити імітаційну модель діагностування технічного стану двигунів бронетанкової техніки. Дослідження розробленої імітаційної моделі дозволить своєчасно виявляти можливі відмови двигунів бронетанкової техніки при експлуатації.

Важливою характеристикою якості вимірювань параметрів, які характеризують технічний стан технічного об’єкта є достовірність. Достовірність вимірювання характеризує ступінь довіри до результатів вимірювань і ділить їх на дві категорії: достовірні та недостовірні, залежно від того, відомі або невідомі імовірнісні характеристики їх відхилень від дійсних значень відповідних величин [4, 5]. Достовірність характеризує імовірність того, що дійсне значення вимірюваної величини знаходиться у границях дійсного розподілу. Результати вимірювань, достовірність яких невідома, не представляють цінності й у ряді випадків можуть служити джерелом дезінформації. Це дозволяє для кожного конкретного випадку

вибирати методи і засоби вимірювань, що забезпечують отримання результату із заданою точністю.

При впровадженні систем діагностування, автоматичних пристроїв і автоматизованих систем управління до сучасних моторних систем бронетанкової техніки достовірність контролю параметрів функціонування дизельних двигунів має важливе значення. Для оцінювання достовірності вимірювань можливо використовувати декілька різних методів або джерел отримання вимірювальної інформації. Всі ці методи та способи вимірювання інформації реалізуються в інформаційно-вимірювальній системі інформативних параметрів динамічних режимів роботи дизельних двигунів.

Математичні перетворення застосовуються для того, щоб одержати про нього додаткову інформацію, недоступну у вихідному виді. Надалі сигнал у часовій області буде називатися «вихідним», а перетворений сигнал – трансформованим. Серед багатьох відомих перетворень сигналів найбільш популярним є перетворення Фур'є.

Більшість сигналів, що зустрічаються на практиці, представлені в часовій області, тобто сигнал є функція часу. У такий спосіб ми одержуємо амплітудно-часове подання сигналу. Для більшості додатків обробки сигналу це подання не є найкращим. У багатьох випадках найбільш значима інформація схована в частотній області сигналу. Частотний спектр є сукупність частотних (спектральних) компонент, він відображає наявність тих або інших частот у сигналі. У результаті перетворення Фур'є вібрації, заданого в часовій області, ми одержуємо його спектр. Замість значень часу на осі абсцис графіка вібрації будуть тепер відкладені значення частоти, а вісь ординат буде відображати амплітуду тієї або іншої частоти в вібрації. Найчастіше інформація, не помітна в часовому поданні вібрації, а проявляється в його частотному поданні.

При дослідженні вібрацій в дизельних двигунах необхідно проводити вимірювання чотирьох параметрів (двигун, генератор і в двох місцях на рамі). Суттєвим є те, що всі вимірювання цих вібрацій проводяться або в статистичному режимі, або в динамічному режимі з використанням спеціалізованих стендів. Але в умовах реальної експлуатації двигунів динамічні режими роботи, навантаження будуть відмінними від стендових. Таким чином, значення вібрації не будуть достовірними в повній мірі й за ними не можна прийняти рішення про відповідність параметрів вузлів та систем встановленим вимогам. Отже, необхідно проводити всі вимірювання вібрацій в динамічному режимі в реальних умовах експлуатації. Для цього повинна бути використана інформаційно-вимірювальна система вимірювання вібрацій динамічних режимів роботи дизельних двигунів.

Розроблена імітаційна модель, яка дозволяє проводити дослідження вібрацій в дизельних двигунах бронетанкової техніки за результатами вимірювання чотирьох параметрів. Результати використання імітаційної моделі дозволили визначити раціональні параметри технічного обслуговування двигунів зразка бронетанкової техніки іноземного виробництва.

Список використаних джерел

1. С.В. Герасимов, Л.В. Гаценко. **Моделювання генерації сигналів спеціальної форми для контролю технічного стану радіоелектронного обладнання**, *Комплексне забезпечення якості технологічних процесів та систем* (КЗЯТПС – 2022): матеріали тез доповідей XI Міжнародної науково-практичної конференції, Чернігів: НУ «Чернігівська політехніка», 2022, Т. 2, С. 176.
2. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.
3. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International*

Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.
4. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference «Application of information technologies in the preparation and operation of law enforcement forces»*, March 15, 2022, p.p. 31-32.
5. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference «Scientific Trends and Trends in The Context of Globalization»*, UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.
6. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

УДК 621.396

Валько В.В., Бабарика А.О.

МОЖЛИВОСТІ ТАНДЕМНОГО ЗАСТОСУВАННЯ БПЛА ТА БАРАЖУЮЧОГО БОЄПРИПАСУ ДЛЯ ЗБІЛЬШЕННЯ ДАЛЬНОСТІ УРАЖЕННЯ ЦІЛЕЙ

Безпілотні літальні апарати (БПЛА), або дрони, вже зарекомендували себе як незамінний інструмент для розвідки, спостереження, нанесення ударів та інших операцій. Однак, подальший розвиток військових технологій привів до інтеграції з БПЛА ще одного високоточного засобу ураження – баражуючих снарядів. Баражуючі снаряди мають можливість тривалий час залишатися в повітрі в певному районі, «очікуючи» на ціль, що робить їх особливо ефективними в динамічних умовах сучасних бойових дій. Основна відмінність БС від інших високоточних боєприпасів полягає в їх здатності до тривалого автономного польоту. Завдяки цьому БС можуть виконувати завдання за принципом «вистрілив і забув» – після запуску оператор не контролює кожен етап операції, або ж особисто здійснює керування польотом де це необхідно [1].

Баражуючі снаряди стають дедалі важливішою частиною військового арсеналу різних країн, оскільки вони поєднують здатність до самостійного виявлення цілей з високою маневреністю та ефективністю. Такі снаряди особливо корисні в сценаріях, де ворог використовує приховані або захищені позиції. На відміну від традиційної артилерії чи авіаційних бомбардувань, баражуючі снаряди здатні завдавати ударів з мінімальним ризиком побічних ушкоджень, що робить їх ідеальними для операцій у населених районах або в умовах, де важливо зберегти інфраструктуру [2]. Тому актуальним завданням роботи є дослідження конструктивних та технологічних рішень виготовлення БС, а також розробка методів інтеграції з безпілотними системами.

Розвиток баражуючих снарядів і їх інтеграція в сучасні дронові системи є важливим кроком до досягнення значної переваги в веденні бойових дій. Майбутнє таких систем пов’язане з постійним удосконаленням їх технологій, що дозволяє покращити оперативну ефективність, точність та надійність у різноманітних бойових умовах. Розвиток новітніх матеріалів, вдосконалення систем донаведення в умовах РЕБ, а також підвищення дальності польоту відкривають нові перспективи для створення

більш досконалих і ефективних бойових систем, що відповідатимуть вимогам майбутніх військових операцій.

Список використаних джерел

1. Жуган О. С., Калиниченко Д. С. Застосування баражуючих боєприпасів для боротьби з повітряними цілями противника. Ракетно-космічна техніка і технологія. 2023. № 1 (153). С. 45–58.
2. Rachok R., Katerynchuk I., Prokopenko Y., Strelbitskyi M., Babaryka A., Basarab O. Separate Issues of the Rational Construction of a Wireless Sensor Radio Network. 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). Lviv. Ukraine, 2024. P. 121-124. doi: 10.1109/TCSET64720.2024.10755682.

УДК 355.6

Винту А.О., Мільшин С.І.

РОЙОВІ БЕЗПІЛОТНІ СИСТЕМИ – СТРАТЕГІЧНИЙ ПОТЕНЦІАЛ ДЛЯ ОБОРОНИ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

У контексті повномасштабної збройної агресії російської федерації проти України, проблема ефективного вогневого ураження противника набуває стратегічного значення. Одним із перспективних напрямів розвитку військових технологій є застосування ройових безпілотних повітряних суден (далі - БПС). Ця технологія, що базується на принципах колективного інтелекту та децентралізованого управління, відкриває нові можливості для нанесення високоточних та масованих ударів по об'єктах противника.

Розробка ройового інтелекту для безпілотних систем (БС) розпочалася у 2000-х роках, коли з'явилася можливість об'єднати велику кількість малогабаритних дронів у єдину мережу.

Ройовий інтелект БС – це концепція колективного інтелекту, що дозволяє групі автономних БПС координувати свої дії для виконання складних завдань. Він базується на принципах самоорганізації, децентралізації та колективного прийняття рішень. У рої БС кожен агент функціонує автономно, приймаючи рішення на основі локально зібраних даних та взаємодії з іншими агентами. Комунікація між БПС здійснюється через мережу зв'язку, що забезпечує координацію дій та прийняття колективних рішень. Для оптимізації поведінки рою застосовуються алгоритми ройового інтелекту, такі як алгоритм рою частинок або мурашиний алгоритм, що моделюють поведінку природних роїв. Кожне БПС оснащене сенсорними системами (камери, радари, лідари), що дозволяють збирати інформацію про навколишнє середовище. Ройовий інтелект забезпечує адаптацію БПС до змін у зовнішньому середовищі. Ройові БПС можуть працювати як під управлінням оператора, так і в автономному режимі. В автономному режимі БПС використовують алгоритми штучного інтелекту для прийняття рішень та координації дій.

Ройові безпілотні системи демонструють високу ефективність у виконанні складних завдань завдяки масштабованості, відмовостійкості та адаптивності, обумовленим децентралізованою архітектурою та алгоритмами ройового інтелекту, однак їх застосування обмежене необхідністю розробки складного програмного забезпечення для управління, забезпечення стійкого зв'язку та протидії засобам радіоелектронної боротьби, що можуть порушити функціонування системи.

Ця технологія знаходиться на стадії активного розвитку, і її потенціал ще не повністю розкритий. Разом з тим, приклади застосування ройових БС вже існують. Наприклад Міністерство оборони США провело випробування рою з 103 БПС Perdix, які продемонстрували здатність до скоординованих дій.

Впровадження ройових БС у військовий арсенал України стикається з низкою науково-технічних та оперативно-тактичних викликів. Дослідження цих викликів, аналіз потенційних переваг та недоліків технології, а також розробка стратегій її ефективного застосування є актуальними завданнями для забезпечення обороноздатності України.

Відповідно, напрямками подальших досліджень є: методи застосування ройових БС для потреб Сил безпеки й оборони України, методика відбору таких БС для комплектування підрозділів військових формувань України, програма дослідної експлуатації ройових БС з подальшим формуванням рекомендацій застосування цих систем.

Гетьман А.В., Плугова О.Б., Сайко В.Г., Комаров В.О.

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ В УМОВАХ БОЙОВИХ ДІЙ

В умовах стрімкої еволюції сучасних технологій та зростання загроз електронного характеру, радіоелектронна боротьба (РЕБ) стає важливим елементом військової стратегії та безпеки країни, а в умовах сучасного ведення війни радіоелектронна боротьба має вирішальне значення для обох сторін конфлікту.

Розроблення високотехнологічної зброї дало потужний поштовх до розвитку систем, які змогли б ефективно протидіяти новим загрозам. Тепер паралельно з традиційними засобами ураження все більшої актуальності набувають системи радіоелектронної боротьби (РЕБ). Комплекси радіоелектронної боротьби відіграють значну роль не тільки на полі бою, а й у мирний час. Їх використовують для забезпечення захисту критичних об’єктів (наприклад, атомних станцій та гідротехнічних споруд), різноманітних підприємств стратегічного значення або важливих міжнародних зустрічей. Також деякі комплекси РЕБ допомагають цивільній авіації та судноплавству, виступаючи як навігаційне спорядження. Переоцінити потенціал засобів РЕБ з урахуванням реалій сучасних війн майже неможливо, тому провідні світові держави активно їх розвивають.

Радіоелектронна боротьба – це процес захисту від радіоелектронних засобів противника, які можуть використовуватись для перешкоджання комунікацій, контролю та розвідки. Іншими словами – РЕБ, це є системи та комплекси, які виконують різноманітні завдання залежно від свого призначення. Застосування РЕБ можна розділити на три основних напрями:

- радіоелектронне придушення;
- радіоелектронний захист;
- радіоелектронна розвідка.

Основними завданнями РЕБ є: дезорганізація управління військами противника; зниження ефективності ведення розвідки і застосування зброї і бойової техніки противника; забезпечення надійної роботи систем і засобів управління своїми військами і зброєю. Ключове завдання систем радіоелектронного придушення (РЕП) – вивід із ладу систем розвідки, РЛС ворога, а також будь-яких систем озброєння, які використовують оптично-електронні або радіоелектронні засоби наведення на ціль.

Одним із важливих аспектів радіоелектронної боротьби є комплексний технічний контроль та маскування, що передбачає використання екранів, що захищають від

радіосигналів, та інших заходів для забезпечення безпеки електронних систем. Також важливою є протидія за допомогою спеціальних систем розвідки та контррозвідки для виявлення ворожих елементів електронної боротьби та їх локалізації.

Для порушення функціонування ворожих систем використовуються в основному два методи:

– перший - встановлення радіозавад (активних й пасивних),
– другий - генерування фальш-цілей (імітаційні радіолокаційні завади).

Для створення активних завад використовують станції прийому-передачі радіосигналів або спеціальні передавачі завад, а для створення пасивних завад використовують відбивачі радіохвиль. Перші два види завад націлені на маскування або дезінформацію сигналів. Імітаційні завади застосовують для створення хибної інформації. За структурою такі завади подібні до сигналів, що використовуються в радіолокаторі, і тому створюють на його індикаторі відмітки хибних цілей, подібні до реальних. Цей ефект призводить до перевантаження обчислювача великою кількістю хибних сигналів, до втрати частини (або всіх) корисних сигналів, до збільшення імовірності хибної тривоги, що, в підсумку, призводить до ухвалення помилкових рішень. Якщо йдеться про радіолокатори керування зброєю, то застосування противником імітуючих завад може призводити до зриву автоматичного супроводження цілі по одній або декільком координатах (напрямку, дальності, швидкості) та до перенацілювання слідкуючих систем на хибні цілі. Частота повторення імітаційних завад може не співпадати або співпадати з частотою повторення зондувальних імпульсів радіолокатора, який намагаються придушити

Активні завади можуть бути настільки інтенсивними, що вони повністю заблокують радіолокаційний приймач. Тоді на виході приймача вже не буде імпульсних сигналів, а замість цього буде мати місце певна постійна напруга. В таких випадках зашумлена область на екрані індикатору радіолокатора не стає яскравішою, а навпаки, згасає.

У випадку активних завад до внутрішніх шумів приймача радіолокатора додається шум у вигляді завади. Таким чином, відношення «сигнал-шум» погіршується. Це, в свою чергу, призводить до зниження імовірності виявлення та до збільшення імовірності хибної тривоги. У випадку застосування потужних активних завад може відбуватися повне маскування цілі, тобто має місце ситуація, коли ціль радіолокатором не виявляється. Також в практиці радіоелектронної боротьби застосовують шумові завади різних видів. Найбільш розповсюдженими є загороджувальні завади (по часу, по частоті, по куту) та прицільні завади. Загороджувальні шумові завади мають достатньо велику ширину спектру та застосовуються у випадках, коли параметри радіолокатора, який потрібно заблокувати, не відомі. Прицільні завади, навпаки, мають спектр, узгоджений із спектром сигналів радіолокатора, який придушується.

До пасивних маскувальних завад відносяться завади, спричинені відбиттями зондувальних сигналів радіолокатора від хмар дипольних відбивачів.

Обидва типи зазначених маскувальних завад виконуються постійним потоком хаотично-шумових сигналів, внаслідок цього радіолокаційний ефір забивається, що не дає змогу відразу виявити потрібний сигнал. Ці дезінформуючі сигнали являться тотожними до оригінального сигналу, але містять хибні дані.

Також до способів протидії РЕБ можна віднести використання систем захисту від кібератак та інших видів кібернетичних загроз, що можуть бути використані для атак на електронні системи.

Для протидії негативному впливу зазначених маскувальних завад проводять заходи радіоелектронного захисту. Так, наприклад, для придушення (блокування) пасивних маскувальних завад використовують відмінності їхніх спектральних характеристик від спектральних характеристик сигналів відбитих від реальних цілей. Останні, як правило, рухаються у просторі набагато швидше, а значить мають більші значення допплерівського зсуву несівної частоти.

Маскувальні активні завади зазвичай мають вигляд радіочастотних коливань, які подібні до власних шумів радіолокаційного приймача. Також, за шириною частотного спектра завади ділять на прицільні та загороджувальні. Ширина спектра прицільних завад є тотожною з пропускною здатність радіоприймача. Такі завади є налаштованими на фіксовану частоту та мають вузький спектр дії. Для їх створення потрібні точні параметри локатора, котрий потрібно дестабілізувати. Такий тип завад дозволяє створити перевищення рівня завади над відбитим радіолокаційним сигналом для станцій з невеликим радіусом дії. Загороджувальні же завади перекривають частину радіочастотного діапазона. Активні завади можуть одночасно буди маскувальними та дезінформуючими, при умові що радіолокаційний сигнали буде зондуючого типу, які модульовані по амплітуді та інших характеристик сигналу. В залежності від типу сигналу, що придушується, та класу радіоелектронного засобу, обираються різні інформаційні критерії. Оцінку маскувальним завадам прийнято давати за допомогою ентропії завадового сигналу. Маскувальні завади зобов’язані перешкоджати можливій передачі корисного сигналу, з ймовірністю появи деякими обмежуючими умовами. Одною з таких умов є передбачення корисного сигналу. Рівень відомих даних може коливатися, але апріорна відомість про корисні сигнали, за правилами розподілу сигналів, які підвладні даному класу, повинні бути відомими. В інакшому випадку працездатність системи може бути під питанням. Замасковані завади створюють певні умови, які після отримання корисного сигналу під дією такої завади, залишає в системі інформаційного забезпечення, невпевненість в достовірності даних. Така невизначеність забезпечує маскувальні сигнали від потенційного усунення. Під час створення маскувальних завад засобами радіозв'язку, після прийому сигналу та його аналізу, невизначеність не зазнає змін. Під час першого наближення ентропія рівна апостеріорній невизначеності, яка в свою чергу рівна ентропії впливу шумового завадового сигналу. Щоб зменшити кількість отриманих даних, потрібно збільшити ентропію сигнала. У розробників завадових пристроїв завжди є необхідна інформація щодо критеріїв, які допоможуть створити кращій варіант ЗС. Для оцінювання якості завадового сигналу без прив'язки до подавляючих пристроїв і принципів прийняття рішення противником в умовах завад, використовують інформаційні критерії. Для їх використання при оцінці якості імітаційних сигналу потрібно знати апостеріорні статистичні характеристики хибних цілей.

Найважливішою енергетичною характеристикою завадового сигналу є мінімальне відношення енергії сигналу до енергії корисного сигналу на вході приймального радіоелектронного пристрою, який блокується в смузі його лінійної частини, при якому з’являється інформаційний збиток. Інформаційний збиток утворюється внаслідок впливу завад, він проявляється в затримці передачі даних, імітації та маскуванні. Характер збитків, який буде нанесений інформації залежить від видів завадового сигналу та пристроїв радіочастотного придушення. Коефіцієнт придушення (КП) визначається за формулою (1). КП зазвичай виражають через співвідношення потужностей завадового і корисного сигнала на вході пристроя:

$$КП = Рз/Рс$$

де Рз — потужність завадового сигналу;

Рс — імпульсна потужність корисного сигналу.

Числові значення КП можуть бути знайденими тільки для заданого завадового сигналу і типу придушуючих пристроїв. Внаслідок цього енергетичний критерій на відміну від інформаційного потребує точних параметрів придушуючих систем.

Висновки. У ході аналізу сучасних методів радіоелектронної боротьби виявлено, що ця галузь стає все важливішою у контексті сучасних військових конфліктів та загроз кібербезпеки. Загальною метою радіоелектронної боротьби є забезпечення функціонування електронних систем та інших пристроїв в умовах впливу радіосигналів, що може бути використано для розвідки, перешкоджання та навіть

знищення. Для досягнення цієї мети використовуються сучасні різноманітні методи та засоби, такі як комплексний технічний контроль та маскування, захист від кібератак, системи захисту від електромагнітного імпульсу та використання резервних систем зв'язку та комунікації.

УДК 623.6

Глущенко М.О.

ОХОРОННІ КОМПЛЕКСИ НА ОСНОВІ РАДІОЛОКАЦІЙНИХ ЗАСОБІВ ВИЯВЛЕННЯ

В даний час для цілодобової, всепогодної охорони периметрів, територій і акваторій, де немає можливості обладнати захисну огорожу, з'явилися новітні радіолокаційні засоби виявлення (РЗВ), що дозволяють контролювати територію в реальному часі на фоні схеми місцевості, перекривати небезпечні напрямки на прилеглій території, відстежувати всі переміщення всередині об'єкта, ідентифікувати порушника (людину, групу людей, транспортний засіб), визначати їх кількість, характер поведінки, а в деяких випадках наявність зброї.

Крім того, РЗВ можуть використовуватись і для виявлення малорозмірних літальних апаратів у приземному просторі, визначення координат цілей (азимуту та дальності), ЕПР, радіальної швидкості та ширини допплерівського спектру.

За цілевказівками від РЗВ можуть наводитися на цілі світлотехнічні засоби та оптичні засоби спостереження. Це може значною мірою вже на ранніх етапах полегшити виконання завдань щодо попередження проникнення порушника на територію, що охороняється і дозволить оператору ефективно координувати дії групи реагування.

Особливістю застосування охоронних РЗВ є рівень електромагнітного випромінювання який має бути гранично низьким, щоб відповідати санітарним правилам і нормам. При цьому показники якості виявлення (зокрема дальність дії) повинні досягатися не збільшенням потужності передавача, а підвищенням ефективності передачі інформації, наприклад, шляхом використання методів розширення спектру, удосконаленням методів та алгоритмів обробки даних.

Найважливішими розробками для відродження та розвитку української радіолокації стало створення малогабаритних допплерівських РЗВ для розвідки наземних, надводних та повітряних цілей ближньої зони.

Основними тенденціями розвитку малогабаритних РЗВ є перехід до технології активних фазованих антенних решіток та побудови на їх основі РЗВ широкого функціонального призначення.

Для малогабаритних РЗВ основними діапазонами хвиль залишаються X- та S-діапазони. Розширюється коло виробників, які використають технологію циліндричних антенних решіток переважно в L-діапазоні хвиль.

РЗВ українського виробництва за тактико-технічними характеристиками та за технологіями, які використовуються під час побудови, не поступаються закордонним аналогам.

З постійним розвитком технологій та можливостей РЗВ охоронні комплекси удосконалюються, стаючи більш точними, ефективними та здатними протистояти різним загрозам безпеці, включаючи повітряний, наземний та морський простір.

УДК 623.644, 623.647

Горєлишев С.А., Залевський Г.С.

ІТЕРАЦІЙНИЙ МЕТОД РОЗРАХУНКУ ХАРАКТЕРИСТИК РОЗСІЮВАННЯ ДЕЯКИХ КОМБИНОВАНИХ ОБ'ЄКТІВ РЕЗОНАНСНИХ РОЗМІРІВ

Підходи до математичного моделювання характеристик вторинного випромінювання радіолокаційних об'єктів визначаються складністю їх конструкції, характеристиками матеріалів, з яких виготовлені елементи конструкції об'єктів та їх електричними розмірами [1]. Найбільш трудовитратними з точки зору розрахунків є комбіновані об'єкті резонансного розміру.

Комбінований об'єкт звичайно є об'єктом складної форми, що має як металеві, так і діелектричні елементи конструкції. Електромагнітне поле (ЕМП), яке розсіяне комбінованим об'єктом, у метровому і дециметровому діапазонах довжин хвиль може бути розрахованим як когерентна сума полів, розсіяних його елементами. Сума розсіяних ЕМП окремих металевих і діелектричних компонентів комбінованого об'єкту з урахуванням їх фази дозволяє отримати загальне ЕМП комбінованого об'єкту без урахування їх електромагнітної (ЕМ) взаємодії.

Для більш детального врахування ЕМ взаємодії металевих і діелектричних елементів конструкції необхідно застосовувати ітераційні методи, зокрема описаний у роботах [2-4]. Застосування ітераційних методів та систем інтегральних рівнянь (ІР), що описують щільності струмів на поверхнях реальних комбінованих об'єктів, пов'язані із значними часовими витратами і потрібними комп'ютерними ресурсами.

В якості нульового наближення передбачається розрахунок ЕМП як сума розсіяних окремо металевими та діелектричними компонентами комбінованого об'єкту. Тобто розсіяння плоскої хвилі $\left(\overset{\rho}{E}^0, \overset{\rho}{H}^0\right)$ з точки опромінення розглядаємо тільки на металевої компоненти V_2 з поверхню S_2 при відсутності діелектричної компоненти V_3 з поверхню S_3. Знаходженню підлягають еквівалентні електричні $\overset{\rho}{J}^e_{s2}\left(\overset{\rho}{Q}_{s2}\right)$ струми у точках на поверхні металевої компоненти комбінованого об'єкту, поверхня якого містить елементи з малими радіусами кривизн (краю), за допомогою модифікованого інтегрального рівняння магнітного поля (ІРМП) у просторово-частотному поданні.

Одночасно розраховується ЕМП, яке розсіяне діелектричної компонентою V_3 з поверхню S_3 при відсутності металевої компоненти V_2 з поверхню S_2 комбінованого об'єкту. Еквівалентні електричні $\overset{\rho}{J}^e_{s3}\left(\overset{\rho}{Q}_{s3}\right)$ та магнітні $\overset{\rho}{J}^m_{s3}\left(\overset{\rho}{Q}_{s3}\right)$ струми у точках на поверхні діелектричної компоненти комбінованого об'єкту розраховуються за допомогою система інтегральних рівнянь Мюллера (СІРМ) [5,6]. Як показано у [6], СІРМ для щільності електричного струму на поверхні диелектричного розсіювача має єдине рішення на всіх частотах.

Напруженості ЕМП, розсіяного всім комбінованим об'єктом без урахування взаємодії аналізованих металевих і діелектричних компонентів, є когерентна сума полів, розсіяних його елементами.

$$\overset{\rho}{H}^0_{рез}\left(\overset{\rho}{Q}_{пр}\right) = \overset{\rho}{H}^0_2\left(\overset{\rho}{Q}_{пр}\right) + \overset{\rho}{H}^0_3\left(\overset{\rho}{Q}_{пр}\right), \quad (1)$$

$$\overset{\rho}{E}^0_{рез}\left(\overset{\rho}{Q}_{пр}\right) = \overset{\rho}{E}^0_2\left(\overset{\rho}{Q}_{пр}\right) + \overset{\rho}{E}^0_3\left(\overset{\rho}{Q}_{пр}\right). \quad (2)$$

Врахування взаємодії компонентів комбінованого об'єкта проведемо шляхом ітераційного процесу, який полягає у послідовному опроміненні компонентів один одного та знаходженні щільності поверхневого струму на поверхнях S_2 та S_3 відповідно. На етапі ітераційного процесу ξ шляхом застосування поверхневих струмів

на діелектричної компоненти комбінаційного об’єкта $\overset{\rho}{J}{}^{e(\xi-1)}_{s3}\left(\overset{\rho}{Q}_{s3}\right)$ і $\overset{\rho}{J}{}^{m(\xi-1)}_{s3}\left(\overset{\rho}{Q}_{s3}\right)$, які розраховані на попередньому етапу $\xi-1$, отримуємо напруженість магнітного поля $\overset{\rho}{H}{}^{(\xi)}_{3}\left(\overset{\rho}{Q}_{s2}\right)$ у кожної точці поверхні S_2 металевої компоненти V_2.

Аналогічно у кожної точці поверхні S_3 діелектричної компоненти V_3 комбінованого об’єкту розраховуємо за допомогою $\overset{\rho}{J}{}^{e(\xi-1)}_{s2}\left(\overset{\rho}{Q}_{s2}\right)$ напруженість магнітного $\overset{\rho}{H}{}^{(\xi-1)}_{2}\left(\overset{\rho}{Q}_{s3}\right)$ та електричного $\overset{\rho}{E}{}^{(\xi-1)}_{2}\left(\overset{\rho}{Q}_{s3}\right)$ поля. Далі, при знаходженні щільності струму на металевої компоненти комбінаційного об’єкта $\overset{\rho}{J}{}^{e(\xi)}_{s2}\left(\overset{\rho}{Q}_{s2}\right)$ при ξ-й ітерації в якості напруженості магнітного поля опромінення використовується сума напруженості магнітного поля, що опромінює металеву компоненту комбінованого об’єкту $\overset{\rho}{H}{}^{0}\left(\overset{\rho}{Q}_{s2}\right)$ і напруженості магнітного поля, розсіяного діелектричної компонентою $\overset{\rho}{H}{}^{(\xi-1)}_{3}\left(\overset{\rho}{Q}_{s2}\right)$ на $(\xi-1)$-ой ітерації в точках $\overset{\rho}{Q}_{s2}$.

Паралельно, шляхом рішення СІРМ при ξ-й ітерації знаходиться щільність електричного $\overset{\rho}{J}{}^{e(\xi)}_{s3}\left(\overset{\rho}{Q}_{s3}\right)$ та магнітного $\overset{\rho}{J}{}^{m(\xi)}_{s3}\left(\overset{\rho}{Q}_{s3}\right)$ струму на поверхні S_3. При цьому у якості напруженості первинного ЕМП використовується сума відповідних складових ЕМП опромінення діелектричної компоненти комбінованого об’єкта $\left(\overset{\rho}{E}{}^{0}\left(\overset{\rho}{Q}_{s3}\right),\overset{\rho}{H}{}^{0}\left(\overset{\rho}{Q}_{s3}\right)\right)$ і ЕМП, розсіяного металевої компонентою об’єкта $\left(\overset{\rho}{E}{}^{(\xi-1)}_{2}\left(\overset{\rho}{Q}_{s3}\right),\overset{\rho}{H}{}^{(\xi-1)}_{2}\left(\overset{\rho}{Q}_{s3}\right)\right)$, знайденим в точках $\overset{\rho}{Q}_{s3}$. Тим самим враховується електромагнітна взаємодія різних елементів конструкції. Далі на кожної ітерації можна знайти сумарне розсіяне поле всього комбінованого об’єкту відповідно до формули (1,2).

Описану процедуру необхідно повторювати декілька разів. Кількість ітерацій залежить від складності комбінованого об'єкта. Як критерій визначення кількості ітерацій може виступати збіжність поверхневих струмів на металевій V_2 та діелектричній V_3 компонентах для подальших ітерацій із заданою точністю δ.

Даний ітераційний метод можливо використати для розрахунку наприклад вторинного випромінювання наприклад, для тактичних безпілотних летальних апаратів (БПЛА), які у своєму складі мають елементи з металевою поверхнею, діелектричні елементи та радіопрозори елементи, тобто їх необхідно розглядати як комбіновані об’єкти.

Розміри БПЛА і розмах крил можуть мати довжину порядку 2 м, що для метрового і дециметрового діапазону буде відповідати резонансним розмірам. Так, аналізуючи конструкцію таких БПЛА бачимо що фюзеляж, крила і стабілізатори, як правило, виготовляються з діелектричного матеріалу і мають тонкі стінки (до 5 мм). Тому слід очікувати, що у метровому і дециметровому діапазонах фюзеляж БПЛА буде радіопрозорим. Про це додатково свідчить той факт, що під ним, як правило, розташовуються антени системи управління, зв’язку та передачі даних. Такі елементи конструкції як рухова установка (двигун із глушником), блоки управління і корисного навантаження є елементами з металевою поверхнею, а паливний бак, що має тонкі стінки, наповнений бензином та гвинт можна вважати однорідним діелектричним об’єктом. Розміри перерахованих елементів складають одиниці-десятки сантиметрів.

Але для використання запропонованого ітераційного метода важливу роль буде грати розташування металевих та діелектричних компонентів відносно один до одного та відстань між ними.

Таким чином запропоновано методи моделювання характеристик радіолокаційного розсіювання БПЛА, що містить металеві і діелектричні елементи конструкції. Даний

підхід дозволяє достатньо точно розраховувати характеристики радіолокаційного розсіювання деяких комбінованих БПЛА у метровому і дециметровому діапазонах хвиль при прийнятній тривалості проведення розрахунків.

Список використаних джерел

1. Вторинне випромінювання безпілотних літальних апаратів (математичне моделювання): монографія / О.І. Сухаревський, І.В. Калужинов, В.О. Василець та ін. // Під ред. О.І. Сухаревського. – Х.: ХАІ, 2022. – 270 с
2. Комбинированный метод расчета характеристик рассеяния объектов сложной формы и его применение для моделирования спектров винтовой модуляции вертолетов / Г.С. Залевский, М.М. Бречка, В.А. Василец, О.И. Сухаревский // Системи обробки інформації. – 2014. – Вип. 4(120). – С. 80– 85.
3. Sukharevsky O.I. Iterative Algorithm for Simulation of EM Scattering by Objects, Contained Constructive Elements of Different Electric Sizes / O.I. Sukharevsky, G.S. Zalevsky, V.A. Vasilets // 2017 XXIInd International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED), Sept. 25 – 28, 2017: Proc. – Dnipro, Ukraine. 2017. – P. 190-193.
4. Combined Calculation Method for the Scattering Characteristics of Complex Shaped Objects and Its Application to Model Helicopter Rotor Modulation Spectra / G. Zalevsky, M. Brechka, V. Vasilets, et al. // 2020 IEEE Ukrainian Microwave Week (UkrMW-2020) : 21-25 Sept., 2020 : Proc. Vol. 2, 2020 IEEE 6th International Symposium on Microwaves, Radar and Remote Sensing (MRRS). – Kharkiv, 2020. – P. 473-477.
5. Васильев Е.Н. Возбуждение тел вращения / Е.Н. Васильев. – М. : Радио и связь, 1987. – 272 с.
6. Harrington R.F. Boundary Integral Formulations for Homogeneous Material Bodies / R.F. Harrington // Journal of Electromagnetic Waves and Applications. – 1989. – Vol. 3, No. 1. – P. 1–15.

УДК 654.1

Давіденко С.В., Заєць Я.Г., Рижов Є.В., Опалинський В.Б.

ЩОДО ІНТЕГРУВАННЯ ТРЕКЕРА В СИСТЕМУ КЕРУВАННЯ ПОЛЬОТОМ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

Хід російсько-української війни продемонстрував зростаючу роль безпілотних систем для отримання переваги в бойовому протистоянні. В цих умовах добре себе зарекомендували автономні трекери модельного ряду SLA. Але для отримання більших обсягів корисної інформації та гнучкого керування трекінгом, з метою покращення безпеки, непомітності та вірогідності підтвердження ураження необхідно інтегрувати трекер з польотним контролером та GNSS. Нова серія трекерів модельного ряду Bug як раз і інтегрується безпосередньо в БпЛА. Такий трекер бере дані з GNSS борту, а коли борт збито і живлення зникло, вмикає власний приймач GNSS. Він активується після старту і міняє режим роботи при заході на ціль за командою з Mission Planer.

Використання вбудованого трекера дозволяє спростити активацію автономного трекера на борту під час виконання місії, бо коли трекер автономний, підрозділ перед місією повинен сам вирішувати питання, куди та як розмістити трекер, щоб його було зручно активувати при старті в обмежених часовим рамках. Також інтеграція трекера в штатне обладнання дозволяє вирішити питання радіонепрозорості корпусу, впливу випромінювання інших систем, вібрації, незручного доступу тощо, з якими в бойовій обстановці розбиратись немає часу. Крім того щільне подавлення засобами РЕБ та

спуфінг створюють великі зони, де автономний трекер самотужки не може визначити координати в повітрі.

Трекер не має «дорогої» захищеної військової системи типу СРПА або аналогів тому має значно гірший прийом ніж бортова система GNSS. На землі, в автономному режимі, це не є великою проблемою, але дані в польоті є дуже важливими. Інтеграція дозволяє трекеру використовувати зовнішню військову систему GNSS, і переходити на власну тільки при потребі. При інтеграції можна краще вирішувати проблему фіксації «останньої» милі перед ударом за рахунок збільшення частоти фіксації та передавання точок перед ударом. Дані про стан борту передаються автоматично. Є можливість отримання додаткової інформації з польотного контролера по запиту. На відміну від автономного, який має попередньо налаштований алгоритм, інтегрований трекер має гнучке керування трекінгом, може в залежності від місії та зони польоту міняти режими роботи від режиму «сну» або режиму «онлайн».

Інтегрований трекер Bug має ударозахищений вологостійкий корпус з власним живленням, яке дозволяє відстеження БпЛА по території України та так званої росії з автономністю від 7 днів. Він передає наступну інформацію: координати GNSS, стан трекера (заряд АКБ, режим, температура, тощо), стан БпЛА (швидкість, висоту по барометру, прискорення, кути нахилу, температуру, тощо), стан середовища (температура, РЕБ/СПУФ, тощо), час і дату, та іншу за потребою (наприклад залишок пального чи оберти двигуна). За рахунок затримки увімкнення передавання даних відсутня фіксація точок старту, що забезпечує «безпечний старт» для екіпажу. Можливе аварійне відкриття парашуту, кероване трекером, в разі втрати бортом власного живлення або фіксації початку падіння борту. Також є можливість активації плати самознищення борту за командою з трекера, по часу або по настанню події.

Отже використання інтегрованого трекера в системі керування польотом БпЛА дозволяє здійснювати фіксацію ударів DeepStrike, моніторинг польоту бортів DeepStrike, для виконання місій з ведення розвідки, бомбардування, передавання вантажів на ворожу територію а також для виявлення технічних проблем, зон дії РЕБ, зон ураження ППО, відстеження та розшуку навчальних бортів.

Даник Ю.Г.

УПРАВЛІННЯ РИЗИКАМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Технології штучного інтелекту стають ключовими для забезпечення розвитку економіки та ефективного вирішення питань національної безпеки і оборони.

Кількість, можливості і спрямованість застосування кодів ШІ постійно зростають. На цей час активного розвитку і використання набули: ChatGPT, Jasper, Copy.ai, Canva AI, Adobe Firefly, Midjourney, Hootsuite, Synthesia AI, HubSpot AI, Adobe Sensei, Copilot, Gemini, LLaMA, DeepSeek та багато інших. Можна прогнозувати позитивну нелінійну прогресію зростання кількості і можливостей різноманітних ШІ.

При цьому, слід враховувати, що крім переваг, розвиток і використання штучного інтелекту пов’язані зі значними загрозами та ризиками, які необхідно своєчасно виявляти та управляти ними для їх вчасної нейтралізації або зниження до безпечного рівня.

Аналіз теорії, практики і досвіду вирішення завдань управління ризиками розвитку та використання ШІ у провідних державах світу свідчить, що основною тенденцією і проблемою при його здійсненні є забезпечення вірного прогнозування загроз пов’язаних зі ШІ, ймовірності та наслідків їх реалізації.

При цьому, слід ретельно враховувати інтенсивні зміни, в умовах достатньо високого ступеню невизначеності, як у розвитку науки і технологій так і впливу

великої множини зовнішніх і внутрішніх факторів які є визначальними відносно вирішення питань безпеки пов'язаних зі ШІ. Саме це є необхідними та достатніми умовами розробки і реалізації ефективних та адекватних механізмів управління ризиками розвитку та використання ШІ в усіх сферах.

Як показали проведені дослідження розвиток напрямів застосування ШІ, під впливом сучасних воєнних та інших конфліктів, суттєвим чином модулюється в сторону надання йому та надбання ним ознак і функцій специфічної зброї, яка слабо контролюється людиною або, навіть, такої, контроль над якою може бути з легкістю втрачений, особливо коли йдеться про автономні кіберфізичні автономні системи, які будуть знаходити все більшого застосування в протиборстві будь-яких конфліктуючих сторін, як на рівні держав так і недержавних структур, терористичних організацій тощо.

Можна прогнозувати формування та розвиток багатоаспектної та багаторівневої системи конфліктів різної природи та їх причинно-наслідкового розвитку, як між штучними інтелектами, керованими людиною, згідно її волі та під її управлінням так і таких, які почнуть виникати між штучними інтелектами вже поза системи «людина-ШІ». Такі питання, на цей час, здебільшого відносять до, так званих етичних проблем ШІ, не враховуючи причини і природу їх виникнення.

Питання етики штучного інтелекту, згідно з вікіпедією, є частиною етики технологій, характерною для роботів та інших штучно створених інтелектуальних істот. Її поділяють на робоетику, яка вирішує питання моральної поведінки людей при проектуванні, конструюванні, використанні та корегуванні діяльності штучно розумних істот та машинну етику, яка торкається проблем моральної поведінки штучних моральних агентів. Упускаючи, при цьому, питання та інструменти регулювання та управління, створення та застосування дієвих механізмів безпеки.

Особливої важливості, при цьому, набуває пошук, впровадження та використання механізмів контролю та управління ризиками, які пов'язані з погано контрольованою та часто безвідповідальною поведінкою розробників і користувачів ШІ в протиборчих системах та сторонах сучасних конфліктів. Все частіше з'являється також інформація про різноманітні конфлікти в системах «людина-ШІ-людина», «ШІ-ШІ» та «ШІ-людина».

Подібні питання, які демонструють, що проблема протиборства у вигляді змагальності ШІ при вирішенні антагоністичних за змістом задач вже стала реальністю. Наприклад, змагання, коли одні системи ШІ використовуються для створення реалістичних, але неправдивих текстів, зображень, відео тощо, при цьому, для виявлення таких фейків паралельно розробляються інші системи ШІ, що веде до постійної гонки озброєнь між генеративними та детективними моделями. Такі конфлікти початково розглядались в рамках генеративних змагальних мереж (Generative adversarial networks, GANs), які були запропоновані в 2014 році Яном Ґудфелоу, як клас алгоритмів штучного інтелекту, що використовуються в некерованому навчанні. На той час цей конфлікт ШІ розглядався, як змагання двох штучних нейронних мереж, одна з одною в рамках гри з нульовою сумою. Проведені дослідження показали, що при моделюванні конфліктів в рамках алгоритмів Бойда це не є грою з нульовою сумою, але ці питання є предметом окремого розгляду.

Так, на цей час, де-факто формується окремий важливий напрям в сфері ШІ – конфліктологія ШІ, в рамках якого повинні досліджуватись питання виникнення протиріч, зіткнення інтересів та особливості взаємодії в системах: окремих осіб, різних цільових аудиторій, суспільства, держави, природи, ШІ і кібер-фізичних систем керованих ШІ та взаємодії людини, суспільства, ШІ, кібер-фізичних систем керованих ШІ і природи. А також різноманітних комбінацій багатокомпонентних систем, які можуть організовуватись різними акторами та самоорганізовуватись. При цьому типологія, учасники, часові рамки, спрямованість та інші параметри і наслідки

конфліктів в зазначених мінливих системах «людина-суспільство-держава-природа-техносфера-ШІ» динамічно і найчастіше, хаотично, змінюються.

Для оцінювання ризиків таких конфліктів можуть бути застосованими методи аналізу сценаріїв (Scenario Analysis) та FMEA (Failure Mode and Effects Analysis), який використовується для виявлення критичних точок, у яких алгоритми можуть дати збій, аналізу можливих збоїв, такі як некоректні прогнози через недостатню якість даних або помилки в автоматичному тестуванні коду, оцінки ймовірності, тяжкості і наслідків реалізації ризиків, а також розробки планів їх мінімізації, а також методика «Оцінка ризиків інформаційної безпеки» (ISO/IEC 27005). Адаптація ISO-стандартів дає змогу структуровано визначити загрози.

Одним з потужних інструментів управління ризиками використання штучного інтелекту є нормативно-правове регулювання.

Так, наприклад, автономні ударні роботизовані засоби керовані ШІ (Lethal Autonomous Weapons, LAW) є предметом міжнародного обговорення, зокрема в рамках ООН (Конвенція про певні види звичайної зброї, CCW). Але їх створення, розвиток і використання розглядається і в нормативно-правових актах багатьох країн.

Основні нормативні аспекти, щодо автономних ударних роботизованих засобів керованих ШІ:

– міжнародне гуманітарне право (МГП) забороняє використання зброї, яка не може розрізняти цивільних та комбатантів (Протокол I до Женевських конвенцій);

– кодекс НАТО щодо військового застосування ШІ (NATO AI Strategy), прийнятий у 2021 році, передбачає етичні принципи використання ШІ у військовій сфері, включаючи прозорість, підзвітність і необхідність людського контролю над летальними рішеннями. При цьому, відповідно до цього кодексу Країни НАТО, можуть розробляти LAWS, забезпечуючи належний контроль за їхнім використанням;

– в 2018 році Європарламент прийняв резолюцію, щодо заборони розробки і використання автономних бойових систем, що можуть приймати рішення про застосування смертоносної сили без людського контролю в ЄС. В 2023 прийнятий AI Act (очікується впровадження у 2025 році), який проголошує, що автономні бойові системи можуть потрапити під категорію «високого ризику», що вимагатиме суворих тестувань і сертифікації. Пропонований EU AI Act і нормативи GDPR задають жорсткі вимоги щодо класифікації ризиків, прозорості алгоритмів та етичного застосування високоризикових систем, включаючи автономні бойові засоби. Таким чином, у межах ЄС розробка та використання LAWS обмежується, але не забороняється остаточно;

– дозвіл на розробку LAW, з акцентом на необхідності «людського контролю» (Human in the Loop/On the Loop) в США.

Аналіз нормативно-правового забезпечення розвитку та використання ШІ є складним завданням, оскільки ця сфера швидко розвивається, а законодавство знаходиться в процесі формування. Однак, можна виділити основні тенденції та існуючі ключові документи, які прийняті та введені в дію, як на міжнародному рівні, так і в провідних державах світу.

Дуже важливим, з точки зору нормативно-правового регулювання в сфері ЩІ є аналіз досвіду США. У США наразі немає єдиного федерального закону, який би комплексно регулював розвиток та використання ШІ. Однак, існують окремі ініціативи та нормативні акти на рівні штатів та федеральних агентств, спрямовані на регулювання певних аспектів розвитку та використання ШІ. Національний інститут стандартів і технологій (NIST), розробляє AI Risk Management Framework, тобто стандарти ризик-менеджменту для компаній, що розробляють і використовують ШІ та настанови щодо етичного використання ШІ, включаючи забезпечення прозорості, справедливості та підзвітності. Деякі штати, такі як Каліфорнія, прийняли закони, що стосуються конфіденційності даних та використання технологій ШІ, зокрема в сферах розпізнавання обличь та автономних транспортних засобів. У 2020 році в США було

прийнято Закон про національну стратегію штучного інтелекту (National AI Initiative Act), який спрямований на координацію досліджень та розробок у сфері ШІ, але не встановлює конкретних обмежень щодо його використання.

Executive Order 13960 (2020) регламентує використання ШІ в сфері оборони, підкреслюючи важливість тестування та сертифікації військових ШІ-систем. Він передбачає регулювання державного використання ШІ, зобов'язання щодо прозорості та безпеки, підконтролюваності ШІ, його етичності і пояснювальності. Також передбачена: обов'язковість прозорості ШІ в державному секторі та відкритості алгоритмів, які використовуються урядом, пріоритет безпеки у впровадженні ШІ, використання відкритих стандартів при роботі з державними структурами США, документування впливу ШІ на процеси безпеки.

В 2022 році в США прийнятий AI Bill of Rights, спрямований на захист прав громадян при використанні ШІ у прийнятті рішень. Відповідно до нього використання ШІ для аналізу загроз має бути пояснюваним, щоб уникнути юридичних ризиків.

В 2023 році прийнятий Указ Президента 14110 «Про безпечний, надійний та відповідальний розвиток і використання штучного інтелекту» Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, який встановив нові стандарти безпеки для ШІ та передбачив розробку етичних норм і принципів підзвітності для систем ШІ. Але в США зосереджені більше на галузевому регулюванні ШІ, а не на створенні єдиного системного нормативно-правового забезпечення.

У ЄС формування нормативної бази з регулювання технологій ШІ відбувається одночасно, як на загальноєвропейському рівні урядування, так і в державах-членах. Пріоритетом європейського підходу є встановлення етичних стандартів впровадження ШІ. Повноваження з напрацювання політики у цій сфері розвитку наразі здійснює Європейська Комісія. За її ініціативи створено Європейський Альянс зі штучного інтелекту, який охоплює понад шість тисяч стейкхолдерів і слугує платформою для публічних дискусій. У найближчій перспективі планується створення самостійного органу – Європейської ради з питань ШІ (European Artificial Intelligence Board). Зокрема, цьому питанню присвячений VI Розділ Пропозиції щодо Регламенту Європейського Парламенту та Ради про встановлення гармонізованих правил щодо ШІ (Акт про штучний інтелект). 1 серпня 2024 року в ЄС набув чинності Акт про штучний інтелект, який є першим подібним регуляторним документом у світі. Метою цього акту є гарантування безпеки та дотримання основних прав громадян у процесі розвитку технологій ШІ.

В ньому представлена прийнята класифікація систем ШІ за рівнем ризику.

Неприйнятний ризик - системи ШІ, які становлять загрозу для фундаментальних прав, такі як системи соціального рейтингування та ті, що можуть маніпулювати поведінкою людей. Такі системи заборонені.

Високий ризик - системи, що використовуються в критичній інфраструктурі, освіті, управлінні персоналом, державних послугах та біометричній ідентифікації. Такі системи підлягають суворим вимогам щодо безпеки та нагляду.

Обмежений ризик - системи, як-от чат-боти та генератори дипфейків, які вимагають забезпечення прозорості та інформування користувачів про взаємодію з ШІ.

Мінімальний ризик - системи ШІ, інтегровані в інші програмні продукти, наприклад, спам-фільтри або ШІ в комп'ютерних іграх. Такі системи не підлягають спеціальному регулюванню в рамках Акта.

Серед вимог до систем з високим ризиком:

– створення системи управління ризиками, яка функціонуватиме протягом усього життєвого циклу системи;

– забезпечення якості та безпеки даних, що використовуються для навчання, перевірки та тестування моделей ШІ;

– надання технічної документації для демонстрації відповідності системи вимогам законодавства та забезпечення можливості оцінювання такої відповідності органами влади.

Із заборон можна виділити:

– використання систем ШІ, які можуть маніпулювати поведінкою людей або використовуватися для соціального рейтингування.

– використання біометричних систем для розпізнавання емоцій на робочому місці або для біометричної ідентифікації у реальному часі службами правопорядку.

На основі проведеного аналізу, для мінімізації ризиків використання ШІ, пропонується зробити обов'язковими в законодавстві всіх держав, яке розглядає врегулювання питань розвитку і застосування ШІ, такі основні принципи:

– обов'язковий людський контроль ШІ. Всі рішення, пов'язані з застосуванням сили, мають підлягати підтвердженню або контролю відповідальними особами. Це мінімізує ризик помилок або неконтрольованих дій системи.

– оцінка ризиків і сертифікація всіх без виключення систем ШІ. Перед впровадженням систем необхідно проводити всебічну оцінку ризиків, включаючи аналіз сценаріїв можливих збоїв, впливу на безпеку персоналу та цивільного населення. Отримання сертифікації відповідності встановленим стандартам безпеки є обов'язковим.

– прозорість алгоритмів та відповідальність. Всі етапи розробки і тестування систем мають бути документально зафіксовані, забезпечуючи можливість зовнішнього контролю з боку уповноважених органів і міжнародної спільноти. Визначення відповідальності за прийняті рішення є ключовим для запобігання зловживань.

– відповідність міжнародному гуманітарному праву. Використання автономних бойових систем має відповідати нормам міжнародного гуманітарного права, зокрема принципам пропорційності та розмежування між комбатантами і цивільним населенням.

УДК 004.738

Данило Н.Р., Данильчук Р.О., Площик А.С.

АНАЛІЗ МЕТОДИК РОЗПІЗНАВАННЯ ОБ'ЄКТІВ З ВІДЕОПОТОКУ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Швидкий розвиток технологій комп'ютерного зору та штучного інтелекту суттєво розширив можливості розпізнавання об'єктів у відеопотоці. Нейронні мережі представляють певні покращені результати при вирішенні завдань виявлення, класифікації та відстеження об'єктів на відео, тим самим, роблять себе потрібними для забезпечення службово-бойової діяльності силових структур.

Продовж останніх років, сучасні системи зазнали змін, особливо, це стосується систем розпізнавання об'єктів на основі відеопотоків. Для прикладу, архітектура YOLOv4 (You Only Look Once version 4) здатна обробляти до 65 кадрів за секунду з точністю mAP 43,5% [2]. Що дає можливість робити аналіз відеопотоків майже в реальному часі, не зважаючи на вартість графічних процесорів. Також, важливо відзначити, що найсучасніші моделі YOLOv8 і DINO-RT можуть ідентифікувати об'єкти розміром від 10 до 15 пікселів на зображенні, відкриваючи можливість аналізу відео з надвисокою роздільною здатністю [1]. Застосовуючи апаратні прискорювачі, такі як Google TPU або NVIDIA Jetson, продуктивність можна збільшити в 3-5 разів, тим самим, зменшити енергоспоживання всього до 30 Вт, що робить можливим розгортання цих систем на безпілотних платформах з обмеженим енергоспоживанням .

Аналіз сучасних методів розпізнавання об’єктів показує, що вони базуються на кількох ключових підходах. Двоступеневі детектори, такі як Faster R-CNN, спочатку шукають регіони інтересу, а потім класифікують об’єкти в цих регіонах. Цей підхід забезпечує високу точність до 84% навіть для складних сцен, але вимагає багато обчислювальних ресурсів. Одноступеневі детектори, такі як YOLO та SSD, виконують обидві задачі одночасно, жертвуючи 5-10% точністю в обмін на 2-3 рази більшу швидкість. Цікаво, що гібридні архітектури, такі як EfficientDet, намагаються знайти баланс між швидкістю та точністю, автоматично налаштовуючи свою інфраструктуру на основі доступних ресурсів.

Розробка систем відстеження об’єктів на основі відео є вражаючим досягненням. Сучасні алгоритми, такі як DeepSORT і ByteTrack, здатні відстежувати до 500 об’єктів одночасно з частотою оновлення 120 Гц, зберігаючи їх ідентичність, навіть якщо камера тимчасово перебуває поза полем зору протягом 30 секунд [7]. Цей прогрес став можливим завдяки поєднанню глибоких нейронних мереж для візуального виділення ознак і вдосконалених алгоритмів прогнозування руху. Сучасні системи використовують не лише класичні фільтри Калмана, але й рекурентні нейронні мережі (LSTM/GRU) для моделювання нелінійних траєкторій руху, прогнозуючи рухи об’єктів із точністю до 87%. Неймовірно, але ці системи здатні «запам’ятовувати» до 10 000 унікальних ідентифікаторів об’єктів під час спостереження, що критично важливо для аналізу руху в густонаселених районах [7].

Проблемні питання застосування нейронних мереж для розпізнавання об'єктів з відео залишаються актуальними. Складність роботи в умовах обмеженої видимості є критичною для силових структур. Дослідження показують, що точність розпізнавання знижується на 40-60% при роботі в нічний час або в умовах туману. Іншою проблемою є висока обчислювальна складність, особливо для систем, що працюють на віддалених об'єктах. Сучасні моделі потребують від 4 до 32 ГБ оперативної пам'яті та значних обчислювальних потужностей, що ускладнює їх розгортання на мобільних платформах.

Перспективними напрямками розвитку систем відеоаналітики є впровадження мультимодальних підходів. Інтеграція даних від тепловізорів, радарів та звичайних відеокамер дозволяє підвищити надійність розпізнавання на 25-30%. Вражаючим прикладом ефективності такого підходу є система «SentinelEye», розгорнута на кордоні в 2023 році. Вона поєднує оптичні камери, тепловізори та радари міліметрового діапазону, що дозволило досягти 94% точності виявлення рухомих об'єктів у повній темряві та при складних погодних умовах. Система здатна класифікувати об'єкти на відстані до 8 км та визначати їх швидкість і напрямок руху з точністю до 97% [5]. Надзвичайно цікавим фактом є те, що комбінування відеоаналітики з акустичними сенсорами дозволяє виявляти об'єкти навіть поза прямою видимістю камер, використовуючи алгоритми тріангуляції звуку та відбитих радіохвиль. Технологія федеративного навчання нейронних мереж дозволяє покращувати моделі без передачі чутливих даних у централізовані сховища, що критично важливо для силових структур.

Розробка спеціалізованих нейромережевих архітектур для конкретних сценаріїв використання демонструє значний потенціал. Наприклад, мережі з увагою до частин зображення (attention mechanisms) покращують розпізнавання частково закритих об'єктів на 15-20%. Впровадження архітектури Transformer у системи комп'ютерного зору дозволило досягти нового рівня розуміння контексту сцени та взаємодії між об'єктами.

Одним із найцікавіших нововведень у цій галузі є розробка моделей відео, які поєднують розпізнавання об’єктів із розумінням природної мови. Ці моделі, такі як Flamingo (DeepMind) і VideoGPT, здатні не тільки розпізнавати об’єкти, але й описувати їхні дії та взаємодії природною мовою [3,6]. Вони досягли вражаючих показників точності до 89% у визначенні аномальної поведінки та потенційно небезпечних ситуацій.

Захоплюючим напрямком є використання нейронних мереж для відновлення деталей на зображеннях низької якості. Моделі з високою роздільною здатністю, такі як Real-ESRGAN і SwinIR, здатні збільшити роздільну здатність зображення в 4-8 разів, зберігаючи деталі, що є критичним для розпізнавання номерних знаків і облич на відстані. Реальні тести показали, що використання цих методів може підвищити точність розпізнавання текстових міток у відеозаписах низької якості на 45-60% [4].

Квантування та оптимізація нейронних мереж для розгортання на периферійних пристроях є окремим динамічним напрямком досліджень. Сучасні методи, такі як Quantization-Aware Training та динамічне зведення до форми (pruning), дозволяють зменшити розмір моделі в 5-10 разів при зниженні точності лише на 1-3% [3]. Це відкриває можливості для розгортання повноцінних систем розпізнавання на периферійних пристроях з обмеженими ресурсами.

Інтеграція нейромережевих детекторів із системами управління дронами та роботизованими комплексами створює принципово нові можливості для охорони об'єктів та проведення розвідки. Наприклад, система автономних безпілотних комплексів «SkyGuardian» використовує нейромережеві алгоритми для виявлення вторгнень на теритоії що охороняються . Безпілотні комплекси здатні ідентифікувати порушника, класифікувати його (людина, транспортний засіб, тварина) і супроводжувати до прибуття сил реагування. Точність класифікації сягає 98,3% при використанні мультимодальних датчиків.

Неймовірно цікавим є використання генеративних змагальних мереж (GAN) для симуляції різних умов спостереження та розширення навчальних наборів даних. Технологія Neural Radiance Fields (NeRF) дозволяє створювати фотореалістичні 3D-реконструкції сцен із обмеженої кількості зображень, що дає можливість тренувати алгоритми розпізнавання для будь-яких умов освітлення, погоди та кутів огляду. Доведено, що використання таких синтетичних даних підвищує стійкість моделей на 25-35% у нестандартних умовах розгортання [6].

Важливим аспектом є розробка методів, стійких до спроб обману системи. Дослідження показують, що звичайні системи розпізнавання можуть бути введені в оману за допомогою спеціальних методів або модифікацій об'єктів. Нові підходи навчання підвищують стійкість системи до таких атак на 30-40%, що критично важливо для систем безпеки.

Список використаних джерел

1. Моделі YOLOv. URL: https://docs.ultralytics.com/ru/models/yolov8/ 2. Bochkovskiy A., Wang Y., Liao H.-Y. M. YOLOv4: Optimal Speed and Accuracy of Object Detection. 2018. URL: https://arxiv.org/abs/2004.10934
3. Kartashov V., Oleynikov V., Zubkov O., Sheiko S. Optical Detection of Unmanned Air Vehicles on a Video Stream in Real-Time. 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) : Proceedings. 2019. URL: https://doi.org/10.1109/UkrMiCo47782.2019.9165362
4. Tang M., Yu B., Zhang F., Wang J. High-Speed Tracking With Multi-Kernel Correlation Filters. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2018. P. 4874-4883.
5. Jiang P., Ergu D., Liu F., Cai Y., Ma B. A Review of Yolo Algorithm Developments. Procedia Computer Science. 2022. Vol. 199. P. 1066-1073. URL: https://doi.org/10.1016/j.procs.2022.01.135
6. Szegedy C., Liu W., Jia Y., Sermanet P., Reed S., Anguelov D., Erhan D., Vanhoucke V., Rabinovich A. Going Deeper With Convolutions. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Boston, MA, USA, June 7-12, 2015. P. 1-9.

7. Fang W., Wang L., Ren P. Tinier-YOLO: A Real-Time Object Detection Method for Constrained Environments. IEEE Access. 2020. Vol. 8. P. 1935-1944. URL: https://doi.org/10.1109/ACCESS.2019.2961959

УДК 378.147:004.85

Данилюк І.А., Радзівілов Г.Д., Куцаєв В.В.

ІНТЕГРАЦІЯ КВАНТОВИХ ТЕХНОЛОГІЙ У ВІЙСЬКОВІ СПЕЦІАЛЬНОСТІ: НЕОБХІДНІСТЬ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Розвиток квантових технологій відкриває нові можливості у військовій сфері, зокрема у криптографії, навігації, розвідці та управлінні бойовими системами [1, 2]. У сучасних умовах зростаючих кіберзагроз та необхідності посилення обороноздатності держави інтеграція квантових технологій у військову підготовку є вкрай важливим завданням. Особливого значення набуває адаптація освітніх програм у військових навчальних закладах, які здійснюють підготовку фахівців за спеціальностями 122 «Комп'ютерні науки», 125 «Кібербезпека та захист інформації», 126 «Інформаційні системи та технології», 172 «Електронні комунікації та радіотехніка», 253 «Військове управління (за видами збройних сил)», 255 «Озброєння та військова техніка» [3]. У цьому контексті важливим є підготовка мультидисциплінарних спеціалістів (квантофахівців), здатних застосовувати квантові алгоритми та технології у військових операціях.

Значення квантових технологій для військової сфери полягає в тому, що квантові технології, зокрема квантові обчислення, квантова криптографія та квантові сенсори, можуть значно підвищити ефективність військових операцій [1, 2]. Одним із ключових напрямів є квантова криптографія, яка дозволяє створювати захищені канали зв'язку, що неможливо перехопити або зламати за допомогою класичних методів, а також підготовка заходів до захисту від квантових (брутальних) атак. Це критично важливо в умовах гібридної війни та кіберзагроз.

Квантові сенсори дозволяють значно покращити розвідку та навігацію, забезпечуючи високу точність у визначенні місцезнаходження об'єктів навіть в умовах активних електронних перешкод. Квантові обчислення, у свою чергу, можуть забезпечити швидке моделювання та прогнозування бойових сценаріїв, що сприятиме оперативному прийняттю рішень у бойових умовах.

Інтеграція квантових технологій у військову освіту пов'язана з низкою викликів. Перш за все, існує дефіцит кваліфікованих викладачів і науковців, які володіють необхідними знаннями в галузі квантових технологій. Крім того, навчальні заклади мають обмежені ресурси для створення сучасних лабораторій і проведення досліджень у цій сфері.

Також необхідно адаптувати навчальні програми таким чином, щоб вони відповідали сучасним потребам військової науки та технологій [3].

Це передбачає включення курсів із квантової механіки, квантової криптографії, квантових обчислень та їх застосування у військових системах. Для ефективної підготовки квантофахівців необхідно розробити методичні матеріали та впровадити практичні заняття з використанням симуляторів квантових комп'ютерів та реальних квантових засобів.

Для ефективної підготовки квантофахівців у галузі квантових технологій необхідно розробити освітньо-професійну програму, орієнтовану на квантові обчислення, квантове програмування та використання квантових засобів телекомунікацій. Така програма повинна включати фундаментальні дисципліни з квантової механіки,

квантової теорії інформації, алгоритмів для квантових комп'ютерів та практичні аспекти їх застосування у військовій сфері. Інтеграція цих дисциплін у підготовку військових квантофахівців забезпечить високий рівень їхньої кваліфікації та сприятиме розвитку інноваційних оборонних технологій.

Ключовими складовими таких освітньо-професійних програм автори вважають наступні складові:

1. Вивчення квантової фізики – для глибшого розуміння квантових технологій необхідно включити курси з квантової механіки, які розкриватимуть основні принципи суперпозиції, заплутаності, інтерференції та квантових станів, що лежать в основі квантових обчислень.

2. Квантове програмування – обов'язковим елементом навчання має стати опанування квантових мов програмування, таких як Qiskit, Quipper, Q#, OpenQASM та інших. Це дозволить студентам не тільки ознайомитися з принципами роботи квантових алгоритмів, а й розробляти ефективний програмний код для квантових обчислювальних та телекомунікаційних систем.

3. Алгоритмічні методи та криптографія – підготовка квантофахівців повинна передбачати вивчення розробки постквантових алгоритмів, здатних забезпечити стійкість до потенційних загроз квантових атак. Особлива увага має приділятися квантовій криптографії як ключовому інструменту захисту державних та військових інформаційних ресурсів.

4. Практичне застосування квантових технологій – освітні програми повинні включати лабораторні заняття з використанням квантових симуляторів та реальних квантових обчислювальних пристроїв, що дозволить слухачам перевіряти та вдосконалювати свої знання на практиці.

На думку авторів інтеграція квантових технологій у військові спеціальності полягає у наступному [3]:

122 «Комп'ютерні науки» та 125 «Кібербезпека та захист інформації»

Квантові технології безпосередньо впливають на галузі комп'ютерних наук і кібербезпеки. Навчальні програми повинні включати основи квантового програмування, методи розв'язання складних обчислювальних задач за допомогою квантових алгоритмів (зокрема алгоритму Шора та Гровера), а також принципи квантової криптографії для створення захищених комунікацій.

126 «Інформаційні системи та технології»

Військові інформаційні системи повинні бути адаптовані до використання квантових технологій. Підготовка фахівців у цій сфері має включати вивчення квантових мереж, новітніх методів передачі інформації та застосування квантових датчиків у системах зв'язку.

172 «Електронні комунікації та радіотехніка»

Квантові комунікації можуть забезпечити абсолютно безпечний зв'язок для військових підрозділів. Студенти, що навчаються за цією спеціальністю, повинні отримати знання про принципи роботи квантових радарів, квантової телепортації інформації та методи квантового захищеного зв'язку.

253 «Військове управління (за видами збройних сил)»

Квантові технології можуть значно покращити систему управління військовими операціями. Це включає аналіз великих масивів розвідувальних даних, оперативне прийняття рішень на основі квантових симуляцій та прогнозування військових дій за допомогою квантового машинного навчання.

255 «Озброєння та військова техніка»

Квантові сенсори та квантові матеріали можуть бути використані у створенні високотехнологічного озброєння. Військові інженери повинні володіти знаннями про квантові детектори, покращені методи управління бойовими системами та перспективи використання квантових технологій у військовій техніці.

Таким чином, на думку авторів, інтеграція квантових технологій у військову підготовку квантофахівців є стратегічно важливим кроком для посилення обороноздатності країни. Освітні програми у вищих військових навчальних закладах повинні адаптуватися до нових викликів та враховувати стрімкий розвиток квантових обчислень, криптографії та сенсорики. Завдяки цьому Україна зможе підготувати висококваліфікованих військових квантофахівців, здатних ефективно використовувати квантові технології у сучасних умовах ведення бойових дій та забезпечення національної безпеки.

Список використаних джерел

1. Квантовые технологии в сфере обороны и безопасности. [Електронний ресурс]. – Режим доступу: https://www.nato.int/docu/review/ru/articles/2021/06/03/kvantovye-tehnologii-vsfere-oborony-i-bezopasnosti/index.html.
2. Войтовський К. Є., «Глобальні тренди розвитку науки і технологій: нові виклики і можливості». – Національний інститут стратегічних досліджень. [Електронний ресурс]. – Режим доступу: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/globalni-trendi-rozvitkunauki-i-tekhnologiy-novi-vikliki-i.
3. Данилюк Ігор, Куцаєв Володимир, Шаповал Віталій «Перспективи та можливі напрямки підготовки квантофахівців для військової галузі.» – Збірник тез доповідей VI Міжнародної науково-практичної конференції. Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану, Одеса: Військова Академія, 2024, С. 316-317.

УДК 623.4.05

Дубовський Ю.В., Присяжний А.Є., Карлов В.Д..

АНАЛІЗ МОЖЛИВОСТЕЙ ДИСТАНЦІЙНОГО КЕРУВАННЯ СТРІЛЕЦЬКОЮ ЗБРОЄЮ

На даний час війна вносить нові вимоги в тактику застосування стрілецької зброї, а особливо великокаліберних кулеметів (ВКК), та висуває нові вимоги та підходи в підготовці особового складу. Досвід ведення бойових дій, під час широкомасштабної агресії російської федерації показує, що основна мета застосування ВКК це нанесення втрат противнику у живій силі та здійснення неможливості ведення ним ефективного і точного вогню. Також ми бачимо що в сучасному бою щільність бойових порядків противника може бути набагато менша, дальність ведення вогню набагато зростає, а цілі переважно мобільні.

Розвиток сучасних високотехнологічних зразків озброєння суттєво підвищує ймовірність ураження «дронів-камікадзе» та крилатих ракет. Але разом з тим на практиці часто застосовується загороджувальний вогонь зі стрілецької зброї, бортового озброєння бронетанкової та автомобільної техніки, кораблів. Вже ні для кого не секрет, що будь-яка літаюча ціль може бути збита. І головною проблемою у цьому є виявлення цілі та проведення успішної її атаки. З аналізу реальних бойових дій ми бачимо що для цього можуть використовуватися різні зразки озброєння. Для знищення невеликих легких БПЛА може використовуватись стрілецька зброя, особливо великокаліберна, а для знищення важких великих БПЛА потрібно залучати зенітні ракетні комплекси.

У доповіді обґрунтовано що для підвищення імовірності знищення БПЛА основна ідея полягає у забезпеченні максимальної ефективності та швидкості роботи роботизованої платформи та систем управління бойовою роботою озброєнням за рахунок систем дистанційного керування та систем машинного зору, що забезпечує

зниження людського фактору у процесах управління бойовою роботою. Стверджується, що за таких обставин першочергового значення набуває подальший розвиток та вдосконалення систем дистанційного керування стрілецькою зброєю для підвищення ефективності боротьби з малорозмірними цілями та застосуванні по наземним та надводним цілям на збільшених дистанціях ведення вогню. На прикладах ведення бойових дій ми бачимо, що такі системи дистанційного керування підвищують захищеність особового складу бойової обслуги та забезпечують адекватний рівень боротьби в якості снайперського кулемету із сучасними засобами повітряного нападу, наземними (надводними) рухомими небронюваними та легко бронюваними цілями, стаціонарними об'єктами, живою силою противника.

Проведено аналіз недоліків застосування великокаліберних кулеметів для знищення наземного супротивника та оборони військових і цивільних об'єктів; вдосконалення (модернізації) існуючих зразків зенітного та стрілецького озброєння для підвищення ефективності в боротьбі з малорозмірними повітряними цілями та проаналізовані основні науково-технічні проблеми, що виникають при модернізації стрілецької зброї. Розглянуті основні напрямками такої модернізації, а саме проведено порівняльний аналіз різних можливих способів технічної реалізації електронної апаратури та виконуючих механізмів роботизованих систем стрілецької зброї, показані їх недоліки і переваги. При цьому, на основі аналізу сучасного бойового досвіду, наведено приклад практичної реалізації здійснення дистанційного керування великокаліберним кулеметом Володимирова танковим. Показані переваги використання мікроконтролерів в різних системах дистанційного керування стрілецькою зброєю та однотипних крокових двигунів в каналах наведення. Використання мікроконтролерів в каналах наведення по азимуту та куту місця дозволяє покращити точність наведення та запам'ятовувати кутові координати пристріляних цілей для швидкого наведення на них.

Наведено результати використання стрілецької зброї у бойових діях та обґрунтовано що за розглянутими алгоритмами дистанційного керування стрілецькою зброєю можлива побудова рухомих роботизованих систем стрілецької зброї на самохідних дистанційно керованих шасі. Однак звертається увага на те що при використанні можливих засобів дистанційного керування ВКК всі способи модернізації мають бути без суттєвих змін конструкції кулеметів, в першу чергу спускового механізму.

Також наголошується, що при використанні систем дистанційного керування стрілецькою зброєю оператор знаходиться не на лінії вогню, а в безпечному місці.

Таким чином системи дистанційного керування стрілецьким озброєнням дозволяють розташовувати особовий склад бойової обслуги в безпечних місцях укриття, що підвищує захищеність особового складу бойової обслуги, вести розвідку та виявлення цілей через телевізійний оптичний приціл, прицілюватись з дуже високою точністю, керувати режимами стрільби (одиночний постріл, подвійний постріл або постріли короткими чергами – 3…5 патронів) та контролювати результати стрільби через телевізійний оптичний приціл. При стрільбі по стаціонарним об'єктам за допомогою таблиць стрільби та системи «Кропива» можна визначати дані прицілювання для першого пострілу, що дуже важливо для підвищення ефективності стрільби та маскування позицій.

Дуболазов Ю.О., Коротій О.О.

ОПТИМІЗАЦІЯ ПОШУКУ: ВЕКТОРНІ БАЗИ ДАНИХ

У часи, коли ми працюємо із величезними обсягами інформації, звичайні реляційні бази даних часто не справляються з обробкою та аналізом складних даних. Векторні

бази даних (далі - ВБД) з'явилися як відповідь на це, пропонуючи ефективний спосіб зберігання, індексації та пошуку багатовимірних даних, які представлені у вигляді векторів. ВБД призначені для роботи з різними типами даних, такими як числові ознаки, текст, зображення, аудіо та складні дані, зокрема молекулярні структури. Завдяки зростанню складності та обсягу даних, ВБД стають все більш важливими у різноманітних застосуваннях у різних галузях.

Векторна база даних – це тип бази даних, який зберігає дані як вектори високої розмірності. Ці вектори є математичними представленнями особливостей або атрибутів даних. Іншими словами, замість того, щоб зберігати дані в рядках і стовпцях (як реляційні бази даних), ВБД зберігають дані як точки в багатовимірному просторі.

Принцип роботи ВБД ґрунтується на використанні векторних вкладень, де кожному об'єкту призначається вектор, що фіксує різні характеристики об'єкта. Ці вектори розроблені так, що подібні об'єкти мають вектори, які знаходяться близько один до одного у векторному просторі. Це дозволяє ефективно виконувати пошук схожості, що є ключовим для багатьох застосувань.

ВБД зазвичай використовують один або декілька алгоритмів наближеного пошуку найближчих сусідів (англ. Approximate Nearest Neighbor, ANN). ANN дозволяють здійснювати пошук базою даних за допомогою вектора запиту, знаходячи найближчі відповідні записи бази даних.

ВБД мають декілька ключових характеристик, які роблять їх цінними для різних застосувань. Вони забезпечують ефективне керування даними, включаючи відмовостійкість і надійний механізм запитів. Крім того, вони підтримують високу продуктивність, дозволяючи виконувати запити з низькою затримкою, що є критично важливим для додатків штучного інтелекту в реальному часі. ВБД інтегрують семантичне розуміння в ранжування релевантності, підвищуючи точність результатів пошуку. Також вони ефективно індексують і зберігають вектори з великою кількістю вимірів, враховуючи складні представлення. Важливою особливістю є здатність здійснювати пошук за схожістю, що сприяє швидкому та ефективному пошуку найближчих сусідів і дозволяє оперативно ідентифікувати схожі об'єкти. Масштабованість таких баз даних дозволяє обробляти великі обсяги даних і запитів без втрати продуктивності. До того ж вони підтримують різні типи даних і запитів, роблячи їх універсальним інструментом для різних застосувань.

ВБД мають переваги над реляційними базами даних у кількох аспектах. Вони забезпечують ефективність пошуку схожості, оскільки оптимізовані для швидкого та точного пошуку, що корисно для рекомендаційних систем, пошуку зображень та обробки природної мови. Крім того, вони здатні обробляти високорозмірні дані, працюючи ефективно з великим числом розмірностей, на відміну від реляційних баз даних. Також ВБД відзначаються гнучкістю та масштабованістю, що дозволяє адаптуватися до змінних потреб та великих обсягів даних.

Однак вони мають і недоліки. ВБД більш складні у налаштуванні порівняно з реляційними базами даних. Вони також мають обмежену підтримку транзакцій, що може бути проблемою для деяких застосувань.

ВБД є відносно новою технологією. Очікується, що в майбутньому вони будуть відігравати ще більш важливу роль в обробці та аналізі даних, особливо в контексті зростання популярності штучного інтелекту та машинного навчання.

Вплив ВБД на розвиток технологій буде значним, оскільки вони:

- дозволяють ефективно керувати та використовувати складні дані;
- покращують семантичний пошук;
- підвищують продуктивність моделей штучного інтелекту;
- створюють більш точні та контекстуально релевантні відповіді.

ВБД є потужним інструментом для роботи з високорозмірними даними та завданнями, пов'язаними з пошуком схожості. Вони знаходять застосування в різних

галузях і очікується, що їх роль в обробці та аналізі даних буде тільки зростати в майбутньому.

УДК 004.01

Душкін В.Д. Сидоренко І.І.

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ІНТЕРНЕТ-РЕСУРСІВ ЗДОБУВАЧАМИ ОСВІТИ ПРИ ВИВЧЕННІ МАТЕМАТИЧНИХ ДИСЦИПЛІН

Проведення такого дослідження з виявлення пріоритетних для курсантів джерел інформації при підготовці до математичних дисциплін є актуальним завданням викладацького складу, що забезпечить у майбутньому створення саме тих видів джерел інформації, з якими найзручніше працювати здобувачам освіти.

У нашому сторіччі Інтернет є одним із основних джерел отримання інформації у різних галузях діяльності у том числі освітній. Навіть на початку сторіччя дослідження, що були проведені у рамках проекту Pew Internet & American Life Project, свідчили що 78% молодих громадян США віком від 12 до 17 років вважали, що Інтернет допомагає їм у навчанні, а 71% використовували Інтернет як основне джерело інформації. Залучення Інтернету у сферу освіти набуло широкого розмаху і в Україні. Однак результати дослідження, які були наведені у Національному звіті за результатами міжнародного дослідження якості освіти PISA-2022 свідчать, що значна кількість здобувачів освіти в українських школах не мала доступу до сучасних інтернет-технологій або цей доступ був обмежений. Таке обмеження обумовлюється різними причинами: нерівномірністю доступу до Інтернету у сільський та міський місцевості, війною в Україні та пов’язаними з нею руйнуванням інфраструктури та міграцією населення.

Анкетним методом була зібрана статистична інформація щодо визначення степеня важливості різних джерел інформації для здобувачів освіти при підготовці до виконання завдань та виконання контрольних вправ до занять та модульного контролю з дисциплін КМПД та ОВМтаФуВС. У питаннях анкети, яка була створена за допомогою Google Forms було запропоновано зробити порівняння семи різних джерел інформації:

1. Підручники та навчальні посібники обсягом більше 150 сторінок;
2. Навчальні посібники обсягом від 50 до 150 сторінок;
3. Навчальні посібники обсягом менше 50 сторінок;
4. Власний конспект;
5. Звернусь за допомогою товариша;
6. Знайду потрібний матеріал в Інтернет;
7. Скористаюсь інформацією, що надана викладачем на освітній он-лайн платформі, зокрема у Гугл клас.

Порівняння об’єктів здійснювалось за допомогою методу парних порівнянь [1,2]. Вибір цього методу зумовлений тим, що на думку психофізіологів він дає більш точні результати ніж метод простого ранжування при дослідженні великої кількості об’єктів.

До опитування було залучено 76 респондентів. За результатами обробки анкет були складені матриці попарних порівнянь. На основі аналізу цих матриць були визначені ранги усіх джерел інформації у різних підгрупах досліджуваних.

Степінь узгодженості думок здобувачів освіти перевірялась за допомогою методів кореляційного аналізу. Зокрема було проведено попарне порівняння рангів за допомогою коефіцієнта кореляції Спірмена [3,4]. Враховуючи те, що формула для обчислення коефіцієнта кореляції Спірмена є виразом формули для обчислення

коефіцієнту кореляції Пірсона у випадку ранжованих данних, для її знаходження було використано функцію Exel КОРРЕЛ. За допомогою Exel були складені матриці парних кореляцій оцінок рангів у різних підгрупах. На основі цих даних було зроблено висновок, що за шкалою Чеддока зв'язок є сильним у підгрупах з високим рівнем знань курсантів а у підрупах курсантів зі слабким рівнем знань він є помітним.

Для перевірки статистичної значущості коефіцієнтів Спірмена, використовувались розрахунки на основі t статистики. Результати обчислень довели, що більшість обчислених значень величин t статистик для підгруп з високим рівнем знань перевищують критичні значення tkp для рівня довіри 0.95.

Для перевірки узгодженості думок у всіх підгрупах одночасно по відношенню до факторів було розраховано коефіцієнт конкордації Кендалла [5]. Проведені розрахунки свідчать, що коефіцієнт конкордації у підгрупах з високим рівнем знань та усіх групах перевищує значення 0.7. Таким чином думки експертів вважаються узгодженими. Перевірка значущості коефіцієнта конкордації К ґрунтувалась на близькості статистики $M \cdot (n-1) \cdot K$ до хи-квадрат розподілу з k=n-1 ступенями вільності. Проведені обчислення свідчать про значущість узгодженості думок опитуваних у підгрупах з високим рівнем знань на рівні довіри у 95%

За результатами дослідження зроблено висновки, що основними джерелами інформації, якими користуються курсанти під час самостійної роботи є матеріали, що надані викладачем у курсі на освітній платформі Гугл клас, інформація з мережі Інтернет та матеріали власного конспекту. Друковані видання з обсягом більше 150 сторінок користуються найменшою популярністю у здобувачів освіти під час самостійної підготовки, інші друковані видання мають середній та низький рейтинг серед здобувачів освіти. Узгодженою є думка щодо пріоритетів джерел інформації у підгрупах курсантів з високим рівнем знань; у підгрупах курсантів із слабким рівнем знань не було визначено чітких пріоритетів щодо використання тих чи інших джерел інформації.

Список використаних джерел

1. Kendall, M & Smith, B.. (1940). On the Method of Paired Comparisons. Biometrika. 31. 324-. 10.1093/biomet/31.3-4.324.
2. Rossman, Allan & David, Herbert. (1989). The Method of Paired Comparisons (2nd ed.).. Journal of the American Statistical Association. 84(406). 621. DOI: 10.2307/2289964.
3. Yadolah Dodge (2008). Spearman Rank Correlation Coefficient. In: The Concise Encyclopedia of Statistics. Springer, New York, NY. https://doi.org/10.1007/978-0-387-32833-1_379
4. Spearman, C.: The Proof and Measurement of Association between Two Things. Am. J. Psychol. 15, 72–101 (1904)
5. Kendall, M.G. (1975) Rank Correlation Methods. 4th Edition, Charles Griffin, London.

Жилінський І.В., Яровий В.С., Свідзінський Ю.О., Ющенко Ю.М.

ВАРІАНТ ВВЕДЕННЯ КОМПЛЕКСНОЇ ОЦІНКИ НАДІЙНОСТІ БАЗОВОГО ШАСІ РУХОМОГО СКЛАДУ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Сьогодні, в умовах війни з рф, країни-партнери України здійснюють технічну допомогу (вогневі засоби ураження, засоби зв'язку, навігації, радіоелектронного обладнання, спостереження та попередження, автомобільна та бронетанкова техніка і т.ін.), а також активізувалося багато різних підприємств з виготовлення або модернізації базового шасі колісної техніки для потреб оборони. Для якісного виконання бойових завдань військовим

частинам необхідна надійна техніка, яка не допустить, завдяки своїй надійності, втрат особового складу бойових підрозділів, що є найголовнішим і найпріорітетнішим завданням.

Розглянуто поняття надійності базового шасі рухомого складу озброєння та військової техніки. Запропоновано в якості показника надійності базового шасі рухомого складу озброєння та військової техніки використовувати узагальнений комплексний показник надійності.

Однією з складових боєготовності базового шасі рухомого складу озброєння та військової техніки є її надійність. Підвищення надійності базового шасі рухомого складу озброєння та військової техніки є однією з найважливіших задач, які стоять перед розробниками, виробниками та фахівцями. В процесі експлуатації базового шасі рухомого складу озброєння та військової техніки, їх властивості не залишаються постійними, а під впливом внутрішніх і зовнішніх факторів з часом видозмінюються і частіше в гіршу сторону, що приводить до погіршення технічних параметрів та зниженню боєготовності.

У зв'язку з різким підвищенням складності базового шасі рухомого складу озброєння та військової техніки, необхідне ретельне наукове обґрунтування військово-технічних рішень при розробці, випробуваннях, виробництві, модернізації й експлуатації такого шасі. При цьому необхідно оцінити сучасний рівень надійності базового шасі рухомого складу озброєння та військової техніки та спрогнозувати необхідний рівень його надійності при проведені заміни техніки. Необхідно відмітити, що умови експлуатації базового шасі рухомого складу озброєння та військової техніки носять випадковий характер і мають ймовірнісні характеристики дорожніх умов, швидкостей руху, маси перевезеного вантажу (бойового обладнання), режиму руху та ін. При цьому відмови агрегатів і вузлів цієї техніки можуть виникати як при нормальних (відмови, появу яких можна чекати в різних агрегатах техніки), так і при екстремальних умовах експлуатації (дорожньо-транспортна подія, бойові дії). Тому відмови базового шасі рухомого складу озброєння та військової техніки краще розподілити на ті, які прогнозуються, і ті, які не прогнозуються. З урахуванням розглянутих властивостей та типів відмов, пропонується оцінювати надійність базового шасі рухомого складу озброєння та військової техніки комплексним показником – узагальненим коефіцієнтом надійності, який визначається наступним чином:

$$K_H = P_Б(t) \cdot P_Р(t) \cdot P_З(t),$$

де $P_Б(t)$ – ймовірність безвідмовної роботи базового шасі рухомого складу озброєння та військової техніки;

$P_Р(t)$ – ймовірність відновлення працездатного стану базового шасі рухомого складу озброєння та військової техніки після виникнення відмови;

$P_З(t)$ – ймовірність збереження працездатного стану базового шасі рухомого складу озброєння та військової техніки при зберіганні.

Таким чином залежність для оцінки рівня надійності базового шасі рухомого складу озброєння та військової техніки дозволяє визначити вплив на нього окремих властивостей та намітити шляхи забезпечення високого рівня надійності базового шасі рухомого складу озброєння та військової техніки на етапі розробки вимог до сучасних зразків техніки Збройних Сил України та інших військових формувань держави.

Заєць Я.Г., Давіденко С.В.

ЩОДО ПРОТИДІЇ ВИЯВЛЕННЮ РОБОТИ СТАНЦІЙ СУПУТНИКОВОГО ЗВ'ЯЗКУ «STARLINK»ЗАСОБАМИ РАДІОТЕХНІЧНОЇ РОЗВІДКИ

Передавальний пристрій терміналу Starlink працює в УКХ діапазоні (Ku, Ka) від 12 до 22 ГГц та невеликою потужністю. Основна потужність радіосигналу спрямована до супутників але у зв'язку з неоднорідністю атмосфери та фізичним особливостям

побудови антен та розповсюдження радіосигналів частина потужності розсіюється у просторі. Виявити працюючий комплект терміналу засобами радіотехнічної розвідки з поверхні можливо на відстані 5-10км (в окремих випадках до 30 км в залежності від умов місцевості).

Слід пам'ятати що демаскуючими ознаками терміналу є не тільки антена та сигнал антени до супутника, а і випромінення штатного супутникового модему (WiFi сигнал) що теж може бути перехоплений та виявлений засобами радіотехнічної розвідки противника.

З метою недопущення виявлення та визначення місцезнаходження терміналів супутникового інтернету «Starlink», і, як наслідок, усунення загрози в подальшому їх фізичного знищення вогневими засобами противника та негативного впливу на бойові можливості Сил оборони України, доцільно вживати заходи з протидії та приховування демаскуючих ознак терміналів «Starlink» та введення противника в оману, основними з яких є:

– зниження потужності роутера до мінімуму за допомогою програмних засобів (Зменшення потужності випромінювання Wi-Fi-роутера на величину 15-20 dBm надасть можливість зменшити дальність виявлення терміналу з 10 км до 2-3 км);

– встановлення електромагнітних екранів для зменшення рівня випромінювання Wi-Fi-роутера;

– приховування зовнішнього вигляду антени абонентського терміналу за допомогою виготовлення каркасів з радіопрозорих матеріалів, активне використанням умов місцевості та підручних предметів;

– встановлення антени подалі від місць скупчення особового складу, командно-спостережних пунктів (пунктів управління) та інших важливих військових об'єктів;

– встановлення (за можливості) роутера у приміщені з ефективним використанням його направлених властивостей;

– перебудовува штатної схеми увімкнення терміналу «Starlink» для створення провідної мережі інтернет за допомогою мережевого адаптера «Starlink Ethernet adapter» під використання звичайного Wi-Fi-роутера. Таким чином усувається основна демаскуюча ознака належності випромінювання Wi-Fi-роутера до терміналу «Starlink» (специфічний номер MAC-адреси);

– вмикання антени лише за необхідністю;

– обов'язкове вимикання антени під час оголошення повітряної тривоги або знаходження в зоні можливого ведення технічної розвідки противником;

– приховування (за необхідності) з'єднувального кабелю маскувальними засобами та природними масками;

– розгортання імітаторів роботи терміналів з імітацією MAC-адреси та потоку даних;

– створення хибних джерел випромінювання, для ускладнення встановлення місцезнаходження справжнього терміналу «starlink» у зоні спостереження комплексу радіотехнічної розвідки;

– періодична зміна ім'я Wi-Fi мережі та регулярна зміна місцезнаходження терміналу під час використання.

Зінченко М.О., Сайко В.Г., Комаров В.О.

АНАЛІЗ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ РІШЕННЯ БОЙОВИХ І СПЕЦІАЛЬНИХ ЗАВДАНЬ

Розвиток сучасних технологій дозволяє сьогодні безпілотним літальним апаратам (БпЛА) успішно виконувати функції, недоступні їм у минулому. Так БпЛА показали

високу ефективність при виконанні завдань розвідки та ведення спостереження. БпЛА стали «всевидячим оком», дозволивши оператору відстежувати та контролювати розвиток обстановки у заданому районі або на заданому маршруті у реальному масштабі часу. Головна перевага БпЛА, на думку експертів - відсутність на борту людини, тому, незалежно від складності і небезпеки завдання, що виконується БпЛА, життю пілота не загрожує небезпека.

БпЛА здатний виконувати поставлені завдання у зонах бойового зіткнення, хімічного та радіаційного зараження. Йому не потрібні складні системи життєзабезпечення екіпажу. У небезпечних ситуаціях безпілотником можна пожертвувати, особливо тоді, коли їхнє виробництво буде поставлене на потік. Завдяки перерахованим перевагам, БпЛА поступово освоюють функції пілотованої авіації.

Світовий досвід розвитку безпілотної авіації говорить про те, що вже через п'ятнадцять-двадцять років БпЛА зможуть виконувати більшість завдань, які сьогодні вирішує пілотована авіація, виключаючи деякі специфічні функції. Це такі оцінки зарубіжних військових фахівців щодо майбутнього БпЛА військового та спеціального призначення.

У ході бойових дій з'ясувалося, що БпЛА можуть успішно виконувати:

– більше 70% розвідувальних завдань на полі бою або у спецоперації;

– більше 60% завдань із забезпечення охорони військ;

– не менше 90% завдань з бойового ураження живої сили противника та його бойової техніки та озброєння;

– до 40% завдань щодо забезпечення зв'язку.

Тоді було зроблено висновок, що хоча БпЛА неспроможні повністю замінити армійську бойову авіацію, проте можуть істотно доповнити її можливості, чому є підтвердження нині, коли бойова авіація застосовується лише пуску крилатих ракет і скидання КАБ. Причина такого рішення проста: безпілотники дешевші та безпечніші для особового складу – а значить вони ефективніші. В останнє десятиліття спостерігається тенденція заміщення пілотованих повітряних машин безпілотниками в арміях економічно розвинених держав, яка поступово набуває загального характеру. Незважаючи на це, говорити про те, що незабаром над полем бою кружлятимуть лише безпілотники, рано. Незважаючи на простоту, виробництво, розробка та застосування БпЛА – складний, дорогий і трудомісткий процес. Але, як не дивно, – кількість БпЛА у військах різних країн зростає рік за роком, і зростання це вже необоротне. Разом з кількістю БпЛА, що застосовуються у військах, розширюється коло розв'язуваних ними задач. У зв'язку з цим можна виділити чотири групи факторів, що формують сучасні тенденції розвитку безпілотної авіації військового та спеціального призначення:

1) технологічні фактори – удосконалення існуючих та розвиток нових технологій розробки, виробництва та створення БпЛА різного призначення;

2) функціональні чинники – потреби замовника (військового відомства або інших відомств), щоб мати БпЛА, які б відповідали їх практичним потребам;

3) матеріально-фінансові чинники – розрахунок розумної вартості розробки, виробництва та експлуатації зразків БпЛА для відповідного відомства;

4) психологічні чинники – масове використання БпЛА принципово змінює психологію особи, яка приймає рішення.

У цих чинниках головну роль грає функціональне призначення БпЛА. Сучасний у технологічному відношенні безпілотник, нехай навіть за цілком прийнятною вартістю, не потрібен військам, якщо він не здатний задовольняти їхні вимоги.

У різних відомств існують свої вимоги до БпЛА, що ускладнює міжвідомчу взаємодію у цій галузі. Для Збройних Сил України, наприклад, важливою вимогою є низька шумність і мала помітність, а також надійні та захищені канали зв'язку з БпЛА, тоді як для Міністерства внутрішніх справ (МВС) такі вимоги не є суттєвими. Але МВС має підвищені вимоги до всепогодності апарату, здатності стабільно діяти вдень і

вночі, в умовах низьких температур. У результаті БпЛА, прийнятий на озброєння в одному відомстві, може виявитися поганим з точки зору задоволення потреб іншого відомства. Під впливом вищезгаданих факторів формуються тенденції технічного розвитку сучасної безпілотної авіації. Виходячи з аналізу досвіду розвитку безпілотної авіації передових держав, можна зробити висновок: у сучасній безпілотній авіації формуються дві різноспрямовані тенденції:

– по-перше, нарощується функціональне навантаження систем БпЛА, у тому числі, збільшуються дальність польоту та час перебування у повітрі;

– по-друге, мінімізуються розміри БпЛА.

Шляхи практичної реалізації цих двох тенденцій розвитку безпілотної авіації різноманітні. Впровадження сучасних технологій вже найближчим часом дозволяє очікувати цих напрямах проривних змін. Наприклад, удосконалення силових установок та принципово нові підходи у цій галузі покращують тимчасові та просторові параметри польоту БпЛА. Нові можливості розвитку безпілотної авіації відкриються внаслідок створення безпілотних систем автоматичної дозаправки паливом у повітрі. Це дозволить збільшити дальність польоту та час перебування у повітрі будь-якого безпілотника, зокрема й військового. У зв'язку з розвитком нанотехнологій та впровадженням штучного інтелекту відкриваються нові горизонти у розвитку міні та мікро безпілотної авіації. Такі проекти існують, але поки що недостатньо впроваджені. Наприклад, проекти передбачають створення мініатюрних систем БпЛА, здатних літати зграями (типу «рій») над противником (насамперед це зручно у міських умовах), контролюючи кожен крок та кожне слово порушників.

У зв'язку з цим на перший план виходять перспективні системи автоматичного розпізнавання цілей за закладеними в пам'ять комп'ютера зразками теплових зображень цих цілей у різних проекціях. Але, не зважаючи на всі переваги вищезазначених пристроїв та систем, що дозволяють більш ефективно спостерігати за полем бою або за територією, на якій проводяться спецоперації, виявляти цілі і порушників, в них є величезний мінус – вони малоефективні в умовах, коли середовище, що оточує транспортний засіб, перевищує за азимутом його висоту, зокрема, висоту розташування від поверхні землі пристроїв спостереження, що розміщені на в кабіні спецтранспорту. Це стосується місцевості, на якій удосталь різного типу будівель тощо. Противник (порушник) може бачити спецтранспорт, а його екіпаж не може бачити порушників та їх засідки. Рішенням цієї проблеми, на думку авторів роботи, може стати технічне рішення у вигляді застосування прив'язних висотних телекомунікаційних платформ (ВТП) на основі прив'язних БпЛА, які також отримали назву «прив'язаних дронів» – Flying COWs (Cell on Wings).

У цьому напрямку авторами пропонується оснастити об'єкт спецтранспорту обладнанням для відеоспостереження – зовнішнім прив'язним пристроєм спостереження (БпЛА мультикоптерного типу), який можна буде піднімати на висоту і здійснювати огляд місцевості перед спецтранспортом за азимутом на дальностях від 1000 метрів і більше. Прив’язні БпЛА мультикоптерного типу вирізняються мобільністю, малою вагою (через відсутність бортових акумуляторів), швидким розгортанням на місцевості чи на об'єкті техніки, та здатністю працювати в режимі висіння. Зовнішній прив'язний пристрій спостереження – БпЛА, повинен бути оснащений тепловізором, георадаром для інженерної розвідки місцевості, засобами відеоспостереження та засобами зв'язку, що зв'язані, відповідно, із системою управління вогнем та радіостанцією, які розміщені на об'єкті спецтранспорту. Управління зазначеним зовнішнім прив'язним БпЛА буде здійснюватися блоком керування, який додатково буде розміщений в спецтранспорті. Конструктивно і технологічно БпЛА мультикоптерного типу пропонується розмістити на плоскій силовій площадці, яка оснащена вузлами кріплення БпЛА в похідному положенні, що буде закріплена (як варіант конструктивного виконання), або на задній частині корпусу

спецтранспорту (з можливістю у похідному положенні опускатися вниз на вузлах повороту), або на верхній поверхні корпусу спецтранспорту. До складу системи буде входити лебідка з тросом, яка закріплюється на нижній поверхні силовій площадці, а на тросі буде розміщений оптоволоконний кабель і кабель електроживлення для зв'язку з відповідним обладнанням, що розміщене на БпЛА.

Зазначений вище БпЛА повинен мати телекомунікаційного обладнання, що підтримує стандарти 5G/LTE, WiMAX та Wi-Fi. Технологія LTE забезпечить швидкість передачі даних до 1000 Мбіт/с у низхідному каналі та до 500 Мбіт/с у висхідному. Таке обладнання потрібне там, де необхідна висока безпека передачі даних, наприклад, для розвідувальних, військових або спецоперацій в умовах застосування противником (порушниками) засобів РЕБ.

Це один з можливих варіантів застосування БпЛА, який може бути використаний як при проведенні спецоперацій відповідними структурами в умовах міста, так і на полі бою при проведенні військових операцій (шляхом розміщення БпЛА на танку чи іншому об'єкті бронетехніки).

Незважаючи на переваги, які дає використання безпілотної авіації, БпЛА має і серйозні обмеження. Широкомасштабне використання всіма країнами БпЛА, на думку фахівців, може призвести до дезорганізації процесів управління повітряним простором над районом їх використання, особливо над театром бойових дій. Складнощі координації польотів своїх БпЛА будуть багаторазово збільшені наявністю БпЛА противника. Інтерес до розвитку безпілотної авіації проявляється вже дуже давно. Великий поштовх розвитку в цій галузі було зроблено в Україні перед початком широкомасштабної війни з російським агресором. Сучасні розробки БпЛА в Україні навряд можна назвати безпроблемним. На те є безліч причин. Проте безпілотна авіація в Україні не тільки жива, а й має в ряді класів непогані переваги. Наприклад, удари сотнею БпЛА в одному вильоті по аеродромах ппротивника зі знищенням на них не лише літаків противника, а й запасу крилатих ракет.

Висновки. Проаналізувавши все вищевикладене, можна зробити восновок, що військові відомства сучасних розвинених країн світу із кожним роком роблять дедалі більшу увагу на безпілотну авіацію, хоча безпілотники не зможуть повністю замінити пілотовану авіацію ні через десять, та ні через двадцять років. Але в районах бойового зіткнення вони вкрай необхідні. Також на підставі зазначеного вище можна констатувати, що малогабаритний (і дешевий) прив'язний БпЛА у перспективі стане індивідуальним пристроєм зовнішнього спостереження кожного спецзасобу. У перспективі, при появі більш легких і малогабаритних БпЛА, для підвищення бойової ефективності спеціальних підрозділів можна буде на спецзасобі розмістити не один БпЛА, а мінімум три й більше. Використання БпЛА на базі ВТП у складі спеціальних підрозділів значно розширить перелік виконуваних завдань, включаючи інтеграцію штучного інтелекту для управління та координації дій між спецпідрозділами. Крім того, застосування БпЛА, що розміщений на спецзасобі, дозволить вирішувати спеціальні завдання з мінімальними економічними витратами.

УДК 621.396

Зубков А.М., Годебський В.П., Каменцев С.Ю., Сірий Ю.І.

ЛОКАЦІЙНИЙ ГЕОМОНІТОРИНГ ПРИБЕРЕЖНОЇ ВОДНОЇ ПОВЕРХНІ В ІНТЕРЕСАХ АНТИДИВЕРСІЙНОГО ЗАХИСТУ

Локаційний геомоніторинг, як неконтактний спосіб отримання інформації про динаміку зміни цілефонової обстановки при спостереженні наземних (надводних)

об’єктів є фізичною основою для технічного вирішення широкого класу спеціальних та економічних завдань. При цьому актуальним науково-прикладним завданням слід вважати пошук ефективних та технічно недорогих варіантів інструментального забезпечення всепогодного та цілодобового визначення та розпізнавання малоконтрастних надводних об’єктів (типові об’єкти: малий катер; міна; бойовий плавець).

Цілодобовий та всепогодний моніторинг водної поверхні на користь безпеки зони, що охороняється, можуть забезпечити лише радіолокаційні засоби. При цьому підвищення інформативності моніторингу безпосередньо пов’язане з просторовою роздільної здатності радіолокаційної станції (РЛС), яка визначається шириною діаграми спрямованості антени (ДСА) за кутовими координатами та шириною спектра зондувального сигналу по дальності. Одночасно вирішення цієї задачі може бути досягнуто тільки в короткохвильовій ділянці радіодіапазону, зокрема в міліметровому діапазоні.

При цьому полегшується апаратно-програмне комплексування з каналами спостереження інфрачервоного та оптичного діапазонів для досягнення граничної інформативності у сприятливих для них умовах.

Теоретично та експериментально обґрунтовані принципи технічної реалізації малогабаритної локаційної системи для моніторингу прибережної водної поверхні на користь антидиверсійного та протимінного захисту, що задовольняє вимогам критерію «ефективність/вартість»

Основні технічні характеристики РЛС:

1. Зона огляду:
   - за дальністю – 50…2500 м;
   - за азимутом – 120 кут. град.
2. Період обновлення радіолокаційної сцени 1,8…8,2 с.
3. Роздільна здатність:
   - за кутовими координатами – 55…65 кут.хв;
   - за дальністю – 8…9 м.
4. Потужність споживання при електроживленні 27 В – не більше 70 Вт.
5. Загальна маса апаратури – не більше 20 кг.

Мінімізація масогабаритних характеристик РЛС досягнуто за рахунок:

– повністю твердотільного апаратного виконання. Як автогенератор зондуючих сигналів і гетеродин використовуються лавино-пролітні діоди;

– відмови від когерентної обробки ехо-сигналів на користь після детекторного накопичення за допомогою рекурентного фільтра в 256 суміжних елементах за дальністю;

– оптимізації подання радіолокаційної інформації з метою досягнення ефекту тривимірності зображень, що формуються.

У процесі випробувань максимальне хвилювання водної поверхні не перевищувало 1,5 балу. Візуальне відображення інформації здійснювалося одночасно у двох взаємопов’язаних системах координат: «азимут – кут місця»; «азимут – дальність».

Експериментальні дослідження було виконано під час встановлення РЛС на рятувальні катери «ТОКМАК» ВМС України.

У процесі дослідних випробувань РЛС забезпечували виявлення:

- малого катера – на відстані до 1500 м;
- навігаційної віхи – на відстані до 1200 м;
- плаваюча міна, бойового плавця – на дальності до 600 м

Подальшим розвитком є об’єднання радіолокаційного та теплового каналів на основі інтеграції їх апертурних частин та апаратури обробки.

Висновки:

1. Досягнуті технічні характеристики РЛС дозволяють забезпечити локаційний високоінформативний геомоніторинг прибережної водної поверхні на користь антидиверсійного, протичовнового та протимінного захисту на дальностях до 2500 м.
2. Запропонований варіант технічної реалізації РЛС забезпечений вітчизняною елементною базою та матеріалами.

УДК 621.396

Зубков А.М., Красник Я.В., Мартиненко С.А.

НЕДОПЛЕРІВСЬКИЙ МЕТОД ПІДВИЩЕННЯ МАКСИМАЛЬНОЇ ДАЛЬНОСТІ РАДІОЛОКАЦІЙНОГО СПОСТЕРЕЖЕННЯ НАЗЕМНИХ ЦІЛЕЙ

Відомі технічні підходи, які направлені на вирішення задачі радіолокаційного пошуку і виявлення наземних об’єктів, в основному базуються на допплерівських методах селекції рухомих цілей. При цьому із складу об’єктів, які спостерігаються, виключаються малорухомі і нерухомі цілі, які найбільше небезпечні як джерела можливої вогневої дії [1]. Недопплерівські методи, які базуються на надрозрізненні за дальністю, значно підвищують вартість радіолокаційної апаратури [2]. Тому пошук оптимальних за критерієм «ефективність/вартість» технічних рішень, які забезпечують максимальну дальність поза залежністю від типу зондуючого сигналу (когерентний, некогерентний) і які знімають обмеження на наявність чи відсутність руху наземних цілей під час їх спостереження в тактичній глибині, являється актуальним науково-технічним завданням.

Метою роботи є підвищення дальності дії радіолокаційної станції з некогерентним передаючим пристроєм (найбільше розповсюджений на практиці магнетронний автогенератор) із збереженням апаратурної реалізації і вартісних показників.

Для компенсації енергетичних втрат некогерентного накопичення ехо-сигналів в порівнянні з когерентним накопиченням в штатному режимі роботи імпульсної радіолокаційної станції відгалужують частину потужності зондуючого сигналу та подають на вхід приймальної системи для запам’ятовування фазового «портрету» зондуючого сигналу, прийнятий ехо-сигнал в межах кожного елементу розрізнення за дальністю піддають аналогічній процедурі, інвертують фазовий «портрет» зондуючого сигналу, після чого здійснюється комплексне перемноження в межах кожного елементу розрізнення за дальністю прямого та інвертованого фазових «портретів» та когерентне накопичення результатів перемножування.

Алгоритмічно і інструментально мета досягається:

– формуванням внутрішньоперіодних «портретів» зондуючого та ехо-сигналів після квадратурного фазового детектування з використанням високостабільного опорного генератора проміжної частоти, а також обробкою зондуючого сигналу та ехо-сигналу після фазового детектування для зниження вимог до швидкодії аналого-цифрового перетворення [3];

– застосуванням керованого комутатора, керованого перемикача та опорного генератора проміжної частоти спільно з квадратурними фазовими детекторами і аналого-цифровими перетворювачами, що дає можливість фіксувати фазові «портрети» зондуючого сигналу на початку кожного радіолокаційного такту та фазові «портрети» ехо-сигналу у всіх елементах розрізнення за дальністю для виконання інверсної «згортки» при обробці в сигнальному процесорі.

Безсумнівними перевагами запропонованого способу є:

– можливість технічної реалізації на існуючій загальнодоступній елементній базі;
– можливість гнучкої програмної адаптації алгоритму обробки ехо-сигналів для

забезпечення максимальної ефективності при зміні цілефонової обстановки.

Спосіб і радіолокаційна станція для його реалізації запатентовані, а кількісна оцінка приросту ефективності підтверджена методом імітаційного моделювання.

Таким чином обґрунтований і розроблений ефективний інструмент швидкого і малозатратного підвищення дальності спостереження наземних рухомих і нерухомих цілей для радіолокаційних станцій, які стоять на озброєнні і які проектуються.

Необхідно відмітити, що запропонований метод є універсальним оскільки дає можливість компенсувати короткочасні в межах зондуючого радіоімпульсу частотні нестабільності, а також в поєднанні із традиційною системою фазової автоматичної підстройки частоти компенсувати довгочасні нестабільності, які визначаються електроживленням передаючого пристрою.

Список використаних джерел

1. Бакулев А.П., Степин В.М. Методы и устройства селекции движущихся целей. – М.: Радио и связь, 1986. – 288 с.
2. Зубков А.Н. Системы радиовидения миллиметрового диапазона. 1. Принципы построения. Радиоэлектроника. 2005, № 9. С 3-16. 2. Сопоставление и интеграция с оптическими каналами, результаты эксперимента. Радиоэлектроника. 2005, № 10. С 3-10.
3. Спосіб обробки некогерентної пачки ехо-сигналів та радіолокаційна станція для його реалізації: патент 125250 Україна: МПК G01S13/00; заявл. 2.04.2018; опубл. 09.02.2022, Бюл. № 6.

УДК 623

Іванець М.Г., Горєлишев С.А., Іванець Г.В., Баулін Д.С., Хроль Л.О., Кириченко М.І.

СИСТЕМНИЙ ПІДХІД ДО РОЗРОБКИ КЕРУЮЧОГО АЛГОРИТМУ ОЦІНЮВАННЯ БОЄЗДАТНОСТІ ВІЙСЬКОВИХ ПІДРОЗДІЛІВ

Сучасна війна є випробуванням матеріальних та духовних сил народу, держави і її Збройних Сил, що спонукає кожну країну підтримувати свою обороноздатність на такому рівні, щоб гарантовано забезпечити надійний захист суспільства. Обороноздатність держави характеризує її здатність до захисту у разі збройної агресії або збройного конфлікту. Можливості держави щодо забезпечення воєнної безпеки залежать від боєздатності військових підрозділів.

У загальному випадку боєздатність військового підрозділу визначається ступенем укомплектованості, станом озброєння та військової техніки (ОВТ), рівнем підготовки особового складу та його морально-бойовими якостями, злагодженістю підрозділів і штабів, забезпеченістю матеріальними засобами та іншими чинниками [1].

Боєздатність військового підрозділу як єдиної цілісної системи під час виконання бойових завдань залежить від потенційної технічної спроможності цього підрозділу та рівня професійної і морально-психологічної підготовки особового складу до виконання завдань за призначенням:

$$БЗ = F(П_Т, Р_{ПМП}), \quad (1)$$

де $БЗ$ – рівень боєздатності військового підрозділу; $П_Т$ – потенційна технічна спроможність військового підрозділу до виконання завдань за призначенням (ведення бойових дій); $Р_{ПМП}$ – рівень професійної та морально-психологічної підготовки

особового складу підрозділу до виконання завдань за призначенням (ведення бойових дій) [2].

Потенційна технічна спроможністю підрозділу до ведення бойових дій характеризує ступінь відповідності укомплектованості, технічної готовності, ресурсу, тактико-технічних характеристик озброєння та військової техніки підрозділу складності задач, що виконуються. Вона визначається сукупністю матеріальних факторів, які характеризують їх стан та здатність до виконання завдань за призначенням.

Величина потенційної технічної спроможності військових формувань та підрозділів залежить від показників технічної досконалості зразків озброєння та техніки даного формування (підрозділу), а також від експлуатаційних показників цих зразків:

$$П_T = G(K_{TD}, K_E), \quad (2)$$

де K_{TD} – узагальнений коефіцієнт технічного досконалості зразків ОВТ певного військового підрозділу; K_E – узагальнений експлуатаційний коефіцієнт зразків ОВТ певного військового підрозділу.

Під технічною досконалістю зразків ОВТ (технічним рівнем зразків) [3,4] розуміють відносну характеристику якості цих зразків, яка основана на співставленні значень показників ТТХ, що характеризують технічну довершеність оцінюваних зразків, з відповідними значеннями показників базових зразків, прийнятих за еталон.

Узагальнений експлуатаційний коефіцієнт усіх зразків ОВТ військового підрозділу визначається укомплектованістю, технічною готовністю та запасом ресурсу ОВТ підрозділу [5].

Боєздатність військових підрозділів в значній мірі залежить від якості професійної підготовки особового складу та рівня морально-психологічної підготовки до виконання завдань за призначенням. Рівень професійної та морально-психологічної підготовки особового складу визначається укомплектованістю особового складу підрозділу спеціалістами, професійною та морально-психологічною підготовкою до дій в бойових умовах.

$$P_{ПМП} = H(P_{ОС}, P_{ПП}, P_{МП}), \quad (3)$$

де $P_{ОС}$ – ймовірність укомплектованості особового складу підрозділу спеціалістами; $P_{ПП}$ – ймовірність професійної підготовленості до виконання завдань за призначенням (ведення бойових дій): $P_{МП}$ – ймовірність морально-психологічної підготовленості до виконання завдань за призначенням (ведення бойових дій).

Професійна підготовленість до виконання завдань за призначенням (ведення бойових дій) характеризується комплексом знань, умінь, навченості особового складу веденню бойових дій у різній обстановці та у відповідності з їх призначенням, наявністю професіонального досвіду особового складу військового підрозділу [6,7]. Морально-психологічна підготовка спрямована на підвищення психічної стійкості та психологічної готовності особового складу до дій у бою у складних і небезпечних умовах, в обстановці, яка різко змінюється, під час тривалої нервно-психологічної напруги, подолання труднощів, пов’язаних із виконанням військового обов’язку.

Керуючий алгоритм оцінки боєздатності військових підрозділів до виконання завдань за призначенням дозволяє реалізувати системний підхід до оцінювання рівня бойових можливостей підрозділів в залежності від їх потенційної технічної спроможності до виконання завдань за призначенням, ступеня укомплектованості підрозділів спеціалістами та озброєнням, рівня професійної та морально-психологічної підготовки особового складу до ведення бойових дій. Керуючий алгоритм складається з 10 блоків, які розміщені на 6 ієрархічних рівнях.

При цьому передбачається виконання наступних процедур:

– збір, обробку, аналіз інформації про укомплектованість підрозділів озброєнням і технікою, технічний стан, тактико-технічні та експлуатаційні характеристики наявних

та еталонних зразків озброєння;

– збір, обробку, аналіз інформації про укомплектованість підрозділів особовим складом, рівень професійної та морально-психологічної підготовки;

– оцінку потенціальної технічної спроможності підрозділів до виконання завдань за призначенням;

– оцінку ймовірності укомплектованості особового складу підрозділу спеціалістами;

– оцінку ймовірностей професійної та морально-психологічної підготовленості особового складу підрозділів до виконання завдань за призначенням;

– оцінку боєздатності підрозділу;

– формування рішення щодо покращення показників боєздатності підрозділу;

– аналіз ефективності заходів щодо покращення боєздатності підрозділу та корегування рішення.

Це дозволяє обґрунтовано формувати рішення щодо підвищення ефективності заходів, спрямованих на підтримання та відновлення боєздатності підрозділів в разі необхідності. Напрямком подальшого дослідження є встановлення більш детальніших взаємозв'язків між елементами та блоками різних рівнів та автоматизація даних процесів.

Список використаних джерел

1. Романенко І.С., Шуєнкін В.О., Можаровський В.М. Теорія відвертого збитку: монографія. Львів: Національна академія Сухопутних військ України, 2017. 244.
2. Іванець Г.В., Горєлишев С.А., Іванець М.Г. Формалізована математична модель оцінки боєздатності військових підрозділів. *Честь і закон. Харків: НАНГУ*, 2024. № 2(89). С. 62-69. DOI: https://doi.org/10.33405/2078-7480/2024/2/89/309190
3. Василевський О.М., Ігнатенко О.Г. Нормування показників надійності технічних засобів: навчальний посібник. Вінниця: ВНТУ, 2013. 160с.
4. Іванець Г.В., Іванець М.Г., Манжура С.А. Методика оцінки технічної готовності військових підрозділів до виконання завдань за призначенням. *Збірник наукових праць Національної академії Національної гвардії України*. Харків: НАНГУ, 2024. № 2(44). С. 58-68. DOI: https://doi.org/10.33405/2409-7470/2024/2/44/319447
5. Іванець Г.В., Іванець М.Г., Горєлишев С.А., Баулін Д.С., Башкатов Є.Г. Формалізована математична модель забезпечення готовності реагування на надзвичайні ситуації. *Вісник Національного технічного університету «ХПІ». Серія: Машинознавство та САПР*. 2020. №2. С.51-57.
6. Формалізація понять бойової готовності, бойової виучки і підготовки офіцерських кадрів та визначення їх динаміки / Біжан І.В., Ткаченко В.І., Пічугін М.Ф. та ін. *Збірник наукових праць ХВУ*. 2001. №7(37). С. 3-7.
7. Пічугун М.Ф., Карлов Д.В., Воловодюк А.С., Клімішен О.О. Оцінювання впливу системи пілготовки військовослужбовців у навчальних центрах на стан бойової готовності Збройних Сил України. *Збірник наукових праць Харківського університету Повітряних Сил.* 2016. Вип. 2(47). С. 226 – 229.

Калачова В.В., Місюра О.М., Бабенко О.І., Гаврилов Д.С.

ВТІЛЕННЯ ДОСВІДУ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО НАВЧАННЯ ПРОВІДНИМИ ЗАКЛАДАМИ ВИЩОЇ ОСВІТИ УКРАЇНИ В ПІДГОТОВКУ ТА ДІЯЛЬНІСТЬ СИЛОВИХ СТРУКТУР В УМОВАХ ВОЄННОГО СТАНУ

Дванадцятий рік триває російсько-українська війна. Минуло вже три роки, як розпочалось повномасштабне вторгнення окупаційних військ рф на територію України.

На сьогоднішній день кількість руйнацій та пошкоджень досягла значення в 200 000, на відновлення яких потребується більше ніж $500 млрд і, на жаль, ці цифри продовжують збільшуватися щодня! На вересень 2024 року в Україні постраждало від бомбардувань та обстрілів 3798 закладів освіти, 70 з яких – заклади вищої освіти. З них 365 – зруйновані повністю, 5 з яких – університети. Одним з тих міст, яке зазнало величезну кількість руйнувань в результаті повномасштабного вторгнення, є Харків. Згідно з інформацією від Харківського міського голови, на кінець лютого 2025 року, кількість пошкоджених будівель в місті досягла значення близька 8000; руйнувань зазнали: близька 50 % дитячих садочків та шкіл міста, велика кількість об'єктів критичної інфраструктури, соціальні та культурні заклади, лікарні, музеї, бібліотеки тощо! Загальна сума збитків, яких зазнало місто з початку повномасштабного вторгнення рф, вже перевищила $10 млрд! Сумарна ж тривалість повітряних тривог в Харків протягом лише 2024 року, склала 156 діб!!!

Саме в таких жахливих умовах, навчальні заклади України на початку березня 2022 року, змушені були знаходити можливі шляхи вирішення питання щодо організації навчального процесу, який мав бути максимально наближеним до звичного варіанту та безпечним для життя і здоров'я здобувачів освіти та викладацького складу в період дії правового режиму воєнного стану. Після нетривалої перерви в декілька тижнів, навчальні заклади України поновили свою роботу, використовуючи для цього все різноманіття існуючих форм навчання: від стандартної очної його версії (для значно віддалених від лінії фронту регіонів) до виключно дистанційної (в районах, наближених до зони ведення бойових дій), і керуючись Наказами МОН та МО України.

Активне залучення в навчальний процес тих інформаційних технологій дистанційного навчання, які довели свою ефективність під час вимушеного довготривалого карантину 2020-2021 років, пов'язаного з пандемією коронавірусної інфекції COVID-19, та всебічна спонсорська підтримка з боку країн-партнерів України щодо надання доступу до інформаційних технологій дистанційного навчання (додатків, сервісів, платформ тощо), дозволили нашим навчальним закладам не тільки швидко повернутися, майже, до тих самих показників якості освіти, що були до повномасштабного вторгнення, але і зайняти в кінці 2024 року почесні місця (друге та третє) в міжнародному рейтингу The Online Learning Rankings серед кращих університетів світу, які пропонують освітні програми з використанням дистанційних технологій!

10 грудня 2024 року оприлюднено перший рейтинг з онлайн-навчання The Online Learning Rankings 2024. Загалом, до рейтингу увійшли 56 університетів з різних країн світу, таких, наприклад, як: Австралія, Велика Британія, Індія, Іспанія, Німеччина, Саудівськаї Аравія, США, Туреччина та інші. Ще 64 заклади вищої освіти (ЗВО), які заповнювали анкети на участь в оцінюванні, отримали статус «Reporter».

Каразінський університет (ХНУ ім. Каразіна), поряд з 30 іншими ЗВО, увійшов до категорії «Bronze» (третє місце). З українських університетів до рейтингу також увійшли Сумський державний університет (СумДУ) та Національний технічний університет «Харківський політехнічний інститут» (НТУ «ХПІ»), які потрапили до категорії «Silver» (друге місце).

Підтримка сучасних інформаційних технологій займає важливе місце у діяльності ХНУ ім. Каразіна. Незважаючи на війну, університет має понад 200 сайтів (веб-сайти університету, Вченої ради, вступної кампанії, наукової періодики, Центральної наукової бібліотеки, факультетів, навчально-наукових інститутів, кафедр, науково-дослідних інститутів, інших підрозділів та університетських проєктів), що за підсумками 2024 року репрезентують його діяльність та забезпечують інформаційну підтримку роботи з основними цільовими аудиторіями університету. Навчання студентів проходить на освітньому сайті Центру електронного навчання за допомогою апробованої і широко поширеної системи управління навчанням Moodle. Освітня

платформа LMS Moodle та курси дистанційного навчання цього ЗВО розміщенні на хмарних просторах Microsoft Azure. Кожен студент має свій Особистий кабінет на платформі Moodle, навчальний розклад та графік навчального процесу. Теоретичний матеріал вивчається як в режимі off-line, за допомогою електронних навчальних курсів, підручників, аудіо- та відеолекцій, так і в режимі on-line (відео-конференція в ZOOM згідно розкладу занять). Засвоєння практичного матеріалу здійснюється за допомогою віртуальних лабораторних робіт, практичних занять, диспутів і семінарів у режимі відео-конференцій (ZOOM), отримання консультацій у викладачів (в режимах on-line відео/аудіо конференції або off-line). Перевірка знань (проведення модульних/семестрових контрольних заходів, заліків, іспитів) здійснюється засобами платформи LMS Moodle у Особистому кабінеті здобувача освіти. Захист же бакалаврських та магістирських кваліфікаційних робіт, потребує обов'язкового здійснення відео-фіксації події і відбувається він в режимі відео-конференції (наприклад, за допомогою програмного додатку ZOOM). Студентами університету під час дистанційного навчання також використовується вебсервіс Google Classroom. Основна мета цього сервісу - прискорити процес поширення файлів між педагогами та здобувачами освіти. В свою чергу, Google Classroom об'єднує в собі такі веб-сервіси, як: Google Drive – для створення і обміну завданнями; Google Docs, Sheets and Slides - для їх написання; Gmail – для спілкування; Google Calendar – для розкладу та інші вебсервіси. Здобувачі освіти можуть бути запрошені до класу через приватний код, або автоматично імпортуватися з освітнього сайту Центру електронного навчання. Кожна навчальна група створює окрему папку на Google диску відповідного користувача Google Drive, куди подається робота, котру оцінює викладач. Мобільні додатки, доступні на iOS і Android, дозволяють користувачам робити фото та прикріпляти їх до завдань, ділитися файлами з інших додатків та мати офлайновий доступ до інформації. Педагог може відстежувати прогрес кожного здобувача освіти, а після оцінки його роботи, повернути її, супроводжуючи коментарями.

Одним з напрямів освітніх інновацій, що активно розвиваються в НТУ «ХПІ» та безпосередньо скеровані на вдосконалення навчального процесу й підвищення якості освіти, є інформатизація освіти. Найважливішою ланкою цього процесу є застосування інформаційно-комунікаційних технологій у навчальному процесі. Водночас відбуваються зміни змісту та методики навчання, тобто формуються та розвиваються новітні інформаційні освітні технології. Безперервно розвивається інструментальне та програмне забезпечення е-навчання. У навчальному процесі активно використовуються дві власні навчальні оболонки, розроблені безпосередньо фахівцями університету: «Веб-клас ХПІ» та «Система інформаційного менеджменту» (СІМ). Навчальна оболонка «Веб-клас ХПІ» функціонує з 2001 року. З допомогою цієї оболонки розроблено понад 200 дистанційних курсів. Навчальна оболонка «Система інформаційного менеджменту» (СІМ) функціонує в університеті з 2004 року. Навчальним закладом ще в період дії карантину 2020-2021 років, пов'язаного з пандемією коронавірусної інфекції COVID-19, також активно використовувалася для дистанційного навчання платформа LMS Moodle. У цьому інформаційному середовищі на кінець 2021 року було вже створено понад двох тисяч різних дистанційних курсів. Широкомасштабна збройна агресія РФ по відношенню до нашої країни спричинила важку ситуацію як в місті, так і в університеті. Відповідним наказом 24.02.2022 року був утворений тимчасовий штаб оперативного керування життєдіяльністю НТУ «ХПІ». Важким етапом була евакуація студентів, в тому числі іноземців, викладачів та співробітників університету в безпечні місця проживання, яка була успішно виконана. Для забезпечення здійснення навчального процесу під час війни, протягом двох тижнів було здійснено збір інформації стосовно місцезнаходження викладачів, співробітників, студентів університету та встановлення зв'язку з ними. Згідно з наказом від 25.02.2022 було здійснено переведення навчального процесу в дистанційний режим з

використанням платформи Microsoft Office 365 for Education. Наказом від 25.03.2022 було зобов'язано забезпечити підключення науково-технічної бібліотеки до мережі Інтернет, забезпечити підключення Університету до ЄДЕБО, налагодити зв'язок з НАЗЯВО, ДП Інфоресурс, ДСЯО. Наказами від 17.01.2023 та від 29.05.2023 було затверджений оновлений графік навчального процесу. Врахований перехід від дипломного проектування до проведення випускних кваліфікаційних іспитів на бакалавраті із забезпеченням перерозподілу кредитів. Атестація здобувачів вищої освіти здійснювалась у відповідності до термінів оновленого графіку навчального процесу. Атестація здійснювалась у дистанційній формі з використанням платформи Microsoft Office 365 for Education, офіційна ліцензія якої була на момент прийняття рішення присутня в НТУ «ХПІ». Викладацький склад і здобувачі вищої освіти в повній мірі скористались перевагами додатку Microsoft Office, а саме. Платформа Microsoft Office 365 Education має ряд переваг порівняно з багатьма іншими хмарними сервісами. Хмарні сервіси цієї компанії надаються навчальним закладам безкоштовно. Це дуже вагома перевага, оскільки створення і підтримка продуктів такого класу і якості вимагає від компаній-розробників значних ресурсів. Ці сервіси створюються спеціалістами найвищого класу. Це забезпечує стабільну роботу, мінімальну кількість помилок, які швидко виправляються, висока стійкість до злому, відповідність сучасним веб-стандартам, коректне відображення в різних браузерах тощо. Хмарні сервіси цієї компанії регулярно оновлюються. Адаптивний (респонсивний) дизайн цього програмного додатку забезпечує коректне відображення сайтів на мобільних пристроях. Завдяки цьому для роботи з ресурсами, створеними на базі хмарних сервісів цієї компанії, студенти можуть використовувати власні мобільні телефони. Додатку також притаманна простота та зручність користування. Його інтерфейс інтуїтивно зрозумілий.

Сумський державний університет (СумДУ) зайняв почесне друге місце в рейтингу найкращих університетів, які пропонують освітні програми з використанням дистанційних технологій. Ініціювала проведення рейтингу провідна британська агенція Times Higher Education. «MiX» - єдина навчальна платформа СумДУ, яка інтегрована в АСУ «Університет». Ця платформа являє собою систему управління навчанням і є власною розробкою університету. Дизайн інтерфейсу платформи сучасний і інтуїтивно зрозумілий. Інформаційне середовище платформи вміщує в собі велику кількість електронних ресурсів у вигляді курсів дисциплін, що викладаються в університеті, електронних підручників, відео-лекцій тощо. Також, за грантовою програмою від польського фонду Інтермаріум, Сумський державний університет безкоштовно отримав освітню ліцензію на програмне забезпечення FlexSim - програмний продукт, призначений для моделювання та аналізу складних процесів та систем, який надає аналітикам виробничих систем безризикове середовище для побудови та проведення експериментів над моделями.

УДК 621.382.2 + 351.75

Катеринчук І.С., Хоптинський Р.П.

ВИКОРИСТАННЯ П'ЄЗОРЕЗОНАНСНИХ СИСТЕМ У КІБЕРФІЗИЧНИХ СИСТЕМАХ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ

Постановка проблеми. Сучасні загрози, зокрема бойові дії з відсічі агресії рф, гібридні та інформаційні атаки, нелегальна міграція, контрабанда, терористичні дії та спроби незаконного проникнення, ставлять під сумнів традиційні методи охорони кордону та потребують розроблення та використання нових інтелектуальних

технологій і систем. Так Стратегією розвитку Державної прикордонної служби України, що схвалена розпорядженням Кабінету Міністрів України від 23.11.2015№ 1189-р, передбачено створення інтелектуальної системи охорони державного кордону, яка дозволяє інтегрувати сучасні технології для своєчасного виявлення загроз, що є ключовим фактором у забезпеченні стабільності та суверенітету держави. Інтелектуальні системи охорони кордону базуються на застосуванні штучного інтелекту, машинного навчання, Інтернету речей (IoT), біометричних технологій та систем аналізу великих даних. Ці технології дозволяють об'єднати різноманітні джерела інформації (відеоспостереження, радіолокаційні сенсори, п’єзорезонансні пристрої) в єдину мережу, що забезпечує комплексний моніторинг та оперативне реагування. Така система здатна аналізувати дані у режимі реального часу, що забезпечує швидке виявлення і локалізацію загроз, а також оперативну координацію сил безпеки. Це дозволяє мінімізувати час реагування і знизити ризики для державного кордону. Автоматизація процесів спостереження та аналізу даних дозволяє оптимізувати витрати людських та фінансових ресурсів. Завдяки впровадженню сучасних алгоритмів та технологій можна значно знизити витрати на експлуатацію систем охорони та підвищити їх продуктивність. Інтелектуальна система охорони кордону сприяє інтеграції кібербезпеки, фізичної охорони та інформаційних технологій, що створює єдину ефективну систему захисту. Це дозволяє краще координувати дії між різними службами та оперативно реагувати на складні загрози. Сучасні військові конфлікти характеризуються швидкими змінами оперативної обстановки. Інтелектуальні системи здатні адаптуватися до цих змін, аналізувати ситуацію та прогнозувати розвиток подій, що є критично важливим для своєчасного прийняття рішень на кордоні. Впровадження Інтелектуальної системи охорони державного кордону дозволить підвищити рівень національної безпеки України, оптимізувати використання ресурсів, забезпечити оперативне реагування на загрози та створити стійку основу для протидії сучасним викликам; оперативно виявляти і локалізувати спроби несанкціонованого проникнення чи інші загрози; забезпечувати безперервний моніторинг кордону навіть у складних умовах (погодні, географічні особливості, радіоелектронні перешкоди); інтегрувати різні джерела даних для отримання максимально повної картини ситуації; автоматизувати процес прийняття рішень, що сприяє швидкому реагуванню служб охорони кордону.

Інтелектуальна система охорони державного кордону передбачає розгортання [1] – [3]: мережі інтегрованих веж з обладнанням технічного спостереження (радіолокаційні станції, оптико-електронні камери) та засобами передачі даних (для відкритих і рівнинних ділянок); бездротових систем спостереження, здатних здійснювати фото (відео) зйомку при виявлені руху об’єкта (людина, тварина, автомобіль) в полі зору камери і автоматичну передачу отриманого зображення на мобільний термінал або комп’ютер (для напіввідкритих гірсько-лісистих ділянок); сигналізаційних комплексів охорони протяжних ділянок українського виробництва на лінійній частині існуючого загороджувального паркану (колишніх сигналізаційних систем або комплексів) – на окремих напрямках; систем відеоконтролю і сигналізації шляхом встановлення мультиспектральних камер та датчиків на існуючі металеві спостережні вежі; пересувних комплексів технічного спостереження (на базі позашляховика) з можливістю одночасного здійснення радіолокаційного та оптико-електронного спостереження тощо. В основу побудови цих елементів покладено застосування кіберфізичних систем, які представляють собою інтегровані рішення, що поєднують фізичні компоненти (сенсори, камери, датчики) та програмне забезпечення для збору, обробки та аналізу даних. Ці системи дозволяють здійснювати ефективний моніторинг та контроль державного кордону, забезпечуючи високий рівень безпеки.

П’єзорезонансні пристрої знайшли широке застосування в якості засобів стабілізації й селекції частоти – кварцових резонаторів, генераторів й фільтрів, що призначені для

засобів і систем радіотехніки та телекомунікацій, систем радіолокації та навігації, керування, контрольно-вимірювальної техніки тощо. Кварцові резонатори та п’єзорезонансні пристрої на їх основі широко застосовуються в апаратурі космічних і наземних станцій, системах точного часу, системах супутникової навігації, в приймально-передавальному обладнанні космічних апаратів та наземних станцій дистанційного зондування Землі та базових станцій стільникового зв'язку стандартів GSM, CDMA, WCDMA, TD-SCDMA, WiMax, Wibro, в системах оптичного зв’язку, в різноманітних переносних та мобільних радіостанціях та інших.

У досліджені запропоновано використання квадратурного цифрового синтезатора частоти прямого синтезу з тактовим з двочастотним термокомпенсованим кварцевим генератором для підвищення ортогональності опорних сигналів та покращення температурних характеристик квадратурного демодулятора. Таке технічне рішення дозволяє суттєво підвищити точність та завадостійкість демодуляції квадратурних сигналів за рахунок усунення температурно-залежної похибки втрати ортогональності опорних коливань та суттєвого зменшення частотної неузгодженості сигналів.

Напрямками подальших досліджень є оцінка чутливості, діапазону частот, енергоспоживання та інших параметрів, розробка архітектури інтегрованої системи охорони кордону, що поєднує п’єзорезонансні датчики з іншими сенсорами (відеокамерами, радарними системами, IoT-пристроями), забезпечення взаємодії між апаратною частиною та інформаційно-комунікаційними мережами, створення методів аналізу та інтерпретації сигналів, що надходять від п’єзорезонансних систем, з метою виявлення характерних патернів, пов’язаних із незаконним проникненням або іншими загрозами, використання методів машинного навчання для підвищення точності класифікації подій.

Список використаних джерел:

1. Басараб О.К. Щодо створення «інтелектуальної» системи охорони державного кордону / Матеріали міжнародної науково--практичної конференції «Інформаційний вимір гібридної війни: досвід України». Київ: НУОУ, 2017. С. 16
2. Катеринчук І.С. Високотехнологічні розробки в інтересах національної безпеки та оборони // Збірник наукових праць № 2. Хмельницький: Вид-во НДІ ДПСУ, 2012, с. 68-72
3. Anatolii Babaryka, Ivan Katerynchuk, Oksana Komarnytska. Technologies for Building Intelligent Video Surveillance Systems and Methods for Background Subtraction in Video Sequences / Future Intent-Based Networking, LNEE 831, pp. 468-480, 2022. https://doi.org/10.1007/978-3-030-92435-5_26
4. Babaryka, A., Katerynchuk, I., Chesanovskyi, I. A Survey of Intrusion Detection Methods in Wireless Networks. Lecture Notes in Electrical Engineering, 2023, 965 LNEE, hh. 305-3016. Babaryka, A., Katerynchuk, I., Chesanovskyi, I. A Survey of Intrusion Detection Methods in Wireless Networks. Lecture Notes in Electrical Engineering, 2023, 965 LNEE, pp. 305-3016

УДК 614.841.3; 621.315

Катунін А.М., Коломійцев О.В., Роянов О.М., Щолок А.В.

ОЦІНЮВАННЯ НАГРІВУ НАВАНТАЖЕНИХ АЛЮМІНІЄВИХ ПРОВОДІВ ІЗ ДОМІШКАМИ ТИТАНУ У СКЛАДІ СТРУМОВІДНИХ ЖИЛ

Забезпечення безперервного функціонування системи електропостачання на сьогодні є одним з важливих завдань як у військовому, так і у цивільному секторах

економки України. При цьому, особлива увага приділяється оцінюванню пожежної безпеки кабельного господарства, як однієї зі складових системи електропостачання.

Кабелі та проводи при експлуатації у аварійних режимах роботи нагріваються до температур, значення яких можуть бути достатніми для займання ізоляційних матеріалів, що може спричинити до пожеж [1,2]. Тому, на практиці, для профілактики пожеж доцільно оцінювати температуру, до якої може нагріватися кабельний виріб до моменту спрацьовування системи (апарату) захисту.

Найбільш розповсюдженими металами для виготовлення струмовідних жил для кабелів та проводів є мідь та алюміній. На фоні високих цін на мідь алюміній набирає привабливості у якості сировинного матеріалу з точки зору витрат на виготовлення кабельних виробів.

Мідь значно важче алюмінію (щільність міді становить 8,9 г/см^3, алюмінію – 2,7 г/см^3). Отже, мідний провідник у 3,3 рази важчий за алюмінієвий при однаковому розмірі. Однак, алюміній має лише 0,61% провідності міді, і щоб провести такий самий струм, алюмінієвий провідник повинен бути більше мідного за площею на 0,61%.

На даний час цінове відношення між міддю та алюмінієм сягає 3,5 разів. У свою чергу, аналіз необхідних обсягів ізолюючого та захисного матеріалів для виготовлення алюмінієвих проводів вказує на додаткове зниження цінової привабливості алюмінію – за умови, якщо потрібно виготовлять алюмінієвий провід, який буде еквівалентним за струмовим навантаженням мідному, то необхідно забезпечити витрати ізолюючого та захисного матеріалів більше, ніж для мідного проводу.

При оцінюванні пожежної небезпеки кабельних виробів одною з основних характеристик металу струмовідної жили є його електрична провідність. Але, до матеріалів струмовідних жил пред'являються й інші вимоги, які обумовлені особливостями їх експлуатації. З метою покращення таких характеристик, як корозійна стійкість, механічна міцність, жаростійкість у складі алюмінієвих провідників кабельних виробів використовуються домішки інших металів. Основна мета додавання домішок до складу струмовідних жил – покращення експлуатаційних характеристик кабельних виробів.

У [3] проведено аналіз характеристик алюмінію із домішками різних металів. Поряд з покращенням певних властивостей алюмінієвого провідника введення домішкових елементів призводить до зменшення його електричної провідності. При цьому, ступінь та характер даної зміни залежать від властивостей як алюмінію, так і домішок.

Так, титан може додаватися у невеликих кількостях як легувальний елемент для покращення властивостей алюмінієвих сплавів.

До особливостей застосування титану як легувального елементу у алюмінієвих сплавах можливо віднести наступне:

– титан додається у кількостях до 0,15% для зменшення розміру зерна металу (зміцнення структури).

– у якості домішки титан покращує міцність та корозійну стійкість;

– у якості домішки титан надає стабільність матеріалу при високих температурах.

Зниження електричної провідності матеріалу провідника за рахунок наявності домішки титану призводить до зростання температури нагріву навантаженого алюмінієвого проводу у цілому. Нагрів може призвести до займання ізоляції, що може вивести з ладу кабельну лінію або спричинити пожежу.

У [2] використано методику обчислення залежності температури T нагріву матеріалу ізоляції одножильного електричного проводу з одношаровою ізоляцією від сили струму I, що протікає, та часу t його протікання.

На основі наведеної методики отримано графіки залежності температури T нагріву проводу маркорозміруАПВ1 2,5 без домішок та з домішками титану різних об’ємів від часу роботи t при струмах навантаження I=14 А, 24 А, 34 А.

Отримані результати дозволяють зробити наступні висновки щодо впливу домішок

титану на температуру нагріву навантаженого алюмінієвого проводу:

– при струмі навантаження I=14 А температура нагріву навантаженого проводу маркорозміру АПВ1 2,5 за 300 с не досягає 70°С (допустимої тривалої температури проводів з полівинилхроридною ізоляцією), що підтверджує відповідність використаної методики нормативним положенням [4];

– температура нагріву навантаженого проводу маркорозміру АПВ1 2,5із домішками титану об'ємами 0,05 % та 0,1 % до основного матеріалу струмовідної жили залежить як від об'єму домішок у складі струмовідної жили, так і від режиму роботи (струму навантаження);

– незначні об'ємі домішок титану до основного матеріалу струмовідної жили (0,05 %) спроможні впливати на температуру нагріву навантаженого алюмінієвого проводу;

– графіки залежностей температури нагріву проводу маркорозміру АПВ1 2,5 із домішками титану до основного матеріалу струмовідної жили та без домішок при струмі навантаження 14 А (значно менше допустимого струму) мають приблизно однаковий вигляд, близький до лінійної залежності;

– графіки залежностей температури нагріву проводу маркорозміру АПВ1 2,5 із домішками титану до основного матеріалу струмовідної жили та без домішок при струмах навантаження 24 А та 34 А (допустимий струм та вище) мають також приблизно однаковий вигляд, але вже нелінійної залежності;

– при нагріві проводу маркорозміру АПВ1 2,5 з алюмінієвою жилою з домішкою титану у матеріалі жили об'ємом 0,05 % протягом 100 с температура досягає 33°С; 57°С; 89°Сдля струмів навантаження I=14; 24; 34 А; за 200 с – до значень температури 45°С; 87°С; більш 100°С; у свою чергу, при нагріві аналогічного проводу з домішкою титану у матеріалі жили об'ємом 0,1 % протягом 100 с температура досягає 34°С; 58°С; 90°Сдля струмів навантаження I=14; 24; 34 А; за 200 с – до значень температури 47°С; 90°С; більш 100°С.

Список використаних джерел

1. Kulakov O., Kustov M., Katunin A., Roianov O. Investigation of the Impact Properties of the Material of the Isolation on the Parameters of the Loaded Cable Lines. Key Engineering Materials. 2023. Vol. 954. P. 125-133.
2. Катунін А.М., Кулаков О.В., Рудаков С.В., Панасенко С.В. Оцінка впливу струму навантаження на температуру нагрівання кабельних виробів у процесі експлуатації. International Scientific Journal «GrailofScience». 2023. № 24. С. 210-215.
3. Kishkin S.T. Metallovedenie aljuminievyh splavov [Aluminumalloys Metallurgical]. Moscow, NaukaPubl., 1985, 342 p.
4. Правила улаштування електроустановок. Київ: Міненгерговугілля України, 2017. 617 с.

УДК 681.5.015

Кисіль Г.А., Дядюн С.В.

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ІНТЕРАКТИВНОГО ПЕРЕКЛАДУ ТЕКСТІВ ДЛЯ МОВ, ЩО ВИКОРИСТОВУЮТЬ ІЄРОГЛІФИ

У сучасному світі, де знання іноземних мов відкриває нові можливості, вивчення нових мов стає все більш необхідним. Традиційні методи навчання, такі як підручники та заняття з викладачем, можуть бути не достатніми для ефективного засвоєння мови та вимагати багато ресурсів (гроші, час, тощо). Окрім того, деякі мови можуть суттєво

відрізнятися від рідної мови людини, що додатково ускладнює процес. Тому виникає потреба у сучасних інструментах, які полегшують процес навчання та роблять його більш інтерактивним.

Мобільні застосунки для вивчення мов стають все більш популярними завдяки своїй зручності та доступності. Вони дозволяють користувачам вивчати мову у зручний для них час, інтегруючи навчання у повсякденне життя. А також пропонують різні підходи і методики для навчання.

Аналіз потреб та функціональні можливості. Розробка цього застосунку розпочалася з аналізу потреб цільової аудиторії. При вивченні мов, які використовують кандзі, люди, які до цього не стикалися з такими мовами, натрапляють на проблему: читати та писати набагато важче, ніж говорити та сприймати інформацію на слух. Це пов'язано з тим, що дана писемність вимагає від людини великого обсягу знань та можливості впізнавати тисячі символів, кожен з яких може читатись декількома способами у різних словах. Для нашого застосунку на даному етапі реалізовано тільки японську мову, але зберігається достатня гнучкість архітектури для додавання інших мов пізніше.

Основні функції, які були визначені як необхідні для користувачів:

– розбиття японського тексту на окремі слова для полегшення читання;

– можливість ручного та автоматичного перекладу та транскрипції хіраганою для незнайомих слів;

– додавання слів до списку для вивчення та підбір текстів, де ці слова зустрічаються, для кращого засвоєння лексики;

– персональний словник користувача з набором вправ для запам'ятовування слів;

– впізнавання знайомих слів у текстах, запропонованих застосунком.

Далі відбувався пошук вже готових аналогів. Після первинного аналізу стало зрозуміло, що аналогічних застосунків досить мало, і більша частина з них мають інший фокус. Так, найближчим аналогом був Hiragana Times, але на відміну від наших вимог, він не має функціоналу, який допомагав би в запам'ятовуванні та вивченні слів.

Також нещодавно (літо 2024) з'явився новий аналог Yomu Yomu, який за півроку на ринку досяг показників у 50-100 тисяч скачувань в Play Market, що доводить актуальність даної роботи. Але на відміну від даного застосунку, цей ніяк не пов'язує процес розбору текстів та вивчення слів.

Методи та технології розробки.

1. **Фронтенд та інтерфейс**. Для створення кросплатформеного застосунку було обрано фреймворк Flutter. Це дозволяє забезпечити високу продуктивність та нативний вигляд на різних платформах. Менеджмент стану реалізовано за допомогою Cubit, що є частиною пакету Bloc, забезпечуючи простий та інтуїтивно зрозумілий підхід до управління станом у Flutter-застосунках.

2. **Бекенд та логіка**. Для серверної частини застосунку використовується Firebase, що забезпечує масштабованість та надійність. Firebase надає такі сервіси, як аутентифікація, база даних та аналітика, що дозволяє швидко та ефективно реалізувати необхідний функціонал.

3. **Архітектура**. У розробці застосунку використано підхід Clean Architecture, який сприяє розділенню відповідальностей та забезпечує легкість у підтримці та тестуванні коду. Це дозволяє мінімізувати витрати на підтримку та прискорити рефакторинг додатку в майбутньому.

4. **Безпека**. Забезпечення безпеки даних користувачів є пріоритетом. Firebase надає вбудовані засоби для захисту даних, а також можливість використання SSL-шифрування для захисту даних під час передачі між клієнтом та сервером.

5. **Розгортання та масштабування**. Використання Firebase спрощує процес розгортання та масштабування застосунку, дозволяючи легко адаптуватися до зростання кількості користувачів та забезпечувати стабільну роботу.

УДК 371.315.7:004

Кізло Л.М., Андреєва Л.М., Луньков А.В., Матала І.В.

ОСОБЛИВОСТІ ФОРМУВАННЯ ОСОБИСТОЇ І КОРПОРАТИВНОЇ ОБІЗНАНОСТІ ПЕРСОНАЛУ ЩОДО ЗАХИСТУ КІБЕРПРОСТОРУ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Сучасне цивілізоване суспільство характеризується цифровізацією відносин з виходом людства у кіберпростір та проникненням віртуального світу до всіх сфер життєдіяльності. У теперішній час інформаційні технології є невід'ємною складовою майже всіх сфер і галузей сучасного суспільства, а світові тенденції поширення кіберзлочинності та збільшення потужності і кількості кібератак підносить питання щодо захисту кіберпростору держав до категорії основних. Загрози порушення інтересів в кіберпросторі людей, самої держави і людства, в цілому, перетворились із потенційних та гіпотетичних на цілком реальні. Тож протистояння їх поширенню стало пріоритетним завданням для урядів та міжнародної спільноти на національному рівні.

Яскравим прикладом впливу надзвичайно потужної агресії у кіберпросторі стала наша держави, яка напередодні, а особливо з початом російсько-української війни зазнала чисельних кібератак з боку росії на урядові установи, приватні організації та громадян. Напад російських хакерів на Україну розпочався буквально за кілька хвилин до повномасштабного вторгнення армії. За даними агентства Reuters, США, Великобританія та Європейський Союз офіційно звинуватили рф у великомасштабному кібернападі, який 24 лютого 2022 року, за годину до початку війни, зруйнував роботу супутникового Інтернет-сервісу Viasat. Це спричинило знищення десятків тисяч супутникових терміналів.

Від самого початку війни стало також відомо про величезну кількість кібератак на українські ресурси. Компанії, які є складовою критичної інфраструктури, особливо енергетичні, комунікаційні, медіа та фінансові також зазнали руйнівного впливу від кіберзлочинців, оскільки ці галузі, як правило, розглядаються ворогом як пріоритетні цілі для кібератак. Для підтвердження цього доцільно пригадати незграбну спробу атаки хакерського угруповування Strontium. Вони намагалися зосередити всі свої зусилля на отримані доступу до всіх комп'ютерних мереж в Україні, США та ЄС. Цими нищівними діями злочинці планували забезпечити підтримку фізичного вторгнення росії в Україну на тактичному рівні, викрасти та знешкодити всю конфіденційну інформацію. Російські кіберзлочинці, здійснюючи чисельні атаки на об'єкти критичної інфраструктури, державні установи та приватні компанії і до тепер намагаються зруйнувати оборонні можливості держави та збільшити напруженість в сфері міжнародних відносин та кіберсередовищі.

В умовах воєнного стану кіберзлочинність стала глобальною загрозою для Збройних Сил (ЗС) України. Постійно під прицілом кіберзлочинців знаходяться об'єкти критичної інфраструктури. Приміром, відомий український провайдер Укртелеком потрапив під потужну атаку 28 березня 2022 року, під час дії якої зловмисники намагалися зламати та проаналізувати як влаштована ІТ-інфраструктура. В їхні плани входили наміри вивести з ладу Укртелекому та обвалити роботу різних сервісів. Також вони намагалися отримати контроль над базою персональних даних, програмним забезпеченням мереж та функціонуванням обладнання даної компанії.

Проте, це приклади лише масованих атак, про атаки менших масштабів та окремі випадки персональних зламів просто не завжди інформують суспільство, а як показують останні події, війна в інформаційному просторі завдає не меншої шкоди,

аніж війна на полі бою. І це без жодних перебільшень. Кібератаки завдають чималих проблем нашій державі, які мають парадоксальні наслідки, саме тому безпека України суттєво залежить від належного рівня кібербезпеки – як особистої, так і корпоративної.

Здебільшого сучасні заходи із забезпечення кібербезпеки обумовлюються технологічними особливостями та можливостями сучасного кіберпростору, охоплюють технічні питання захисту інформаційних ресурсів та захисту іміджевих позицій, як організації, в цілому, так і її співробітників.

Утім, найбільш вразливим об'єктом у системі забезпечення безпеки все ж вважається людина, а ступінь її вразливості залежить від багатьох факторів: рівня усвідомлення (сприйняття) можливих загроз та їх наслідків; обізнаності і досвіду щодо застосування засобів і методів захисту; індивідуальних психологічних особливостей, світоглядних позицій та морально-етичних цінностей; психологічного клімату колективу; сімейних обставин та інших складових.

Не другорядним компонентом забезпечення кібербезпеки є також рівень «інформаційної культури», яка безпосередньо пов'язана з поняттям «культура кібербезпеки». Поняття культура кібербезпеки (стосовно захисту інформації) почало поширюватися у світі після прийняття у 2003 році Резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки». У звіті Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) 2017 року «Культура кібербезпеки організації» запропоновано таке визначення культури кібербезпеки: знання, переконання, уявлення, норми і цінності особистості стосовно до кібербезпеки та використанню колективних інформаційних технологій.

Отже культура кібербезпеки наукових установ – це компетентність та корпоративні цінності наукового співтовариства, пов'язані із забезпеченням особистої безпеки у кіберпросторі у відповідності із визначеною політикою кібербезпеки наукової установи.

Формування культури кібербезпеки організації (установи) має бути спрямоване на зміну мислення співробітників, сприйняття ризиків та спільної відповідальності щодо забезпечення корпоративної кібербезпеки, виконання заходів із забезпечення особистої кібербезпеки – як звички.

Концепція щодо забезпечення корпоративної кібербезпеки повинна бути орієнтована, перш за все, на попередження загроз витоку електронної інформації щодо результатів наукових досліджень, до їх офіційного опублікування та оформлення авторських прав, попередження випадків неправомірного звинувачення у порушенні авторських і суміжних прав та негативного впливу на іміджеві позиції наукового співтовариства.

Відповідно, у якості основних складових формування особистої культури кібербезпеки можна виділити навчання та мотивування співробітників наукової установи, а також – етичний контроль. Але попри все, основними принципами формування культури кібербезпеки наукової установи можна вважати – своєчасність, зрілість та доступність заходів із формування у співробітників корпоративних етичних норм безпекової поведінки в національному кіберпросторі.

Як позитивний приклад з набуття належного рівня кібербезпекової компетентності персоналу можна розглядати досвід організації процесу його формування в Національній академії сухопутних військ імені гетьмана Петра Сагайдачного. Для цього, як для курсантів так і для наукового та науково-педагогічного складу академії, регулярно проводяться навчання з основ формування особистої та корпоративної культури кібербезпеки і кібергігієни. Програмою занять передбачено і проводяться заходи (лекції, тренажі, інструктажі) для опанування технологіями кіберзахисту та здійснюється контроль (здаються іспити за тестовою методикою) з визначенням рівня засвоєння знань і формування професійної компетентності.

Потрібно завжди пам’ятати про безпеку системи, яка залежить конкретно та абсолютно точно від кожного працівника. Хакери здатні напасти на компанію або ж установу і через робітників різних фірм та установ, викравши їхні дані. Таким способом, у квітні 2022 року, скористались кіберзлочинці – було розповсюджено електронні листи, що мали назву «Військові злочинці РФ.htm», які, уразі їх відкриття, відкривали віддалений доступ до комп'ютерів жертв. В результаті, в особливій небезпеці опинились військові, а також всі державні діячі. За оцінками ІТ-фахівців, за цими інцидентами стоять досвідчені російські військові.

Отже, пам’ятаючи про це, а також про те що інформаційні технології у сучасному світі розвиваються у т ч. і кіберзлочинність, всі категорії людей мають обов’язково звикнути дотримуватись правил кібергігієни та прийняти її за норму повсякденного життя, щоб не боротися з важкими наслідками в разі кібератак.

Проте, доцільно пам’ятати що всі заходи потрібно організовувати з врахуванням розвитку особистості кожного співробітника, пропонувати індивідуальні «вмотиватори» для підвищення усвідомлення про важливість і відповідальність за рівень особистої інформаційної культури і кібергігієни для забезпечення спільної національної кібербезпеки.

Підсумовуючи, зазначимо, що формування культури корпоративної кібербезпеки суб’єктів наукової та науково-технічної діяльності відноситься до завдань системи управління персоналом, виконання яких доцільно спрямовувати на посилення заходів забезпечення особистої безпеки в питаннях захисту інформації з обмеженим доступом, авторських і спільних прав, з метою упередження негативного впливу на іміджеві позиції наукового співтовариства.

З позиції соціального партнерства доцільно звернути увагу на заходи інформування про шкідливість та руйнівні можливості кібератак та способів щодо їх упередження через оптимізацію процесу навчання та посилення мотивації співробітників до дотримання норм корпоративної культури кібербезпеки.

З технічної – це забезпечення співробітників засобами технічного, програмного і криптографічного захисту інформації, надання необхідних послуг (у тому числі, з моніторингу контенту кіберпростору), або, приміром, створення умов для використання електронного цифрового підпису.

З правової – надання своєчасної правової допомоги співробітникам у питаннях захисту авторських і суміжних прав, захисту інтелектуальної власності, ділової репутації кожного.

Але, попри все для створення безпекового кіберсередовища доцільно дотримуватися елементарних правил:

– використовувати засоби захисту особистої інформації, пам’ятаючи, що здоровий глузд – це найкращий захист; захищати локальні мережі підрозділу (відділу) використовуючи правильні паролі;

– використовувати багатофакторну ідентифікацію, яка додає захищеності завдяки персоналізованому способу для входу в систему.

Утім, цей перелік не є достатнім для повного захисту. Для створення надійної і кіберзахищеної інформаційно-комунікаційної системи потрібно здійснювати постійно і регулярно за наступним алгоритмом: моніторинг загроз, оцінку ризиків, планування захисту, аналіз кіберінцидентів та виправлення помилок.

Отже, для підвищення рівня кібербезпеки в Україні необхідно забезпечити належний захист державних установ та критичної інфраструктури, а також підвищувати рівень обізнаності громадян про кіберзагрози та опановувати дієві способи захисту від кібератак.

Кобзев Д. О., Суровицький С. В.

ПІДХОДИ ДО БАЛАНСУВАННЯ ПРОДУКТИВНОСТІ ТА ЗАХИЩЕНОСТІ У ВИСОКОНАВАНТАЖЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У сучасному світі інформаційні системи повинні обробляти великі обсяги даних у реальному часі, залишаючись при цьому захищеними. Високонавантажені системи (High-Load Systems) використовуються у фінансових транзакціях, хмарних сервісах, соціальних мережах та онлайн-платформах, де захист і продуктивність має ключове значення. Баланс між продуктивністю та безпекою є одним із значущих викликів при розробці та супроводі подібних систем.

Продуктивність визначається здатністю системи швидко та ефективно обробляти запити користувачів. Основними показниками продуктивності є пропускна здатність (Throughput) або кількість запитів, які система може обробити за одиницю часу; затримка (Latency) або час очікування відповіді на запит; масштабованість (Scalability) або здатність системи збільшувати продуктивність при збільшенні навантаження.

Захищеність інформаційних систем базується на трьох основних постулатах: конфіденційність або захист від доступу сторонніх осіб; цілісність або запобігання змінам/знищенню даних; доступність або забезпечення безперебійного функціонування сервісів навіть під час атак [1].

Теоретично, застосовуючи всі найкращі практики, ми отримуємо високопродуктивну і максимально захищену систему. На практиці і перше, і друге потребує додаткових ресурсів системи. Наприклад, шифрування трафіку (TLS/SSL) підвищує захищеність, але додає затримки через необхідність виконання шифрування та розшифрування. Так само, фаєрволи, системи виявлення атак (IDS/IPS) та антивірусний захист, використовуючи додаткові ресурси, можуть спричиняти сповільнення обробки запитів.

З іншого боку, надмірне спрощення безпеки заради швидкості створює вразливості, що можуть призвести до зламів та витоків даних.

Беручі до уваги усе вищесказане, необхідно шукати і запроваджувати у щоденній роботі методи оптимального балансування продуктивності та захисту. З найбільш ефективних рішень можна вказати наступні:

– використання кешування, що дозволяє зменшити навантаження на сервери та пришвидшити відповіді. За допомогою CDN (Content Delivery Network) можливо зменшити затримку за рахунок розподілу контенту по різних серверах. Ще один варіант використовувати для зберігання частих запитів у пам'яті Memcached, Redis;

– використання сучасних алгоритмів шифрування, таких як AES-NI, що працюють швидше на апаратному рівні;

– використання для виявлення атак систем SIEM (Security Information and Event Management), які аналізують поведінку користувачів та можуть блокувати підозрілі дії без значного впливу на продуктивність [2].

Комплексний підхід у виборі методів оптимального балансу продуктивності та захисту дозволяє створити ефективну та безпечну систему, здатну працювати в сучасних умовах високих навантажень та загроз.

Список використаних джерел

1. Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition. – Indianapolis: Wiley, 2020. – 1232p.
2. Patrick Debois, John Willis, Jez Humble, Gene Kim, John W. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations. 2nd Edition – Portland: IT Revolution Press, 2021. – 480p.

Козлов Ю.В., Новикова О.О.

ВИРІШЕННЯ ЗАВДАНЬ ПЕДАГОГІЧНОЇ КВАЛІМЕТРІЇ МЕТОДАМИ НЕЧІТКОЇ МАТЕМАТИКИ

У статті [1] наведено різні варіанти формалізованого опису методами нечіткої математики шкал педагогічної кваліметрії, зокрема, удосконаленої чотирибальної шкали (УЧШ). Її характерною особливістю є використання відомого з метрології «методу ноніуса», який дозволяє збільшити число градацій у межах однієї поділки шкали і підвищити розрізнювальну здатність при поданні даних оцінювання результатів навчання суб'єкта навчання (СН). Залишення двох цифр після коми, що відповідає ноніусу 1/100, дозволяє використовувати оцінки типу 2+ або 4–, тобто 2,33 і 3,66 в УЧШ. При цьому абсолютна похибка запису не перевищить ±0,010.

Зауважимо, що опис відповідає прийнятому у нечіткій математиці набору

$$<\beta, T, X, G, M>, \quad (1)$$

де β – найменування змінної; T – множина термів (значень ЛЗ), тобто найменувань нечітких змінних, які задають семантику термів і використовуються для формалізації; деяка універсальна множина X, наприклад, послідовність чисел; G – синтаксичне правило прийняття рішення щодо відповідності терму із множини Т одній зі змінних множини X; M – множина функцій належності $\mu(x)$ термів ЛЗ, тобто набір семантичних правил, що ставлять у відповідність кожному терму деяку змінну на універсальній множині X.

Відмітимо, що при використанні чотирибальної шкали порядку правила нечіткого виводу (критерії прийняття рішень) подають вербальною конструкцією: «твердження (запитання) типу «Збігається чи ні відповідь суб'єкта навчання з еталонною?» – судження (відповіді)»: Так (відмінно – 5 балів); Скоріше так, чим ні (добре – 4); Скоріше ні, чим так (задовільно – 3); Ні (незадовільно – 2), тобто описані значення. G та X із набору (1).

Наявність формалізованого опису УЧШ забезпечує можливість використання процедури фазифікації і отримати результуючу функцію належності (РФН) за одним або кількома правилами із бази продукційних правил системи нечіткого виводу.

Процедура дефазифікації, аналогічна знаходженню характеристик положення (математичного сподівання, моди, медіани) випадкових величин в теорії ймовірності, дозволяє отримати інтегральні показники навченості суб'єктів навчання. Результат дефазифікації – чітке числове значення РФН – за відсутністю явного максимуму визначають одним з таких методів: центру тяжіння (ЦТ), лівого модального значення (ЛМЗ), правого модального значення (ПМЗ), центру площі ЦП), середнього максимуму (СМ).

Декілька зауважень:

– припущення щодо неперервності отриманих числових значень у просторі невеликої розмірності (1-3) з максимально можливим збереженням відстаней між точками для великих обсягів вибірок дозволяє як характеристику положення прийняти медіану;

– використання середніх арифметичних значень (САЗ) оцінок, отриманих методами нечіткої математики, викликає нарікання деяких категорій спеціалістів, хоча для вузьких шкал це не суперечить теорії і доказано результатами аналітичного моделювання [2] і розрахунками (табл. 1 і рис. 1, де б – графічна подоба наведеної на рис.1-а РФН у відповідному масштабі).

Таблиця 1 – Результати дефазифікації РФН аналітичної моделі

метод	ЦТ	ЛМЗ	ПМЗ	ЦП	СМ
Y	3,45	2,00	5,00	3,30	3,88

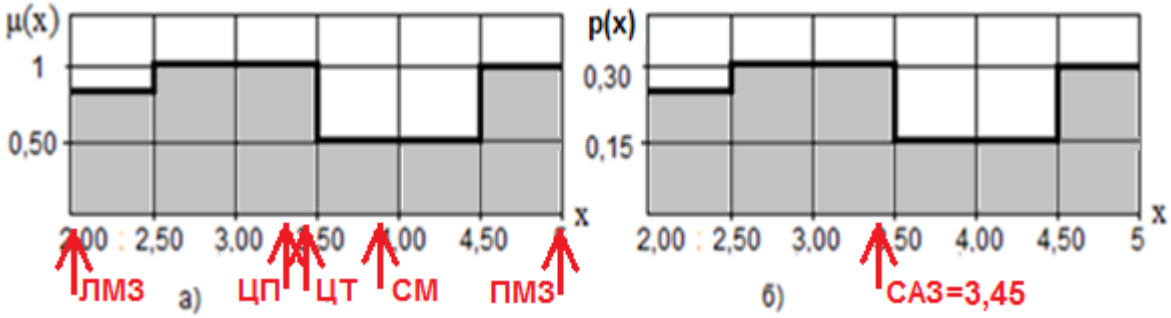


Рисунок 1 – Результуюча функція належності (приклад 1) та її графічна подоба

У табл. 2 подані результати дефазифікації взятих навмання оцінок навченості одного із СН за семестр з навчальної дисципліни кафедри. На рис. 2-а наведена РФН, побудована за цими оцінками, а на рис. 2-б її графічна подоба у відповідному масштабі.

Таблиця 2 – Результати дефазифікації оцінок навченості суб'єкта навчання

метод	ЦТ	ЛМЗ	ПМЗ	ЦП	СМ
Y	3,87	2,00	5,00	3,86	3,75

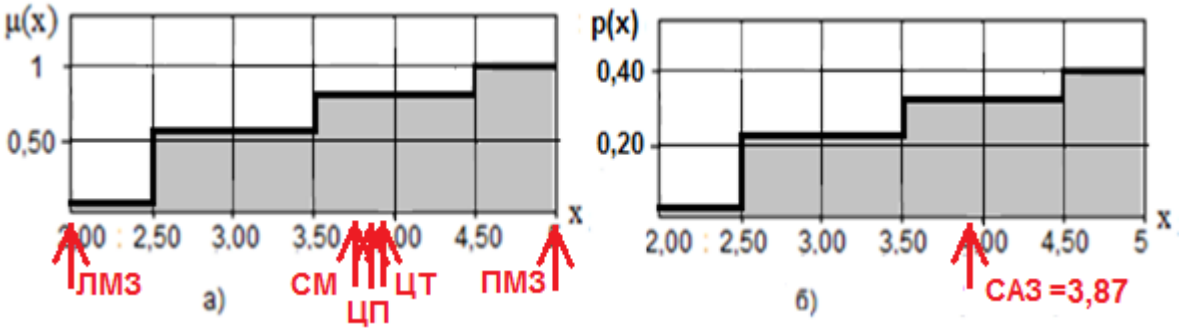


Рисунок 2 – Результуюча функція належності (приклад 2) та її графічна подоба

Порівняння наведених результатів показує, що числові значення центру тяжіння і середнього арифметичного в обох прикладах (і загалом) практично співпадають. Це підтверджує правомірність використання САЗ в якості числового значення РФН.

У цілому, методика вирішення завдань педагогічної кваліметрії методами нечіткої математики можна подати послідовністю таких кроків:

– отримання оцінок рівня навченості (знань, умінь і навичок) СН із використанням гібридної моделі подання оцінних функцій викладача [2] та вираження їх в удосконаленій чотирибальній шкалі;

– розрахунок середніх арифметичних значень оцінок як інтегральних показників навченості (ІПН);

– вираження ІПН у вигляді, прийнятному для побудови рейтингового списку в УЧШ, стобальній або відповідній їй ECTS шкалі.

Список використаних джерел

1. Козлов В.Є. Опис шкал педагогічної кваліметрії методами нечіткої математики/ В.Є. Козлов, О.О. Новикова// Зб. наук. праць Академії внутр. військ МВС України. 2013. Вип.1 (21). С. 25-28. ISSN 2218-1555.
2. Козлов Ю.В. Метод оцінювання рівня навченості суб'єкта навчання/ Ю.В. Козлов, О.В. Дегтярьов, Л.В. Василющенко, В.М. Унгер// Метрологія та прилади. 2024. №1. С. 59-64. ISSN 2663-9564 (online). doi: https://doi.org/10.30837/2663-9564.2024.1.11

УДК 620.1, 621.3

Коломійцев О.В., Комаров В.О., Пустоваров В.В., Іохов О.Ю.

МЕТОД ПРОВЕДЕННЯ ОПТИКО-ВІЗУАЛЬНОГО КОНТРОЛЮ ВИСОКОРОЗТАШОВАНИХ КОНСТРУКЦІЙ ПЛАНЕРІВ БОЙОВИХ ЛІТАЛЬНИХ АПАРАТІВ

Висока ефективність застосування за призначенням бойових літальних апаратів (ЛА) забезпечується:

– з одного боку (внутрішніми факторами) – якісною роботою у штатному режимі автоматизованих систем управління і регулювання, цифрових обчислювальних машин та різного роду елементів, вузлів, блоків, виробів тощо;

– з іншого боку (зовнішніми факторами) – якісним дотриманням цілісності конструктивних елементів ЛА для льотної придатності.

Не виявлені значні та критичні дефекти можуть спричинити руйнування авіаційної конструкції бойових ЛА під час експлуатації. Для підтримки їх у справному стані проводиться дефектоскопічний контроль конструктивних елементів [1-3]. Під час такого контролю здійснюється своєчасне виявлення тріщин, корозії, ушкодження, включаючи бойові, а також порушення нормального становища (руйнування конструкцій). Такий контроль необхідний для своєчасного вжиття заходів щодо усунення виявлених дефектів.

Дефектоскопічний контроль на різних етапах експлуатації бойових ЛА забезпечує, як основний напрямок діагностування, стеження за розвитком у процесі експлуатації допустимих пошкоджень матеріалів, так і, на цій основі, прогнозування працездатності (виконання бойових завдань) бойових ЛА у цілому.

У завдання технічного обслуговування і ремонту бойових ЛА входить як обслуговування, так і відновлення не тільки відмовленого обладнання, а й виявлених деградаційних процесів (втоми і корозії) та пошкоджень, включаючи бойові. Проблема втомного ресурсу ЛА – це напрацювання під час експлуатації до граничного стану, яке визначається критеріями втомної міцності. Вона пов'язана з накопиченням втомних ушкоджень та руйнуванням авіаційних конструкцій від втомних тріщин.

До найпоширеніших форм пошкоджень можливо віднести усі види тріщин (зламів), що виникають внаслідок перевищення граничної міцності елемента конструкції бойового ЛА, а також бойові. Пошкодження зумовлені, в основному, характером механічних та теплових навантажень (статичних, динамічних та їх комбінацій).

Враховуючи той факт, що сучасний розвиток інформаційних технологій за останні роки сприяв величезним змінам як у суспільстві, в загалі, так і у сфері застосування безпілотних літальних апаратів (БпЛА, дрони), можливо стверджувати, що широкий спектр функціональних можливостей БпЛА з кожним днем розширює їх коло застосування як у науковій і цивільній, так і у військовій сферах [4-7].

БпЛА є популярними інструментами для отримання просторових даних для різного роду аналізів, 3-D моделювання, моніторингу за різними напрямками, розвідки тощо. До основних переваг застосування БпЛА можливо віднести наступні: суттєву економічність, високу точність, збереження людського ресурсу, можливість роботи у важкодоступних місцях тощо. Завдяки тому, що БпЛА оснащені найсучаснішими камерами з високими технічними характеристиками (роздільною здатністю, широкими кутами огляду тощо) та засобами автоматизації з елементами штучного інтелекту – вони активно застосовуються для ведення як різного роду моніторингу у цивільній сфері, так і розвідки, прихованого слідкування, знищення повітряних і наземних цілей тощо – у військовій сфері.

Таким чином, розробка пропозицій щодо застосування БпЛА для проведення оптико-візуального контролю високорозташованих конструкцій планера ЛА є актуальнім науко-технічним завданням.

У доповіді проведено аналіз відомих сучасних БпЛА, що використовують комп'ютерний зір та штучний інтелект. Доведено їх технічні характеристики, переваги та недоліки.

Акцентовано увагу на дефекти, які можуть спричинити руйнування авіаційної конструкції бойових ЛА під час експлуатації. Розглянуто основні методи огляду високорозташованих конструкцій планера бойового ЛА. Доведено переваги та недоліки оптико-візуального методу діагностичного контролю бойового ЛА.

Запропоновано метод дефектоскопії зовнішніх поверхонь планера бойового ЛА за допомогою БпЛА мультикоптерного типу, що обладнані сучасними відеокамерами (засобами візуального контролю). Розкрито переваги, сутність та роботу методу.

Акцентовано увагу на те, що завдяки розміщення відеокамер (засобів візуального огляду) на БпЛА у трьох напрямах (вверх, униз та у бік) забезпечується можливість огляду трьохмірно розміщених конструкції планера бойового ЛА без зміни горизонтального положення корпусу БпЛА. Застосування на БпЛА системи підсвічування (електричного джерела світла – освітлювача, що виконаний у вигляді окремого блоку та розміщений біля кожної з відеокамер таким чином, щоб їх оптичні осі знаходяться практично по одній осі), дозволяє досягти можливості огляду конструкції планера бойового ЛА у темні години доби на відкритій ділянці місцевості.

Таким чином, запропонований метод дозволить оперативно та з мінімальною трудомісткістю отримати повну достовірну інформацію про технічний стан конструкції планера бойового ЛА, що діагностується.

Список використаних джерел

1. Порівняння можливостей методів неруйнівного контролю для виявлення пошкоджень у силових елементах консольно закріплених конструкцій літака / О.В. Коломійцев та ін. Collection of scientific papers «ΛΌГОΣ». 2024. С. 121-129. URL: https://doi.org/10.36074/logos-19.07.2024.
2. Удосконалена методика оперативного визначення технічного стану авіаційної техніки, що має ушкодження, включаючи бойові. / О.В. Коломійцев та ін. Grail of Science. 2024. № 42. С. 277-290. URL: https://doi.org/10.36074/grail-of-science.02.08.2024.
3. Аналіз напрямків розвитку військової техносфери країн НАТО / О. Коломійцев та ін. InterConf. 2023. № 37(171). С. 379–397. URL: https://doi.org/10.51582/interconf.19-20.09.2023.033 (дата звернення: 03.03.2025).
4. Особливості застосування безпілотних літальних апаратів коптерного типу / О. Коломійцев та ін. Collection of Scientific Papers «ΛΌГОΣ». 2024. С. 188–198. URL: https://doi.org/10.36074/logos-16.08.2024.038 (дата звернення: 03.03.2025).
5. Особливості застосування нейронної мережі у системі керування групою безпілотних літальних апаратів / О. Коломійцев та ін. Grail of Science. 2024. № 43. С. 322–334. URL: https://doi.org/10.36074/grail-of-science.06.09.2024.042.
6. Designing and evaluating dl-model for vulnerability detection in smart contracts / O. Shmatko and et. Advanced Information Systems. 2024. № 7(4). С. 41–51. URL: https://doi.org/10.20998/2522-9052.2023.4.05.
7. Пропозиції щодо розробки програмного забезпечення для виявлення людей на цифрових аерофотознімках та потоковому відео комп'ютерного зору безпілотного літального апарату / О.В. Коломійцев та ін. Grail of Science. 2024. № 45. С. 411-420. URL: https://doi.org/10.36074/grail-of-science.01.11.2024.

УДК 623.746

Коломійцев О.В., Рудаков І.С., Бесова А.О., Бордунова К.І.

ПІДВИЩЕННЯ БЕЗПЕКИ ПОЛЬОТІВ ГРУПИ ОДНОТИПНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПІД ЧАС МОНІТОРИНГУ НА ОСНОВНІ ТЕХНОЛОГІЇ МАШИННОГО НАВЧАННЯ

Під час проведення моніторингу автономними безпілотними літальними апаратами (БпЛА) вирішальне значення має система надійного уникнення різних типів об’єктів, яка використовує різні типи датчиків. Одним із таких датчиків є комп’ютерний зір, який є основою системи бачення та одним із варіантів уникнення перешкод шляхом використання даних зображень як джерела точної інформації.

Підвищення безпеки польотів групи однотипних БпЛА під час моніторингу може бути досягнуто за рахунок [1, 2]:

– вдосконалення існуючих та впровадження ряду нових методів і технологій;

– покращення алгоритмів координації (використання розподілених алгоритмів, які дозволяють групи однотипних БпЛА приймати самостійно рішення на основі часткової інформації) та алгоритмів групового (ройового) інтелекту для підвищення ефективності та гнучкості (успішного виконання поставлених завдань);

– оптимізація ресурсів (оптимізація маршруту польоту, управління живленням тощо), розподіл завдань між однотипними БпЛА з урахуванням їх ресурсів та можливостей тощо.

Сучасні технології штучного інтелекту відкривають нові можливості для розробки та використання групи однотипних БпЛА. До основного складу категорій штучного інтелекту можливо віднести наступні: машинне навчання, нейронні мережі та алгоритми оптимізації.

Оптимізаційні алгоритми можливо застосовувати для розв'язання багатьох завдань, які пов'язані із поліпшенням функціональності та ефективності застосування групи однотипних БпЛА під час моніторингу у міський забудові.

Таким чином, підвищення безпеки польотів групи однотипних БпЛА під час моніторингу на основні технології машинного навчання є актуальним науково-технічним завданням.

Використання технології штучного інтелекту (методів машинного та глибокого навчання), дозволяє аналізувати отримані дані у реальному масштабі часу та приймати більш точні рішення, а також розпізнавати складні паттерни та прогнозувати поведінку групи однотипних БпЛА. Застосування адаптивних методів (самонавчання та динамічне планування), дозволяють БпЛА самостійно навчатися на основі отриманого досвіду уникнення зіткнень (подолання перешкод тощо) та швидко адаптуватися до нових ситуацій. За рахунок однотипності БпЛА будуть спроможні передавати накопичений досвід один-одному, що прискорить процес самонавчання.

У доповіді проведено аналіз відомих сучасних БпЛА, що використовують штучний інтелект як у цивільній, так і військовій сферах. Доведено їх технічні і тактико-технічні характеристики, переваги та недоліки.

Розглянуто основні підходи до технології машинного навчання: навчання з учителем, навчання без учителя та навчання з підкріпленням. Відмічено, що алгоритми машинного навчання забезпечують частково або повністю автоматизовані методи аналізу даних.

Проведено аналіз основних методів регресії: лінійної, логістичної, поліноміальної, гребеневої, Least Absolute Shrinkage and Selection Operator та ElasticNet. Відмічено, що ансамблеве навчання розподіляє процес прийняття рішень для запобігання зміщенню.

Зазначено, що використання технології штучного інтелекту для управління групою

однотипних БпЛА, надає можливості для автоматизації процесів прийняття рішень, підвищення точності та швидкості реагування, а також підвищення загальної ефективності моніторингу, у тому числі міської забудови.

Використання алгоритмів машинного навчання дозволить здійснити аналіз ситуацій у міський забудові, ідентифікацію об'єктів, планування маршрутів польоту та взаємодію між БпЛА. Тобто, оптимізувати дії групи однотипних БпЛА, забезпечити їх координацію дій та підвищити загальну ефективність виконання завдань моніторингу.

До основних напрямків застосування машинного навчання для групи однотипних БпЛА можливо виділити наступні:

– забезпечення безпеки повітряного простору, що є критичним для інтеграції групи однотипних БпЛА у загальну авіаційну систему;

– аналіз продуктивності та оптимізація, які включають прогнозування трафіку, підвищення енергоефективності, удосконалення комунікаційних технологій, зменшення затримок, впровадження автоматизації, оптимальне розгортання, планування маршрутів та прогнозування їх змін;

– виявлення та вирішення конфліктів, які виникають під час експлуатації групи однотипних БпЛА шляхом розробки алгоритмів уникнення зіткнень та ефективного управління повітряним трафіком.

На даний час проблематику безпечної та ефективної інтеграції БпЛА у загальний повітряний простір вирішує концепція U-space, яка забезпечує цифрові послуги для контролю та координації польотів БпЛА відповідно до існуючих норм та регуляторних вимог. Ключовим аспектом U-space є точне планування польотів БпЛА, яке здійснюється у чотиривимірному просторі, до складу якого входять: висота, широта, довгота та час на перебування БпЛА у визначеній точці. Однак, такий план може змінюватися через зовнішні фактори: обмеження повітряного простору, наявність інших літальних апаратів або географічні обмеження. Тому, на допомогу приходять методи машинного навчання, які сприяють оптимізації польотів та підвищенню безпеки повітряного руху групи однотипних БпЛА.

Таким чином, інтеграція БПЛА у міський повітряний простір є складним завданням, яке вимагає ретельного планування та розробки регуляторних механізмів. Розроблено та представлено низку науково-практичних пропозицій щодо застосування технології машинного навчання для підвищення безпеки польотів групи однотипних БпЛА для проведення моніторингу.

На приклад, одним із наукових завдань є планування та прогнозування маршрутів БпЛА, що безпосередньо впливає на безпеку польотів групи БпЛА. Запропоновано використовувати еволюційні та хаотичні генетичні алгоритми, які дозволяють адаптувати маршрути БпЛА відповідно до динамічних умов. Однак, навіть з урахуванням передового планування, конфлікти у повітряному просторі можуть виникати. За умови, якщо траєкторії двох БпЛА перетинаються, необхідно застосовувати методи AI та ML для своєчасного виявлення та вирішення конфліктів, запобігаючи можливим зіткненням.

Список використаних джерел

1. Особливості застосування безпілотних літальних апаратів коптерного типу / О. Коломійцев та ін. Collection of Scientific Papers «ΛΌГОΣ». 2024. С. 188–198. URL: https://doi.org/10.36074/logos-16.08.2024.038 (дата звернення: 03.03.2025).
2. Особливості застосування нейронної мережі у системі керування групою безпілотних літальних апаратів / О. Коломійцев та ін. Grail of Science. 2024. № 43. С. 322–334. URL: https://doi.org/10.36074/grail-of-science.06.09.2024.042.

Коляденко Ю.Ю., Бабаєва М.О.

ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ ВІДДАЛЕНОГО ВІДЕОСПОСТЕРЕЖЕННЯ

Сучасні системи відеоспостереження – це самостійна галузь охоронних технологій з власними стандартами. Вони забезпечують комплексний захист об'єктів: від збереження майна та контролю доступу до оцінки роботи персоналу. Відеозаписи дозволяють відстежувати всі події на об'єкті та оперативно реагувати на нестандартні ситуації. Передача інформації від віддаленого відеоспостереження, особливо радіоканалами потребує відповідного забезпечення надійності. В реальних умовах прийом інформації завжди відбувається з помилками. Боротьба з виникаючими помилками ведеться на різних рівнях семирівневої моделі OSI (в основному на перших чотирьох). Для боротьби з виникаючими помилками відомо багато різних способів. Всі їх можна поділити на дві групи: не використовуючм зворотний зв'язок і використовуючи зворотний зв'язок. Найбільш поширені системи, які використовують вирішальний зворотній зв'язк з надлишковими кодами для виявлення помилок. В цьому випадку найчастіше використовуються циклічні коди.

Для підвищення завадостійкості системи передачі інформації віддаленого спостереження пропонується використати циклічний код в виявлення помилок. Для оцінки ймовірності помилки кодової комбінації використовуються параметри коду. До них відносяться: $n=m+k$ – довжина кодової комбінації; m – число інформаційних символів; k – число перевірних символів. Особливу важливість для характеристики коригувальних властивостей коду має мінімальна кодова відстань $d_{\min}$. Якщо код використовується тільки для виявлення помилок кратністю $t_в$, то необхідно і достатньо, щоб мінімальна кодова відстань дорівнювала:

$$d_{\min} \geq t_в + 1. \tag{1}$$

Довжина кодової комбінації n повинна бути вибрана таким чином, щоб забезпечити найбільшу пропускну здатність каналу зв'язку. Надмірність коригуючого коду є величина:

$$r = \frac{k}{n} = \frac{n-m}{n} = 1 - \frac{m}{n}. \tag{2}$$

Ця величина показує, яку частину загального числа символів кодової комбінації складають інформаційні символи. Якщо продуктивність джерела інформації дорівнює H'_t символів в секунду, то швидкість передачі інформації після кодування:

$$I' = H'_t \frac{n}{m}. \tag{3}$$

У реальних каналах зв'язку діють завади, що призводять до появи помилок в кодових комбінаціях. При виявленні помилки декодувальним пристроєм в системах з вирішальним зворотнім зв'язком проводиться перезапит групи кодових комбінацій. Під час перезапиту корисна інформація не передається, тому швидкість передачі інформації зменшується. В цьому випадку:

$$I' = H'_t \frac{m}{n}\left[1 - \frac{P_{\text{вп}}(M+1)}{P_{\text{пр}} + P_{\text{вп}}(M+1)}\right], \tag{4}$$

де $P_{вп}$ - ймовірність виявлення помилки декодером, $P_{\text{пр}}$ - ймовірність правильного прийому; M - ємність накопичувача передавача.

Еквівалентна ймовірність помилки прийому одиничного розряду при застосуванні завадостійкого кодування визначається за формулою:

$$P_e = 1-(1-p_{помkk})^{\frac{1}{m}}, \quad (5)$$

де $p_{помkk}$ - ймовірність помилкового декодування кодової комбінації:

$$p_{помkk} = 1-\sum_{i=0}^{t_в} C_n^i q^i (1-q)^{n-i},$$

q - ймовірність помилки, визначається каналом зв'язку.

В середовищі Matlab проведено аналіз швидкості передачі інформації I' та еквівалентної ймовірності помилки прийому одиничного розряду P_e при застосуванні завадостійкого кодування. Аналіз проведено за умови, що роздільна здатність об'єктиву $F_{об}$ =275 ліній/мм, максимальна частота сигналу $F_{\max}$ =1,36 МГц, продуктивність джерела $H'_t = 3{,}2198\cdot 10^7$ бит/с, відстань зв'язку L =200 км.

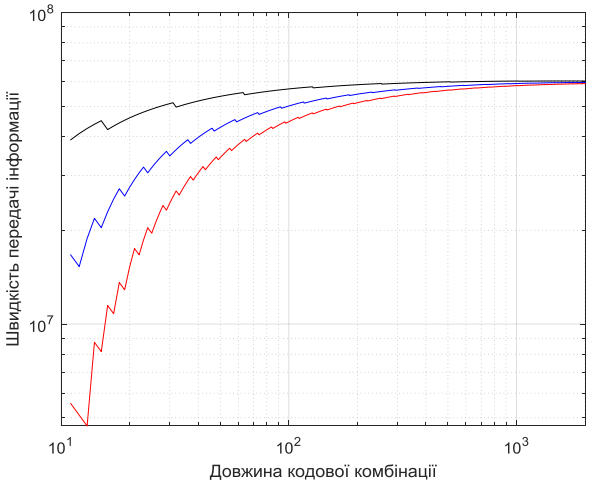


Рисунок 1 – Залежність швидкості передачі інформації від довжини кодової комбінації

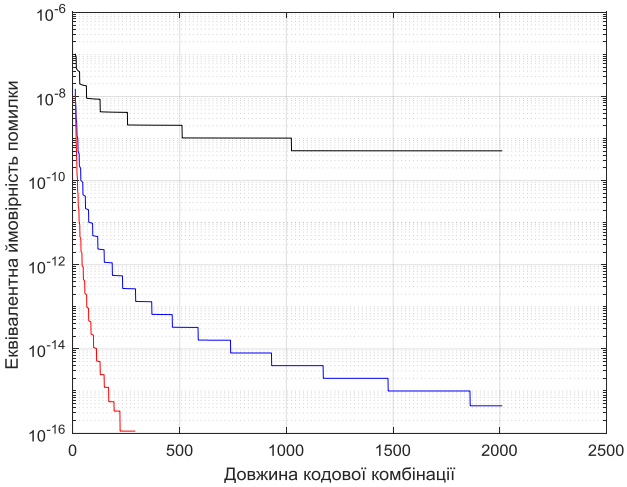


Рисунок 2 – Залежність еквівалентної ймовірності помилки від довжини кодової комбінації

На рис. 1 представлено залежності швидкості передачі інформації від довжини кодової комбінації при різних значеннях помилок, що виявляються. На рис. 2 представлено залежності еквівалентної ймовірності помилки від довжини кодової комбінації при різних значеннях помилок, що виявляються. Нижні криві на цих рисунках відповідають випадку кількості помилог, що виявляються $t_в$ =1, середні криві - $t_в$ =5, нижні криві $t_в$ =10. Аналіз показав, що зі збільшенням довжини кодової комбінації швидкість передачі інформації збільшується. При збільшенні кількості помилок, що виявляються швидкість передачі інформації також збільшується завдяки зменшенню перезапитів. Еквівалентна ймовірність помилки зменшується зі збільшенням довжини кодової комбінації та зі збільшенням кількості помилок, що виявляються кодом.

На основі отриманих даних можна зробити такі висновки:

1. Існує оптимальне значення довжини кодової комбінації та кількості виявлених помилок, яке забезпечує максимальну швидкість передачі інформації при заданій якості.

2. Збільшення швидкості передачі інформації зазвичай пов'язане зі зниженням надійності. Однак, використання ефективних кодів дозволяє досягти високої швидкості при збереженні низької ймовірності помилки.

Коляденко Ю.Ю., Бадєєв В.О.

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МЕРЕЖІ 5G

Технологія 5G продовжує активно розвиватися по всьому світу, стаючи доступною для користувачів у різних країнах. На жаль, в Україні мережі 5G наразі перебувають на стадії розробки і ще не доступні для користувачів. 5G забезпечує надшвидкісні з'єднання, низьку затримку та масове підключення пристроїв. Однак, разом з новими можливостями, виникають і нові загрози для інформаційної безпеки.

Розгортання мереж 5G супроводжується підвищеною увагою до захисту даних та інфраструктури. Збільшення кількості підключених пристроїв, складність мережевої архітектури та зростання обсягу переданих даних роблять 5G мережі привабливою мішенню для кіберзлочинців. Тому створення ефективної системи контролю та управління інформаційною безпекою мережі 5G є критично важливим завданням. Така система повинна забезпечити:

– конфіденційність: захист даних від несанкціонованого доступу;
– цілісність: гарантування, що дані не будуть змінені або знищені;
– доступність: забезпечення безперебійної роботи мережі та доступності послуг.

Актуальність теми. Розвиток технологій 5G створює нові можливості для економіки та суспільства, але одночасно посилює ризики для інформаційної безпеки. Тому розробка ефективних систем захисту є необхідною умовою для успішного впровадження 5G.

У роботі розглянуто можливість підвищення скритності сигналів за рахунок застосування таймерних сигнальних конструкцій (ТСК).

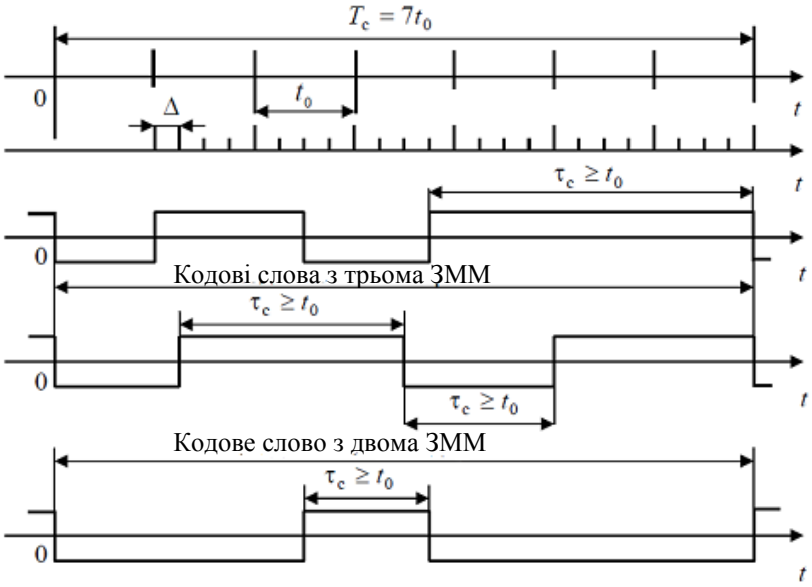


Рисунок 1 – Формування сигнального алфавиту бінарних ТСК на интервалі часу $T_c = 7t_0$ при базовому елементі Δ

Відомо, що індивідуальні двійкові канали мають базу B=1 та використовують надлишковий код. Ефективність використання двійкового каналу можна підвищити за рахунок таймерного методу формування сигнальних конструкцій на заданому інтервалі n - елементного надлишкового коду. Сигнальний алфавіт бінарних ТСК для кожного індивідуального каналу формується на інтервалі часу $T_c = nt_0$ (t_0 - величина, зворотна

смузі пропускання каналу ΔF) при базовому елементі Δ ($\Delta = \frac{t_0}{S}$, $S = 1,2,...,k$ - цілі числа). Приклад формування сигнального алфавиту бінарних ТСК на інтервале часу $T_c = 7t_0$ при базовом элементе Δ показано на рис. 1.

Кожен значущий момент модуляції (ЗММ) може займати на інтервалі формування ТСК позиції, розташовані на відстані $k\Delta \geq t_0$ один від одного по відношенню до попереднього, причому Δ визначається як мінімальна відстань між сусідніми положеннями одного ЗММ у різних конструкціях. Інформація про повідомлення, що переноситься ТСК, міститься в номері часової позиції, яку займає ЗММ. У кожній сигнальній конструкції сигнал з тривалістю Δ в канал не передається. Однак, тривалість елемента Δ враховується, коли на прийомі проводиться оцінка конструкції, що надійшла в порівнянні з усіма можливими реалізаціям. Кількісною мірою структурної скритності ТСК може слугувати ймовірність розкриття структури сигналу $p_{стр}$ за умови, що сигнал вже виявлено.

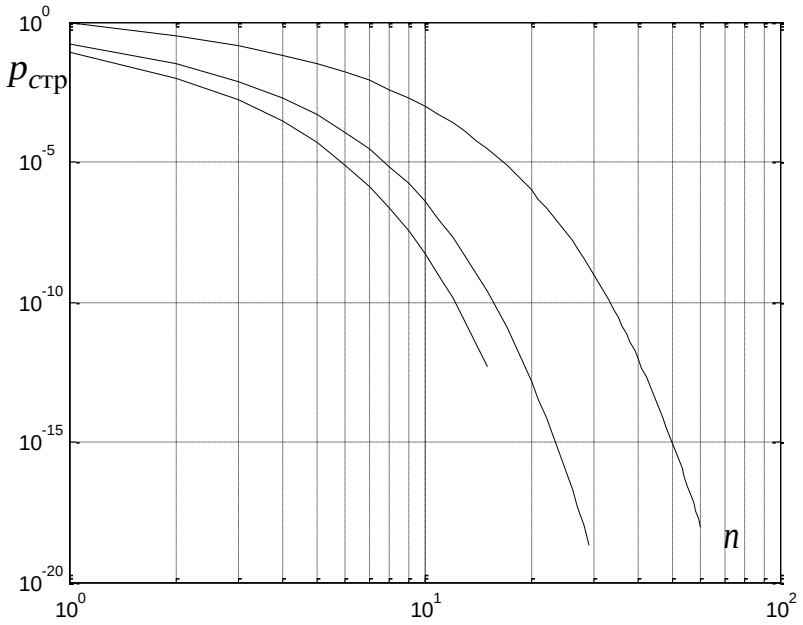


Рисунок 2 – Ймовірності роркриття структури ТСК в залежності від значень n при S =1, S =6, S =12 і i =1 … n .

За допомогою математичного моделювання визначено ймовірність розкриття структури ТСК залежно від значень n, S та i. На рис. 2 наведено графіки ймовірностей розкриття структури ТСК залежно від значень n при S =1 (верхня крива), S =6 (середня крива) та S =12 i =1 … n. Аналіз показав, що ймовірності розкриття структури сигналу $p_{стр}$ значно зменшуються зі зростанням інтервалу T_c формування ТСК. Таким чином, застосування ТСК дозволяє зменшити ймовірність розкриття структури сигналу $p_{стр}$ до значень 10^{-48}.

Результати проведеного дослідження свідчать про високий потенціал застосування ТСК для підвищення рівня інформаційної безпеки. Збільшення інтервалу формування ТСК дозволяє суттєво ускладнити процес аналізу структури сигналу для зловмисників,

що робить системи, які використовують ТСК, більш стійкими до різних видів атак. Отримані дані можуть бути використані при проектуванні та впровадженні систем захисту інформації в різних галузях, де висуваються високі вимоги до конфіденційності переданих даних.

УДК 623.1/.7: 621.396.931:007.5

Коркін О.Ю., Ковалішин С.С., Коркіна Н.О., Симоненкова І.В.

ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ КАНАЛУ УПРАВЛІННЯ НАЗЕМНОГО РОБОТИЗОВАНОГО КОМПЛЕКСУ В УМОВАХ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

В умовах активної фази російсько-української війни зростає необхідність у безпілотних наземних комплексах (БпНК) для зниження втрат особового складу та підвищення ефективності виконання бойових завдань. БпНК можуть використовуватися для вогневої підтримки, розвідки, постановки активних завад, логістичних операцій, евакуації поранених, вивезення пошкодженого озброєння, військової та спеціальної техніки з поля бою тощо [1, 2].

Сучасні бойові дії супроводжуються активним застосуванням засобів радіоелектронної боротьби (РЕБ), що ускладнює використання БпНК силами оборони України. Одним із варіантів забезпечення надійного каналу управління такими комплексами є комплексне використання адаптивних антенних решіток (ААР) у поєднанні з методом множинного доступу з прямим розширенням спектра (DS-CDMA, англ. Direct Sequence Code Division Multiple Access), мобільних самоорганізованих мереж (MANET, англ. Mobile Ad hoc Network) та технологій штучного інтелекту (ШІ). У специфічних завданнях, зокрема логістичних та розмінування, перспективним рішенням може бути використання оптоволоконного зв’язку. Сучасні системи РЕБ здатні здійснювати глушіння, перехоплення та спуфінг сигналів, що значно ускладнює управління БпНК. Найбільш вразливими є традиційні радіоканали, такі як LoRa (від Long Range), Wi-Fi (802.11 a/b/g/n/ac) на 2.4/5 ГГц, частина систем FHSS (англ. Frequency-Hopping Spread Spectrum) (де кожен крок перестрибування має вузьку смугу) тощо. Основними викликами є глушіння сигналів на критичних частотах, затримка та втрата пакетів у мережевій інфраструктурі, ризик кібератак та компрометації зв’язку.

Одним із перспективних підходів є використання ААР, які забезпечують не лише статичне, а й динамічне формування діаграми направленості сигналу, що значно підвищує стійкість до завад у складних умовах. Це дозволяє досягти селективного спрямування енергії у напрямку необхідних об'єктів, що суттєво зменшує негативний вплив навмисних завад. Адаптивне керування параметрами прийому дає змогу знижувати рівень шуму [3, 4], що, в свою чергу, покращує якість зв'язку та підвищує ефективність використання радіочастотного спектру. Крім того, можливість використання рознесення сигналів дозволяє уникати мультиплексних завад і створює умови для значного поліпшення якості зв'язку в умовах фізичних перешкод або радіозавад [6, 7].

Застосування ААР у поєднанні з іншими сучасними технологіями та методами забезпечує високу ефективність роботи в умовах високого рівня електромагнітних завад, дозволяючи протистояти засобам глушіння сигналів, що здійснюються системами РЕБ. Це дозволяє зберігати стабільний і високоякісний зв'язок навіть у найскладніших умовах на полі бою. Однак, незважаючи на численні переваги, основним недоліком цієї технології є висока вартість розробки та впровадження ААР,

що потребує значних фінансових та технологічних ресурсів. Це може обмежити їхнє широке застосування на тактичному рівні.

Тим не менше, попри високу вартість, переваги ААР у забезпеченні стійкості до завад і збереженні якості зв'язку в умовах активної РЕБ можуть виправдати вкладення, особливо коли мова йде про застосування на оперативному рівні, де кожен елемент зв'язку критичний для успіху операції. Інтеграція такої технології в систему управління БпНК може стати важливим кроком до забезпечення надійної та ефективної комунікації на полі бою.

Технологія DS-CDMA забезпечує високу стійкість до завад завдяки широкосмуговому передаванню сигналів, що ґрунтується на використанні псевдовипадкової розгортки. Така система дозволяє ефективно використовувати спектр частот та знижувати вплив шуму і завад завдяки розподілу сигналу на велику смугу частот. Вона також дозволяє мультиплексувати кілька користувачів без втрати якості зв'язку, оскільки кожен користувач має унікальний код, що дає змогу відокремлювати сигнали один від одного. Крім того, DS-CDMA ефективно пригнічує перехресні завади, що значно покращує якість зв'язку в умовах складної електромагнітної ситуації. Поєднання цієї технології з адаптивними антенними решітками дозволяє значно підвищити рівень захисту каналів управління БпНК, особливо в зонах активного застосування РЕБ, де традиційні методи зв'язку можуть виявитися вразливими до електронних атак, таких як глушення або перехоплення сигналів.

MANET є перспективним і гнучким рішенням для управління БпНК в динамічних бойових умовах, де швидко змінюється ситуація на полі бою. Основними перевагами таких мереж є здатність автоматично переналаштовувати топологію мережі в реальному часі, а також здійснення підтримки багатошляхової передачі даних, що дозволяє значно підвищити надійність зв'язку в умовах високої рухливості. Це дозволяє зменшити вплив фізичних перешкод та завад, оскільки дані можуть передаватися кількома маршрутами, що зменшує ризик повної втрати зв'язку в разі пошкодження або глушіння одного з каналів. Ще одна важлива перевага MANET полягає в можливості побудови мережевої інфраструктури без потреби у стаціонарних вузлах, що дозволяє створювати високоякісні зв'язки навіть у віддалених або тимчасових точках. Поєднання адаптивних антенних решіток, DS-CDMA та MANET може забезпечити постійну адаптацію маршрутів зв'язку, що дозволяє обходитись з зонами глушіння, переміщеннями та зміною умов на полі бою.

Одну з ключових ролей у сучасних системах управління БпНК може відігравати ШІ**,** забезпечуючи динамічне управління мережами зв'язку та навігації в реальному часі. Одним із основних напрямків його застосування є прогнозування зон радіоелектронного впливу, що дає змогу заздалегідь врахувати можливі ризики для зв'язку та адаптувати маршрути передачі даних і руху БпНК для мінімізації цього впливу. Інтелектуальне керування параметрами антенних решіток, зокрема підбором оптимального напрямку та величини підсилення для кожного каналу зв'язку, дозволяє значно підвищити ефективність розподілу енергії та поліпшити якість зв'язку в умовах РЕБ. Крім того, ШІ може використовуватися для аналізу спектрального середовища, визначаючи найменш завантажені частоти для передачі даних, що дозволяє уникати каналів, які можуть бути переповнені або піддаються інтенсивному впливу РЕБ. ШІ також забезпечує автономність прийняття рішень, що дозволяє БпНК діяти без постійного контролю з боку оператора, що особливо важливо для автономних місій, де кожна затримка або помилка в управлінні може призвести до значних наслідків. Всі ці фактори разом підвищують ефективність роботи БпНК, покращують їх стійкість до зовнішніх загроз і забезпечують високу автономність в складних умовах бойових дій.

Застосування оптоволоконних ліній в завданнях розмінування та матеріально-технічного забезпечення військ може бути якісною альтернативою традиційному радіозв'язку. Оптоволокно має кілька суттєвих переваг, зокрема, воно забезпечує

високий рівень захисту від радіозавад. Це дає змогу забезпечити надійний зв'язок навіть в умовах активного радіоелектронного впливу, що є важливим для безперервної роботи в складних бойових умовах. До того ж, оптоволокно дозволяє передавати великі обсяги даних без значних втрат якості, що є важливим для передачі даних оперативного та тактичного рівня в реальному часі. Вартість впровадження оптоволоконних систем є відносно доступною, що робить їх економічно привабливими, особливо в умовах, коли необхідно забезпечити стабільний зв'язок на значних відстанях.

Одним з найбільших ризиків при застосуванні оптоволокна є можливість фізичних пошкоджень каналу управління. Враховуючи, що оптоволокно має обмежену стійкість до механічних пошкоджень (наприклад, при розриві мін чи снарядів), це може призвести до втрати зв'язку з БпНК і, як наслідок, до його втрати або виходу з ладу. Тому для забезпечення надійності управління в умовах, де можуть виникнути фізичні пошкодження каналу зв'язку, доцільно передбачати резервні варіанти зв'язку, такі як радіозв'язок або інерціальні навігаційні системи, які можуть бути використані у разі пошкодження оптоволоконних ліній.

Попри зазначені обмеження, оптоволоконний зв’язок залишається надзвичайно ефективним рішенням для завдань розмінування, матеріально-технічного постачання та інших операцій, що вимагають стабільної та швидкої передачі значних обсягів даних. Загалом, оптоволоконні лінії мають значний потенціал для використання у військовій сфері, проте їхнє використання потребує ретельного аналізу бойових умов.

Таким чином, комплексне застосування технологій AAP, DS-CDMA, MANET та штучного інтелекту значно підвищує стійкість каналів управління БпНК до глушіння, спуфінгу та інших загроз РЕБ. Це забезпечує високу надійність зв’язку та дозволяє зберігати керованість БпНК навіть у складних бойових умовах.

Оптоволоконний зв’язок може бути ефективним у завданнях розмінування та логістики, завдяки стійкості до радіозавад, хоча його фізична вразливість обмежує застосування у динамічних бойових операціях.

Попри відносно високу вартість і складність реалізації, впровадження цих технологій є критично важливим для підвищення бойової ефективності та захисту особового складу. Їх інтеграція у систему управління БпНК забезпечить оперативну перевагу над противником та підвищить ефективність дій українських військ в умовах активної радіоелектронної боротьби.

Список використаних джерел

1. Концепція розвитку та застосування наземних роботизованих комплексів (платформ) у підрозділах Сухопутних військ Збройних Сил України, ВКП 3-00(11).01.2022. 21 с.
2. Доктрина «Застосування безпілотних систем у силах оборони України», ОП 3- 0(46), грудень 2023. 54 с.
3. Радиоэлектронные системы: основы построения и теория. Справочник / Ширман Я.Д., Лосев Ю.И., Минервин Н.Н., Москвитин С.В. Горшков С.А., Леховицкий Д.И., Левченко Л.С. / Под ред. Я.Д. Ширмана. М.: ЗАО «МАКВИС», 1998. 539 с.
4. Адаптивная компенсация помех в каналах связи / Ю. И. Лосев. М.: Радио и связь, 1998. 208 с.
5. Борисов І.В., Гурський Т.Г., Ільїнов М.Д., Гриценок К.М. Підвищення ефективності функціонування систем радіозв’язку за рахунок використання адаптивних антенних решіток. *Збірник наукових праць ВІТІ*. 2015. Вип. 1. С. 16–24.
6. Лебідь Є.В., Лазута Р.Р., Коваль О.М. Оцінка ефективності застосування адаптивних антенних решіток у системах радіозв'язку в умовах активної радіоелектронної боротьби. *Збірник наукових праць ВІТІ*. 2020. Вип. 1. С. 46–57.

УДК 355.5/36

Коробецький О.В.

БОРОТЬБА З УДАРНИМИ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ РАЗОВОГО ЗАСТОСУВАННЯ ТИПУ «SHAHED-136» (ГЕРАНЬ-2) ТА ОСОБЛИВОСТІ ЇХ ЛОКАЦІЇ НАД МОРЕМ

З початком широкомасштабного вторгнення на територію України російська федерація використовує ударні БпЛА разового застосування «Shahed-136» (Герань-2) для завдання ударів по об'єктам критичної інфраструктури України. За масштабами втрат, особливо підчас масованих атак такі БпЛА можливо дорівняти до засобів повітряного нападу. До сильних сторін ударних БпЛА «Shahed-136» (Герань-2) слід віднести їх аеродинаміку, можливість виконувати політ на малих та гранично малих висотах при цьому дальність їх застосування може досягати до 2500 км, тому існує імовірність несподіваної появи що різко знижує ефективність ППО. Наявність на борту ударних БпЛА інерційної системи навігації забезпечує польоти в складних метеорологічних умовах вдень і вночі, а також наявність у якості цільового навантаження до 50 кг бойової частини, ставить ударні БпЛА в ряд небезпечних засобів ураження. Тому організація протидії таким ударним БпЛА стає пріоритетним напрямком. Організація протидії ударним БпЛА «Shahed-136» (Герань-2) найбільш ефективна у разі ураження їх на далеких підступах до військових об'єктів та об'єктів критичної інфраструктури. Для боротьби з ударними БпЛА разового застосування «Shahed-136» (Герань-2) застосовується винищувальна (пілотована) авіація, армійська авіація, мобільні вогневі групи та ударні БпЛА перехоплювачі. Застосування винищувальної (пілотованої) авіації, армійської авіації дозволяє знешкодити ударні БпЛА «Shahed-136» (Герань-2) над морем що дає змогу залишати міста та населені пункти в безпеці. Застосування авіації, у свою чергу, ефективно у разі використання автоматизованих систем, але це вимагає певного часу, необхідного для прийняття рішення забезпечити цикл наведення винищувача на ударний БпЛА та розрахунку необхідного часу, а отже і необхідної дальності виявлення ударних БпЛА разового застосування типу «Shahed-136» (Герань-2).

Основними джерелами радіолокаційної інформації про ударні БпЛА разового застосування типу «Shahed-136» (Герань-2) є радіолокаційні станції (РЛС) системи бойового управління винищувальної авіації. Умови функціонування РЛС системи бойового управління та їх тактико-технічні характеристики (ТТХ) значною мірою визначають якість інформації для виконання оперативно-тактичних розрахунків на перехоплення винищувачами ударних БпЛА разового застосування типу «Shahed-136» (Герань-2).

Розташування станцій передачі команд на місцевості, вплив природних явищ на поширення радіохвиль і інші фактори визначають зону наведення та перехоплення ударних БпЛА разового застосування типу «Shahed-136» (Герань-2) винищувачами.

Політ винищувача по розрахунковій траєкторії з дотриманням умов безпеки польоту таких як своєчасне виявлення ударного БпЛА, вихід у точку зближення з ним й атаки, можливі тільки після своєчасного дозволу пункту управління (ПУ) на виконання перехоплення.

Виявлення ударних БпЛА разового застосування типу «Shahed-136» (Герань-2) та інших повітряних цілей у польоті можливе за допомогою станції радіолокаційної розвідки системи бойового управління. Можливості таких станції радіолокаційної розвідки по виявленню цілей дуже знижуються із зменшенням висоти польоту ударних БпЛА разового застосування типу «Shahed-136» (Герань-2), особливо в умовах пересіченої місцевості. При польоті ударних БпЛА разового застосування «Shahed-136»

(Герань-2) на висоті 100 м, засоби радіолокаційної розвідки в умовах прямої видимості цілей можуть виявити їх на дальності до 40 км, на висоті 25 м – на дальності до 21,42 км. При польоті ударних БпЛА типу «Shahed-136» (Герань-2) (на гранично малих висотах з огинанням рельєфу місцевості) перебування їх в зоні видимості короткочасне, що ускладнює своєчасне їх виявлення та розпізнавання. В цих умовах для ефективного виявлення та розпізнавання ударних БпЛА разового застосування «Shahed-136» (Герань-2) доцільно використовувати в комплексі різнотипні радіолокаційні станції (РЛС), і нетрадиційні методи виявлення і збільшення дальності виявлення ударних БпЛА при забезпеченні необхідної точності вимірювання координат.

Особливо важливим є південний напрямок тому що є можливість підльоту ударних БпЛА типу «Shahed-136» (Герань-2) з боку моря на наднизьких висотах. Саме на цьому напрямку проходить границя по Чорному морю і були проведені дослідження можливості використання радіохвилеводів для збільшення дальності виявлення ударних БпЛА типу «Shahed-136» (Герань-2) над морем. З урахуванням проведених досліджень є можливість проведення оцінки дальності виявлення ударного БпЛА типу Shahed-136 (Герань-2) при його знаходженні у тропосферному радіохвильоводі. Враховуючи, що для збільшення дальності виявлення повітряної цілі необхідно з урахуванням метеорологічних умов обрати позицію РЛС, що забезпечить границю тропосферного радіохвильоводу.

УДК 623.4.017:62.396.6

Костиря О.О., Гризо А.А., Лук'янчиков А.А., Черевко А.Є.

РОЗРОБКА ІМІТАТОРА ПОСТАНОВНИКА АКТИВНИХ ШУМОВИХ ЗАВАД ДЕЦИМЕТРОВОГО ДІАПАЗОНУ ХВИЛЬ ДЛЯ ТРЕНУВАННЯ ОБСЛУГ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ

Аналіз набутого бойового досвіду застосування Повітряних Сил Збройних Сил України під час російсько-української війни, починаючи з 2014 року, досвід останніх локальних війн та збройних конфліктів [1–3], визначає основні тенденції використання засобів вогневого та завадового впливу на радіоелектронні засоби як з боку противника, так і навпаки.

Одним із важливих елементів фахової підготовки обслуг радіолокаційних станцій (РЛС) радіотехнічних військ (РТВ) є їх навченість роботі в складних цільових та завадових умовах. Наявні тренажери з підготовки операторів не відповідають у повній мірі вимогам з якості навчання, оскільки формують лише вторинні позначки пеленга на постановник завад та не відтворюють ситуацію погіршення умов виявлення цілей унаслідок одночасної дії активної та пасивної завад, а також вплив автокомпенсатора завад на якість роботи радіолокатора, як це відбувається в реальній обстановці.

У процесі отримання радіолокаційної інформації роль оператора процесу безпосередньо виконує оператор РЛС. Досвід війни показує, що коли процес бойового чергування йде буденно, більшість операторів справляються зі своїми завданнями, але коли виникають нестандартні ситуації, часто може бути розгубленість і втрата контролю. Однією з найбільш поширених позаштатних ситуацій, яка виникає у ході військових конфліктів, є вплив активних завад. Оператор повинен виявити факт дії завади, класифікувати її, оцінити інтенсивність, визначити напрямок дії та ширину сектора подавлення станції. На підставі зібраних даних, тактико-технічних характеристик РЛС, розуміння, як функціонують її системи завадозахисту, оператор повинен вибрати варіант дій і оцінити його ефективність. З зазначеного випливає

необхідність проведення тренувань обслуговуючого персоналу РЛС в складних сигнально-завадових умовах [3, 4].

Використання реальних постановників завад та обладнання пов'язане з істотними труднощами технічного плану і значними матеріальними витратами, а саме:

– висока вартість реального обладнання та його експлуатації;

– неможливість залучення реального обладнання для навчання протягом тривалого часу;

– неможливість неодноразового відтворення навчальних сценаріїв з метою вироблення оптимальної стратегії дії та формування навичок бойової робити;

– висока складність та низька оперативність зміни конфігурації обладнання та параметрів;

– велика тривалість підготовчих робіт;

– складність показу результатів та оцінки можливих альтернативних варіантів дій [5].

Для створення близької до реальної завадової обстановки доцільно замість застосування справжніх дороговартісних постановників активних шумових завад (АШЗ) використовувати малопотужні пристрої імітації, встановленні, як правило, поблизу антени РЛС.

Зазначимо, що такий підхід є цілком правомочним. Практика показала, що ключовим елементом успішного застосування імітатора для тренувань є те, наскільки результат його використання викликає довіру у учнів. Або інакше кажучи, на скільки він є «психологічно достовірним», тобто наскільки добре імітатор може відтворити реальну ситуацію (на відміну від імітації роботи системи) і наскільки реалістичним це видається тому, хто навчається [5].

Такий імітатор був створений авторами, у роботі [6] наведено досвід створення програмно-апаратного комплексу імітації дії постановника АШЗ для тренування операторів РЛС. Наведено варіант побудови пристрою імітації впливу активних завад для РЛС РТВ, який дозволяє максимально наближено до реальної ситуації імітувати дію постановника активних завад (ПАЗ) або передавача завадд, що закидається, для тренування операторів РЛС на реальній позиції. Розроблено та апробовано методику використання розробленого імітатора.

Запропонований програмно-апаратний комплекс може імітувати вплив ПАЗ у діапазоні від 470 МГц до 900 МГц, що дозволяє охопити наявну номенклатуру РЛС РТВ дециметрового діапазону хвиль. Робочі смуги частот пристрою визначаються характеристиками застосованих антенних систем, а використані високочастотні підсилювачі забезпечують роботу у діапазоні частот 1–2000 МГц. Пристрій імітації дії ПАЗ побудовано з використанням готових модулів за схемою «малопотужний збуджувач – підсилювач потужності». Застосування технології COTS (системи COTS – це готові прикладні системи, які пропонують програмний інтерфейс прикладного програмування) забезпечило простоту, високу швидкість розробки та низьку вартість запропонованих технічних рішень. У якості джерела сигналу використовується пристрій HackRF ONE, який реалізовано з застосуванням технології програмно-визначеного радіо – SDR-технології (англ. Software-defined radio) [6].

Високочастотний підсилювач дециметрового діапазону виконано двоканальним, у якості елементної бази використано функціональні модулі радіодіапазону виробництва компанії Aideepen: модуль DC 5G RF – дільник потужності 1:2 та LNA2-2G-64DB – підсилювальний модуль, який забезпечує: коефіцієнт підсилення 64 дБ, рівень шуму 2 дБ. Максимальна вихідна потужність одного модуля 100 мВт, напруга живлення + 12 В, його навантаженням є антенна система у вигляді двох елементної антенної решітки [6].

З метою звуження ширини діаграми спрямованості антени у горизонтальній площині для підвищення її коефіцієнта направленої дії авторами було розроблено та виготовлено прототип антенної системи у вигляді 4-х елементної лінійної решітки.

Антенна система оптимізована на роботу у діапазоні 860–1020 МГц, має кращу спрямованість та прийнятні масо-габаритні характеристики, у якості елементарних випромінювачів використовуються компактні логоперіодичні антени. Амплітудно-фазовий розподіл на розкриві антени утворюється шляхом використання послідовних дільників, для з'єднання яких використовуються відрізки коаксіальних кабелів рівної електричної довжини [7].

Висновки. Розроблений пристрій імітації дії ПАЗ дозволяє операторам РЛС РТВ отримати практичні навички бойової роботи за умов реального впливу АШЗ. Використання імітатора постановника АШЗ дециметрового діапазону хвиль дозволить не тільки проводити фундаментальну підготовку, а й також створювати складні сценарії тренування та вправ, які охоплюють широкий спектр дії оператора.

Досліджений пристрій дозволяє відтворювати різновиди завадової обстановки, які охоплюють переважну більшість можливих варіантів застосування ПАЗ. Програмно-апаратний комплекс можна застосовувати для проведення тактичних навчань підрозділу РТВ та під час навчальних занять для імітації дії ПАЗ повітряного базування або постановника завад, що закидається. У подальшому планується доопрацювання імітатора АШЗ та методики його використання для перевірки ефективності роботи систем компенсації завад діючих зразків РЛС РТВ.

Список використаних джерел

1. Трофимов І.М., Худов Г.В., Білецький С.С., Гризо А.А., Гладіщук О.В. Особливості бойового застосування радіотехнічних військ Повітряних Сил Збройних Сил України в ході російсько-української війни. *Наука і техніка Повітряних Сил Збройних Сил України*. 2024. № 2(55). С. 76-85. https://doi.org/10.30748/nitps.2024.55.08.
2. Російські засоби РЕБ у бойових діях на Донбасі. [Електроний ресурс]. *Ukrainian Military Pages*. Режим доступу до ресурсу: http://www.ukrmilitary.com/2016/05/russian-reb-v-donbasse.html.
3. Гризо А. А., Костиря О. О., Лісогорський Б. А., Ткаченко В. І. Аналіз характеристик та оцінка ефективності застосування потенційних засобів вогневого ураження елементів системи протиповітряної оборони у російсько-українській війні. *Наука і техніка Повітряних Сил Збройних Сил України*. 2023. № 1(50). С. 70-81. https://doi.org/10.30748/nitps.2023.50.08.
4. Гризо А.А., Альчаков О.О., Лашкул І.М., Полтавець В.А. Пропозиції щодо використання багаточастотного зондуючого сигналу для підвищення якості завадозахисту модернізованих РЛС П-18МА та П-18 Малахіт. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 2(35). С. 143-150. Also available online, URL: https://journal-hnups.com.ua/index.php/nitps/article/view/nitps.2019.35.18. (accessed 18/02/2025).
5. Гризо А.А., Костиря О.О., Ковалевський С.М., Ушаков С.І. Реалізація андрагогічного підходу при проведенні курсів підвищення кваліфікації та перепідготовки офіцерів радіотехнічних спеціальностей, призваних за мобілізацією. *Системи озброєння і військова техніка*. 2023. № 1(73). С. 96-105. https://doi.org/10.30748/soivt.2023.73.11.
6. Костиря О.О., Гризо А.А., Федоров А.В., Романов Ю.М. Досвід створення імітаторів перешкодової обстановки для тренування операторів РЛС метрового та дециметрового діапазонів хвиль. *Системи озброєння і військова техніка*. 2022. № 2(70). С. 46-55. https://doi.org/10.30748/soivt.2022.70.06.
7. Гризо А.А., Костиря О.О., Додух О.М. Пристрій пеленгації випромінювання безпілотних літальних апаратів з покращеною характеристикою спрямованості. *Системи озброєння і військова техніка*. 2024. № 1(77). С. 7-15. https://doi.org/10.30748/soivt.2024.77.01.

УДК 621.396.962

Кот В.В., Герасимов С.В.

ІМІТАЦІЙНА МОДЕЛЬ ДІАГНОСТУВАННЯ ТЕХНІЧНОГО СТАНУ ЕЛЕКТРООБЛАДНАННЯ БРОНЕТАНКОВОЇ ТЕХНІКИ

Існуюча апаратура діагностування технічного стану не повністю задовольняє вимогам до процесу технічного обслуговування та ремонту систем енергозабезпечення бронетанкової техніки [1, 2]. Для адекватного опису процесу діагностування технічного стану систем енергозабезпечення зразків бронетанкової техніки як складної технічної системи доцільне представлення такого об’єкту як виробу, що складається із множини комплектуючих модулів [3, 4]. Також необхідно врахувати при дослідженні ефективності контролю технічного стану систем енергозабезпечення бронетанкової техніки те, що в реальній експлуатації відновлення працездатності складових елементів транспорту проводиться за фактом виявлення відмови об'єкта контролю, незважаючи на його працездатність в цей момент [5, 6].

Підвищення вимог до показників якості електроенергії систем енергозабезпечення бронетанкової техніки вимагає удосконалення методів і засобів їх контролю [3, 7]. Однак подальший розвиток таких вимірювальних засобів у значній мірі стримується рівнем їх технічних характеристик при незначній собівартості.

У зв’язку з цим, виникає актуальне наукове завдання в галузі діагностування технічного стану систем енергозабезпечення бронетанкової техніки: удосконалення методів синтезу апаратури контролю технічного стану систем енергозабезпечення.

Метою дослідження є розроблення імітаційної моделі діагностування технічного стану систем енергозабезпечення бронетанкової техніки для підвищення достовірності визначення раціональних інтервалів технічного обслуговування.

Основною ознакою універсальної апаратури діагностування є їх багатофункціональність, тобто здатність вимірювати декілька різних фізичних величин [1, 4].

Ступінь універсальності апаратури діагностування безперервно зростає, і чим вона вище, тим більше апаратура наближаються до вимірювальних інформаційних систем. Одночасно посилюються такі негативні особливості апаратури діагностування порівняно зі спеціалізованими вимірювальними приладами, як ускладнення схеми та зростання кількості режимів вимірювання, що призводить до значного ускладнення функцій керування для забезпечення певної взаємодії функціональних пристроїв апаратури, яка відповідає тому чи іншому алгоритму перетворення інформації. Тому створення високоефективної апаратури діагностування технічного стану потребує вирішення комплексу складних взаємопов’язаних завдань. Найважливіше з них – це уніфікація, яка повинна проводитися за такими напрямками:

– уніфікація методів і засобів первинного та вторинного вимірювального перетворення сигналів у апаратурі діагностування;

– уніфікація вхідних і вихідних сигналів вимірювальних перетворювачів апаратури діагностування;

– уніфікація конструкції функціональних блоків апаратури діагностування на базі єдиних типорозмірів та інтерфейсних функцій.

Розширення універсальності апаратури діагностування нерозривно пов’язано із підвищенням уніфікації й не може вирішуватися у відриві від неї.

Найбільш доцільним при створенні апаратури діагностування є блочно-модульний принцип їх побудови, який полягає у визначенні оптимальної номенклатури функціональних вузлів (блоків), їх уніфікації за певними стандартизованими

показниками та виготовленні у вигляді уніфікованих модулів. Номенклатура уніфікованих модулів апаратури діагностування визначається перш за все комплексом вимірюваних фізичних величин і прийнятим підходом до їх структурної побудови. Насамперед підкреслимо, що нераціональним є безпосереднє вимірювання апаратурою діагностування різнорідних фізичних величин, кожна з яких має свою розмірність, оскільки це потребувало б уведення в нього значної кількості мір вимірюваних величин та інших функціональних пристроїв, що призвело б до значного ускладнення приладу та низького коефіцієнта використання окремих блоків (модулів).

Тому основною розроблення імітаційної моделі діагностування технічного стану системи електрообладнання зразків бронетанкової техніки повинно враховувати принципи побудови аналогової та цифрової апаратури діагностування. При цьому необхідно враховувати моделі проміжного перетворення всіх вимірюваних фізичних величин в один або декілька уніфікованих сигналів, найбільш зручних для наступної обробки, за допомогою аналогових вимірювальних перетворювачів (первинних і вторинних). Мінімальна кількість моделей перетворювачів дорівнює кількості різнорідних фізичних величин при часовому розділенні вимірювальних каналів, коли однорідні фізичні величини вимірюються послідовно в часі з використанням тих самих первинних вимірювальних перетворювачів для однорідних фізичних величин даного виду. Максимальна кількість первинних вимірювальних перетворювачів необхідна при просторовому розділенні вимірювальних каналів, за якого кожній фізичній величині (в тому числі й однорідним величинам, наприклад постійним напругам від різних просторово розміщених об’єктів) відповідає свій перетворювач. Тому запропонована імітаційна модель враховує принцип будови автоматизованих вимірювальних систем і вимірювально-інформаційних систем.

Список використаних джерел

1. С.В. Герасимов, Л.В. Гаценко. **Моделювання генерації сигналів спеціальної форми для контролю технічного стану радіоелектронного обладнання**, *Комплексне забезпечення якості технологічних процесів та систем* (КЗЯТПС – 2022): матеріали тез доповідей XI Міжнародної науково-практичної конференції, Чернігів: НУ «Чернігівська політехніка», 2022, Т. 2, С. 176.
2. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.
3. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.
4. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference «Application of information technologies in the preparation and operation of law enforcement forces»*, March 15, 2022, p.p. 31-32.
5. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference «Scientific Trends and Trends in The Context of Globalization»*, UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.
6. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.
7. O. Daki, S. Herasimov and H. Zubrytskyi, **Digital Correlation Method For Power**

Measurement, *Information Processing Systems*, № 4 (163), 2020, p.p. 15-26, https://doi.org/10.30748/soi.2020.163.02.

Котова М.А., Лабушняк В.В.

АВТОМАТИЗОВАНА МЕТОДИКА КАЛІБРУВАННЯ ЦИФРОВИХ МУЛЬТИМЕТРІВ ЗАКОРДОННОГО ВИРОБНИЦТВА

На даний час у Збройних Силах України та інших військових формуваннях починають широко застосовуватись портативні 3½ та 3¾ - розрядні цифрові мультиметри закордонного виробництва (ЦМЗВ) різноманітних типів (APPA 97, APPA 98, APPA 99, APPA 105N, OWON OW 16A, OWON OW 18A, OWON OW 18E, UNI-T UTM 171E, UNI-T UTM 181E, UNI-T UTM 1136C, Sanwa PM7a, Fluke 17B, Fluke 178 та інші).

Зазначені засоби вимірювальної техніки забезпечують вимірювання постійної та змінної напруги, сили постійного та змінного струму, електричного опору, електричної ємності, частоти змінної напруги і струму, а також температури у широкому діапазоні значень та використовуються замість технічно застарілих комбінованих електровимірювальних приладів, аналогових і цифрових універсальних вольтметрів груп В3 і В7 для контролю параметрів різноманітних зразків озброєння та військової техніки на всіх етапах їх життєвого циклу. Завдяки кращим технічним та експлуатаційним характеристикам, ЦМЗВ забезпечують підвищення якості технічного обслуговування зразків ОВТ.

В зв’язку із багатофункціональністю, процес періодичного калібрування ЦМЗВ має високу трудомісткість, яка пов'язана із необхідністю перевірки метрологічних характеристик мультиметра на всіх режимах та піддіапазонах вимірювання. Кількість позначок калібрування на кожному з піддіапазонів вимірювання складає від трьох до шести. Враховуючи, що ЦМЗВ мають, в основному, вісім режимів вимірювання із п’ятьома піддіапазонами вимірювань на кожному з них, калібрування та оцінка відповідності мультиметра повинна здійснюватись не менш ніж у 144-ох позначках калібрування.

В зв’язку з цим, актуальною на даний час задачею е зменшення трудомісткості процесу калібрування ЦМЗВ шляхом проведення його часткової автоматизації.

У доповіді розглядається методика автоматизованого калібрування ЦМЗВ методом прямих вимірювань з використанням універсального калібратора типу Fluke 5502A, з’єднаного за допомогою дистанційного інтерфейсу з персональним комп’ютером (ПК). При даному методі калібрування оператор встановлює піддіапазон вимірювання ЦМЗВ, після чого на його вхід послідовно подаються вимірювальні сигнали калібратора, які дорівнюють позначкам калібрування. Встановлення вимірювальних сигналів на виході калібратора здійснюється дистанційно за допомогою ПК з використанням спеціального програмного забезпечення (ПЗ). Програмне забезпечення керує вихідними сигналами калібратора у відповідності із протоколами калібрування ЦМЗВ, які зберігаються у базі даних програми. Для сучасних ЦМЗВ (типів APPA 105N, APPA 106, APPA 107N, APPA 109N, APPA 301, APPA 305, Fluke 287, Fluke 289, тощо), обладнаних дистанційним інтерфейсом RS-232, можлива також автоматизація процесів обробки та реєстрації показів мультиметра у позначках калібрування з використанням програмного забезпечення Fluke View Forms або Win DMM100, що надається фірмою-виробником ЦМЗВ.

Впровадження даної методики дозволить зменшити трудомісткість та підвищити оперативність процесу калібрування 3½ та 3¾ - розрядних цифрових мультиметрів закордонного виробництва, які застосовуються у Збройних Силах України.

Красинський С.В., Меркулов О.А., Мироненко О.В., Ніколенко В.В.

ЕКСПЕРТИЗА ЩОДО ВИКОНАННЯ МЕТРОЛОГІЧНИХ ВИМОГ ДО ВИРОБІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ: АКТУАЛЬНІ ПИТАННЯ ОРГАНІЗУВАННЯ ТА ПРОВЕДЕННЯ

Відповідно до положень ДСТУ В 15.009 [1], ДСТУ ISO 9001 [2] та ДСТУ ISO 10012 [3] вимірювання є невід'ємною частиною процесу керування якістю, у тому числі і виробів озброєння та військової техніки (ОВТ). Забезпечити точність і достовірність вимірювань параметрів виробів ОВТ та інших матеріальних об'єктів є головним завданням метрологічної діяльності (МлД) у сфері оборони України. Так, забезпечення єдності вимірювань (ЗЄВ) безпосередньо впливає на якість виробів ОВТ, їхніх складових частин і комплектувальних виробів, якість виконання відповідних процесів, процедур і послуг [4]. ДСТУ В 15.901 [4] розроблено та впроваджено на заміну застарілому ДСТУ В 1.2-95 [5].

Основною метою МлД для виробів ОВТ є підвищення якості, конкурентоспроможності й ефективності застосування (використання, експлуатування) виробів ОВТ [4].

МлД планують і реалізовують з урахуванням принципів керування життєвим циклом (ЖЦ) ОВТ згідно з ДСТУ В 15.001 [6], одним з яких є — безперервність.

МлД планують, організовують та проводять упродовж усього ЖЦ виробів ОВ.

Зазвичай МлД на стадіях ЖЦ планують і організовують у рамках зінтегрованої логістичної підтримки згідно з ДСТУ В 15.005 [7]. Стратегію (концепцію) МлД та початкові метрологічні вимоги викладають в оперативно-стратегічних, оперативно-тактичних і тактико-технічних вимогах до перспективних виробів ОВТ [4], у проєкті плану керування програмою (проєктом) та проєкті плану зінтегрованої логістичної підтримки згідно з ДСТУ В 15.002 [8] та ДСТУ В 15.005 [7].

Метрологічні вимоги (до виробів ОВТ) - вимоги до заходів, спрямованих на забезпечення єдності вимірювань, засобів вимірювальної техніки, вимірювальних (інформаційно-вимірювальних) систем, параметрів (характеристик) виробів озброєння та військової техніки, а також до методів (методик) та умов вимірювання (контролювання) параметрів виробів озброєння та військової техніки (об'єктів вимірювання) та інших об'єктів вимірювань, пов'язаних з ними [4, 9].

Одним із видів МлД є експертиза щодо виконання метрологічних вимог (далі – експертиза ВМВ) до виробів ОВТ [4]. Експертиза ВМВ - аналізування і оцінювання правильності прийнятих технічних рішень стосовно комплексу заходів, спрямованих на досягнення єдності вимірювань та достовірності контролювання параметрів виробів озброєння та військової техніки упродовж їхнього життєвого циклу [9].

Експертиза ВМВ до виробів ОВТ на теперішній час проводиться замість метрологічної експертизи документації (далі - МЕД) на ОВТ (згідно з ДСТУ В 3263-95 [10], який є застарілим та багато положень якого втратили свою актуальність) [11]. Однак, у експертизи ВМВ є, як багато спільного з МЕД, так і є великі відмінності.

Так, експертиза ВМВ (як і МЕД) організовується та проводиться метрологічною службою у системі Міністерства оборони (далі - МО) України (раніше - метрологічна служба МО України та ЗС України) у межах здійснення військово-метрологічного супроводження ОВТ на всіх етапах і стадіях його ЖЦ [12].

Однак, згідно з положеннями ДСТУ В 15.011 [13] експертиза ВМВ є одним з типів наукових і науково-технічних експертиз, аналізів та аудитів та має бути невід'ємним елементом процесів верифікації та валідації ОВТ.

Заключним етапом формування нормативної бази для організування та проведення експертизи ВМВ (трансформування її з МЕД) повинно стати впровадження на заміну

застарілому нормативному документу ДСТУ В 3263-95 проєкту ДСТУ [9], який зараз знаходиться на останній стадії прийняття та надання чинності.

Окрім незавершених питань нормативного забезпечення організування та проведення експертизи ВМВ на даний час можна виділити ще декілька актуальних питань, а саме:

– організування експертизи ВМВ (планування та взаємодія суб'єктів експертизи, підготовка та підвищення кваліфікації фахівців-експертів);

– фінансово-економічні питання (фінансування відряджень членів комісії).

У доповіді визначені пропозиції та шляхи вирішення актуальних питань за напрямком організування та проведення експертизи ВМВ до виробів ОВТ.

Список використаних джерел

1. ДСТУ В 15.009:2023. Система керування життєвим циклом озброєння та військової техніки. Керування якістю. Основні положення. Київ: ДП »УкрНДНЦ», 2023. 112 с.
2. ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT). Системи управління якістю. Вимоги. Київ: ДП «УкрНДНЦ», 2015. 31 с.
3. ДСТУ ISO 10012:2005 (ISO 10012:2003, IDT). Системи керування вимірюванням. Вимоги до процесів вимірювання та вимірювального обладнання. Київ: ДП «УкрНДНЦ», 2005. 27 с.
4. ДСТУ В 15.901:2024. Система керування життєвим циклом озброєння та військової техніки. Метрологічна діяльність. Основні положення. Київ: ДП »УкрНДНЦ», 2024. 32 с.
5. ДСТУ В 1.2-95. Державна система стандартизації військової техніки. Метрологічне забезпечення озброєння та військової техніки. Основні положення. Київ: Держстандарт України, 1995. 19 с.
6. ДСТУ В 15.001:2023. Система керування життєвим циклом озброєння та військової техніки. Основні положення. Київ: ДП »УкрНДНЦ», 2023. 26 с.
7. ДСТУ В 15.005:2022. Система керування життєвим циклом озброєння та військової техніки. Зінтегрована логістична підтримка на стадіях життєвого циклу озброєння та військової техніки. Основні положення. Київ: ДП »УкрНДНЦ», 2022. 36 с.
8. ДСТУ В 15.002:2021. Система керування життєвим циклом озброєння та військової техніки. План керування програмою (проєктом). Єдиний наскрізний план. Основні положення. Київ: ДП »УкрНДНЦ», 2021. 38 с.
9. Проєкт (остаточна редакція) ДСТУ XXXX: 202X. Озброєння та військова техніка. Експертиза щодо виконання метрологічних вимог. Основні положення. 2024. 49 с.
10. ДСТУ В 3263–95. Метрологія. Метрологічна експертиза зразків і комплексів ОВТ. Організація та порядок проведення. Київ: Держспоживстандарт України, 1995. 26 с.
11. Бойко В. М., Ноженко О. М., Меркулов О. А., Герасимов С.В., Кірвас В.В., Зубрицький Г.М. Дослідження аспектів нормативно-правового забезпечення організації та проведення метрологічної експертизи документації на вироби озброєння та військової техніки. *Метрологія та вимірювальна техніка*: Збірник наукових праць Харківського національного університету Повітряних Сил, 2021, 4(70). С. 95-104. https://doi.org/10.30748/zhups.2021.70.14.
12. Про затвердження Положення про метрологічну службу у системі Міністерства оборони України № 288 від 24.05.2017 р. (у редакції наказу МО України № 872 від 30.12.2024 р.): Наказ Міністерства оборони України.
13. ДСТУ В 15.011:2023. Система керування життєвим циклом озброєння та військової техніки. Наукові і науково-технічні експертизи, аналізи та аудити. Основні положення. Київ: ДП »УкрНДНЦ», 2023. 47 с.

УДК 004.057:621.39

Лавренчук А.А., Пастушенко М.С., Стародубцев С.О.

СУЧАСНІ МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ: ІННОВАЦІЇ, ЗАГРОЗИ ТА ЗАХИСТ

У сучасному цифровому світі питання автентифікації набуває все більшої актуальності. Традиційні методи, такі як паролі або токени, вже не забезпечують належного рівня безпеки, оскільки вони можуть бути забуті, втрачені або викрадені. Натомість біометрична автентифікація пропонує надійніший підхід, використовуючи унікальні фізіологічні та поведінкові характеристики користувача [1-3].

Біометричні методи поділяються на дві основні групи: фізіологічні та поведінкові. До фізіологічних належать відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока та навіть аналіз ДНК. Поведінкові методи включають аналіз голосу, динаміку клавіатурного введення, почерк та мікрорухи очей. У порівнянні з паролями, біометрія забезпечує зручність та складність підробки, проте вона також має свої вразливості [4].

Інновації у сфері біометричної автентифікації розширюють можливості використання цих технологій. Наприклад, нейроавтентифікація, що базується на аналізі електроенцефалографічних сигналів (EEG), дозволяє ідентифікувати особу за унікальними електричними імпульсами мозку. Динамічна біометрія, яка включає аналіз мікрорухів очей або використання IMU-сенсорів для розпізнавання ходи, забезпечує ще більш точну автентифікацію. Окрім цього, новітні технології, такі як блокчейн, пропонують способи захисту біометричних шаблонів, мінімізуючи ризики несанкціонованого доступу та компрометації даних [2].

Попри значні переваги, біометричні системи залишаються вразливими до певних атак. Спуфінг, або атаки Presentation Attack, передбачають використання підроблених біометричних даних, таких як фальшиві відбитки пальців чи 3D-маски для розпізнавання обличчя. Deepfake-технології також становлять загрозу, оскільки дозволяють змінювати обличчя та голос користувача в режимі реального часу. Крім того, існує ризик атак на збережені біометричні шаблони, що може призвести до викрадення конфіденційних даних.

Для підвищення рівня безпеки біометричних систем застосовуються різні методи захисту. Мультимодальна автентифікація, яка поєднує декілька біометричних факторів, значно ускладнює можливість несанкціонованого доступу. Блокчейн-технології забезпечують децентралізоване та безпечне зберігання біометричних даних, а квантово-стійка криптографія дозволяє запобігти можливим загрозам майбутнього, пов’язаним із розвитком квантових обчислень [1].

У межах дослідження було проведено аналіз сучасних методів біометричної автентифікації, їхніх переваг, недоліків та потенційних загроз. Основну увагу зосереджено на інноваційних підходах, таких як нейроавтентифікація, динамічна біометрія та використання блокчейн-технологій для захисту біометричних шаблонів.

Було здійснено класифікацію біометричних методів за фізіологічними та поведінковими характеристиками, а також оцінено ефективність різних біометричних систем на основі ключових показників, зокрема FAR (False Acceptance Rate), FRR (False Rejection Rate) та EER (Equal Error Rate). Окрім цього, досліджено загрози, пов’язані з атаками на біометричні системи, включаючи спуфінг, Deepfake-атаки та компрометацію шаблонів.

Результати дослідження показали, що:

1. Традиційні біометричні методи (відбитки пальців, розпізнавання обличчя, райдужки ока) забезпечують високу точність, проте вразливі до атак, особливо при

використанні підроблених даних.

2. Динамічна біометрія та нейроавтентифікація є перспективними напрямами, що дозволяють значно ускладнити підробку автентифікаційних даних, проте потребують удосконалення алгоритмів та технічної бази.

3. Deepfake-технології становлять значну загрозу для біометричних систем, оскільки дозволяють обходити засоби розпізнавання обличчя та голосу, що вимагає впровадження додаткових механізмів виявлення підроблених даних.

4. Використання блокчейну для зберігання біометричних шаблонів значно підвищує безпеку систем, усуваючи ризики централізованого витоку даних, але створює нові виклики, пов'язані з масштабованістю та продуктивністю таких рішень.

5. Мультимодальна автентифікація (поєднання декількох біометричних методів) продемонструвала найвищий рівень надійності, оскільки знижує ймовірність обходу системи шляхом компрометації одного біометричного фактора.

Отримані результати підтверджують, що майбутній розвиток біометричної автентифікації залежатиме від інтеграції новітніх технологій, зокрема штучного інтелекту, блокчейну та квантово-стійкої криптографії. Впровадження комплексних заходів захисту дозволить значно підвищити надійність біометричних систем та мінімізувати ризики несанкціонованого доступу.

Таким чином, біометрична автентифікація є перспективним напрямом у сфері інформаційної безпеки, проте її розвиток потребує постійного вдосконалення. Інноваційні технології та нові методи захисту допоможуть зменшити ризики атак та підвищити надійність цифрової ідентифікації у майбутньому.

Список використаних джерел

1. Бондаренко Г.В., Коваль О.О., Ткаченко М.С. Біометрична автентифікація: принципи, методи та засоби: монографія / за ред. Г.В. Бондаренка. Київ: Техніка, 2020. 312 с.
2. ДСТУ ISO/IEC 19794-1:2016. Інформаційні технології. Біометричні формати обміну даними. Частина 1: Архітектура (ISO/IEC 19794-1:2011, IDT). Київ: ДП «УкрНДНЦ», 2016. 32 с.
3. Зайцев О.П., Гончарук Л.В. Квантово-стійка криптографія: виклики та перспективи // Інформаційні технології і безпека. 2023. № 4. С. 56–69.
4. National Institute of Standards and Technology. Biometric Performance Testing and Reporting URL: https://www.nist.gov/programs-projects/biometric-performance-testing-and-reporting (дата звернення: 12.03.2025)

Лаврут О.О., Лаврут Т.В., Колесник В.О., Жук О.В.

ПОКРАЩЕННЯ ЯКОСТІ УПРАВЛІННЯ ПОТОКАМИ ІНФОРМАЦІЇ У СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ: ПЕРСПЕКТИВИ РОЗВИТКУ

У сучасному світі ефективне управління потоками інформації є важливим аспектом військових операцій. У цій доповіді розглянуто поточний стан управління потоками інформації у військових телекомунікаційних мережах та перспективи їх розвитку.

1. Сучасні технології управління потоками інформації:

– програмно-визначені мережі (SDN) дозволяють централізовано контролювати і управляти потоками інформації шляхом розподілу функцій управління і передачі даних. Це забезпечує гнучкість і оперативність у зміні конфігурації мережі відповідно до поточних потреб;

– віртуалізація мережевих функцій (NFV) дозволяє використовувати програмні

модулі для виконання мережевих функцій, що забезпечує ефективне використання ресурсів та швидку масштабованість, що є особливо важливим у військових умовах, де зміни у конфігурації мережі можуть відбуватися дуже швидко;

– оптимізація трафіку та забезпечення якості обслуговування (QoS) дозволяють пріоритезувати критично важливі дані та забезпечувати їх своєчасну доставку. Цей напрм включає використання методів планування, управління чергами та шифрування для забезпечення надійності та безпеки передачі даних, тензорний аналіз тощо.

2. Перспективи розвитку управління потоками інформації у військових телекомунікаційних мережах:

– штучний інтелект (ШІ) та машинне навчання для управління потоками інформації дозволяє автоматично аналізувати великі обсяги даних та приймати оптимальні рішення, що впливає на ефективність мережі та зменшення затримок у передачі даних;

– інтернет речей (IoT) дозволяє підключати велику кількість пристроїв та сенсорів, що забезпечує збір та обробку даних у реальному часі. Це сприяє підвищенню ситуаційної обізнаності та забезпечує надійне управління потоками інформації;

– квантова криптографія та захищений зв’язок відкривають нові можливості для забезпечення надвисокого рівня захисту даних. Використання квантових технологій у військових телекомунікаційних мережах може значно знизити ризик несанкціонованого доступу до інформації.

Інтеграція інноваційних технологій, таких як ШІ, SDN, квантова криптографія тощо, дозволяє створити високоефективні, гнучкі та захищені комунікаційні системи.

Список використаних джерел

1. Лаврут О.О. Вибір критерію оцінювання якості управління потоками інформації у телекомунікаційній мережі мобільного компоненту перспективної системи зв’язку ЗС України. *Наука і техніка Повітряних сил Збройних Сил України*. 2014. Вип. 3 (16). С. 113-115.
2. Лаврут О.О., Лаврут Т.В. Модель та метод управління трафіком в мережах зв’язку критичного призначення. Prospects and priorities of research in science and technology: Collective monograph. Vol. 2. Riga, Latvia: «Baltija Publishing», 2020. P. 36-60. DOI: https://doi.org/10.30525/978-9934-26-008-7.2-3.
3. Лаврут О.О., Лаврут Т.В., Здоренко Ю.М., Колесник В.О. Модель та метод управління інформаційними потоками у телекомунікаційній мережі тактичної ланки управління. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2021. Вип. 1(40)/2021. С. 13–26. DOI: https://doi.org/10.33099/2311-7249/2021-40-1-13-26.
4. Лаврут О.О., Лаврут Т.В., Мартиненко А.М. Описание системы спутниковой связи как сложного динамического объекта при помощи метода Крона. *Радіоелектронні і комп’ютерні системи: науково-технічний журнал.* 2010.№ 7 (48). С. 251-256.

Лаврут О.О., Лаврут Т.В., Шармін В.В., Бойчук Б.М.

ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ: ПЕРСПЕКТИВИ РОЗВИТКУ

Зв'язок та управління – запорука успіху на полі бою. Без належного зв’язку та координації навіть найсучасніша техніка перетворюється на дороговартісну мішень. Сьогодні розвиток телекомунікаційних мереж військового призначення здійснюється за наступними напрямами:

1. Розвиток 5G та 6G технологій передачі даних. Високошвидкісні бездротові мережі 5G та наступних поколінь забезпечують малу затримку передачі даних, високу пропускну здатність і стійкість до перешкод, що є необхідним для розгортання

автономних бойових систем, таких як безпілотні літальні апарати та наземні роботизовані платформи;

2. Технологія когнітивного радіо. Створення радіосистем, здатних отримувати відомості про особливості власної експлуатації і на основі цих даних корегувати параметри своєї роботи;

3. Квантова криптографія та захищеність зв'язку. Однією з головних загроз для військових комунікацій є кібератаки та можливість перехоплення даних. Квантові комунікаційні технології пропонують високий рівень захисту інформації за рахунок принципу неможливості клонування квантового стану;

4. Розвиток супутникового зв'язку. Використання низькоорбітальних супутникових угруповань, таких як Starlink або OneWeb, забезпечує стійке покриття та глобальний доступ до військового зв'язку навіть у віддалених районах;

5. Штучний інтелект та автоматизація мереж. Інтеграція штучного інтелекту у військові телекомунікаційні системи дає можливість автоматично аналізувати мережевий трафік, передбачати можливі загрози та оптимізувати маршрути передачі даних у реальному часі;

6. Інтеграція з бойовими інформаційними системами. Мережі нового покоління (в тому числі з самоорганізацією Ad-Hoc та Manet) сприяють оперативному обміну даними між різними військовими підрозділами, дозволяючи забезпечити єдине інформаційне поле та підвищити ситуаційну обізнаність командирів;

Отже, удосконалення системи зв'язку та пошук нових підходів до її організації дозволить забезпечувати необхідну перевагу на полі бою.

Список використаних джерел

1. Іохов О.Ю., Лаврут О.О., Лаврут Т.В., Флорін О.П. Сучасні засоби зв'язку та інфокомунікаційні технології у Збройних Силах України та Національній гвардії України: сьогодення та перспективи застосування. *Честь і закон.* 2022. №4/2022. С. 113-122. DOI: https://doi.org/10.33405/2078-7480/2022/4/83/272323.
2. Лаврут О.О. Вибір критерію оцінювання якості управління потоками інформації у телекомунікаційній мережі мобільного компоненту перспективної системи зв'язку ЗС України. *Наука і техніка Повітряних сил Збройних Сил України*. 2014. Вип. 3 (16). С. 113-115.
3. Лаврут О.О. Перспективні підходи та технології побудови систем управління силових структур. «Findings of modern engineering research and developments»: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2022. P. 233-264. DOI https://doi.org/10.30525/978-9934-26-207-4-9
4. Лаврут О.О., Стрюк О.Ю., Польщиков К.О. Тензор – можлива модель опису системи супутникового зв'язку як складного динамічного об'єкту. *Системи озброєння і військова техніка.* 2009. Вип. 4(20). С. 131-134.

УДК 004.415.538

Лановий О.Ф.

КЛАСИФІКАЦІЯ ЗВІТІВ ПРО ДЕФЕКТИ МЕТОДАМИ ШІ

Дефекти в програмному забезпеченні становлять серйозну загрозу надійності комп'ютерних систем. Вони можуть проявлятися у вигляді багів, що призводять до збоїв, некоректних результатів, порушення логіки програми або навіть безпеки системи. Звіти про помилки, що надходять від користувачів великих програмних проектів, достатньо часто виявляються неправильно класифікованими, що змушує

розробників активно залучатися до їх ручної верифікації.

Процес виправлення дефектів повинен бути ініціюваним щоразу, коли в програмній системі виявляється баг, а джерелом інформування про них можуть бути (в залежності від етапу розробки чи використання програмної системи) тестувальники, QA-інженери або користувачі. Для забезпечення можливості розробникам виправити дефект необхідно ідентифікувати проблему шляхом формування звіту або баг-репорту. Звіти про виявлені проблеми представляють собою напівструктуровані документи, які фіксують ситуації або труднощі, що виникають в процесі використання або тестування програмного забезпечення. Як правило, такі звіти містять атрибути, що надають контекстуальну інформацію у вигляді текстових полів, які включають заголовок і опис проблеми і підлягають подальшому аналізу з боку розробників. Ця інформація зосереджує їх увагу на декількох ключових аспектах, зокрема: серйозність проблеми, причина виникнення та коректність класифікації звіту (тобто чи відповідає зазначений тип проблеми реальному характеру вказаного дефекту).

Проведений аналіз повідомлень про дефекти у програмних системах з відкритим кодом (на прикладі Mozilla Firefox) свідчить, що значна кількість проблем, яка фіксується як дефект, насправді не містить справжніх помилок, а пов’язана з впровадженням нових функціональних можливостей, вдосконаленням програмної системи, оновленням документації або ж є помилками самих авторів повідомлень [1]. Останнє досить часто зумовлено недостатнім рівнем технічних знань щодо системи, оскільки більшість авторів таких повідомлень є виключно кінцевими користувачами [2]. Проблема також полягає у тому, що аналіз кожного з таких повідомлень є достатньо складним і трудомістким процесом, який інколи вимагає залучення декількох розробників чи тестувальників, і досить часто призводить до марних витрат часу та ресурсів, коли розробники приходять висновку, що повідомлення про помилку чи дефект є хибним.

Сучасні технології машинного навчання (ML) активно інтегруються в автоматизацію задач в традиційній інженерії програмного забезпечення, включаючи виправлення помилок та їх класифікацію. Проте, процес виявлення помилок залишається складним через обробку неструктурованих даних, які потребують детального аналізу. Також існує широкий спектр можливих конфігурацій і параметрів, що ускладнює прийняття відповідних рішень та може призводити до неточностей в інтерпретації інформації. Інтеграція ML у ці процеси є важливим кроком для підвищення їх ефективності.

Основною метою дослідження є розробка методології визначення, чи дійсно певна проблема є помилкою або ні, що дозволить автоматизувати процес аналізу та класифікації повідомлень про дефекти. Використання отриманих результатів може спростити процес обробки повідомлень про дефекти та підвищити загальну якість програмного продукту.

Баг-репорт – це технічний документ, що описує ситуацію або послідовність дій, що призвела до некоректної роботи об’єкта тестування, з вказанням причин і очікуваного результату. Звіти про помилки є суттєвими артефактами програмного забезпечення, і існує значна кількість наукових досліджень, присвячених їх аналізу [1-3]. Класифікація баг-репортів, зокрема їх неправильна категоризація, можуть суттєво вплинути на якість інструментів і досліджень, що базуються на таких даних.

Неправильна класифікація баг-репортів становить значну проблему. В роботі [3] дослідники вручну класифікували понад 7000 повідомлень про дефекти у програмних проектах з відкритим вихідним кодом та встановили, що майже 30% повідомлень фактично не є звітом про помилку. Це свідчить про суттєвий вплив проблеми неправильної класифікації на результати роботи над дефектами. Таким чином, забезпечення коректної класифікації баг-репортів дозволить суттєво підвищити якість розробки програмних продуктів.

Аналіз проведених досліджень свідчить, що більшість підходів до класифікації звітів

зазвичай покладаються на ознаки, отримані із заголовків, описів або коментарів до звітів про дефекти, які є текстовими полями. Тому в цій роботі основну увагу буде приділено розробці алгоритму класифікації повідомлень про виявлені баги за принципом «баг-не баг» з використанням алгоритмів машинного навчання.

В роботі [1] наведено опис методу, що базується на використанні довгострокової та короткочасної пам'яті (LSTM). Відповідно до цього методу, спочатку звіт про дефекти попередньо обробляється і відображає слова у вектори дійсних чисел, які у подальшому використовуються для обчислення векторного представлення звіту на основі векторних представлень слів, які він містить. Запропонований алгоритм (рис.1) за допомогою бібліотеки TensorFlow2 забезпечує класифікацію звіту за критерієм «баг – не баг».

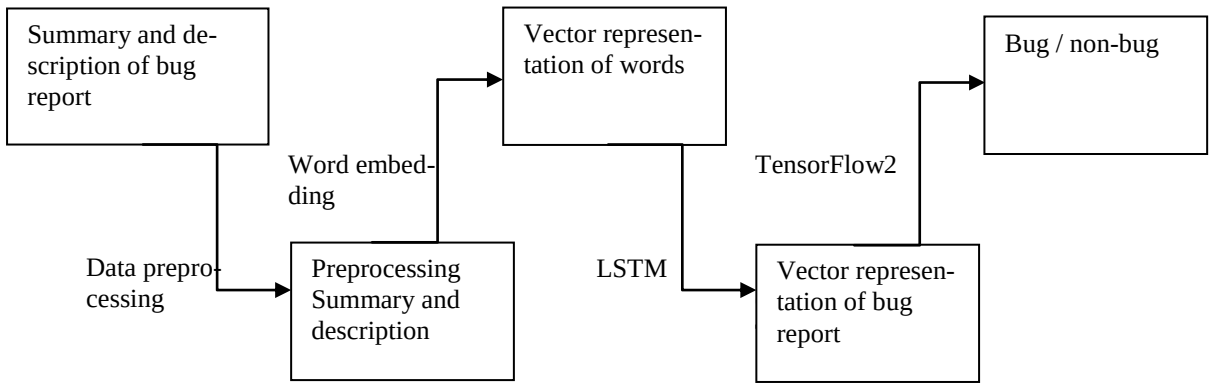


Рисунок 1 – Алгоритм використання LSTM для класифікації баг-репортів

Незважаючи на достатню простоту цього алгоритму, він потребує значного періоду навчання з вчителем для формування бази знань щодо визначення категорії «баг – не баг» та відокремлених обчислювальних ресурсів для збереження накопичених результатів, а також налаштування на відповідну предметну галузь. Тому доречним є аналіз можливості застосування більш простих методів проведення аналізу звітів про дефекти, серед яких найбільш привабливим є використання моделі на основі архітектури трансформерів [4].

Одним із популярних інструментів підтримки розробки програмного забезпечення є GitHub. GitHub надає власну вбудовану систему відстеження проблем (issue tracking system), що дозволяє користувачам створювати звіти про дефекти, пропонувати нові функції або ставити запитання. Ця система забезпечує централізоване зберігання інформації про проблеми, що виникають у процесі розробки, та сприяє їх ефективному вирішенню.

Разом з тим обробка баг-репортів може бути складним завданням через великий обсяг інформації, що надходить, а також через різноманітність стилів опису дефектів. Технології обробки природної мови, зокрема моделі трансформерів, такі як BERT (Bidirectional Encoder Representations from Transformers) або GPT (Generative Pre-trained Transformer), здатних аналізувати текстову інформацію, враховуючи її контекст, робить їх ефективними для автоматизації обробки баг-репортів.

Одним із можливих застосувань таких моделей є бінарна класифікація баг-репортів: автоматичне визначення, чи є звіт про дефект релевантним і потребує уваги розробників, або він може бути відхилений як нерелевантний або дубльований. Завдяки здатності трансформерів розуміти контекст, вони можуть враховувати специфічну термінологію проєкту, аналізувати опис проблеми та навіть передбачати, до якої категорії належить баг-репорт (наприклад, функціональний дефект, проблема з інтерфейсом або пропозиція щодо покращення).

З метою спрощення системи обробки баг-репортів та прискорення її роботи в дослідженні було введено наступні обмеження на вхідні дані:

1) звіти про дефекти, що розміщені на GitHub, будуть аналізуватись лише за текстовим вмістом наступних полів:

– Label: Вказує на тип повідомлення, який може бути одним з наступних: помилка, покращення або питання;

– Issue title: Скорочена назва, що містить опис проблеми;

– Issue body: Основна частина звіту про проблему, яка містить детальний опис дефекту та шляхи, що призвели до його виникнення;

– Issue URL: посилання на баг-репорт, що розміщений на GitHub;

– Repository URL: Метадані, що зберігають посилання на репозиторій проекту на GitHub;

– Creation timestamp: Мітка часу створення звіту про дефект;

– Author association: Вказівка на автора звіту та його відношення до проекту – може приймати значення Owner, Collaborator, Contributor, Member, None.

2) текстова інформація, що міститься в Issue body та буде використовуватись для проведення аналізу, потребує попередньої підготовки, до якої відноситься виключення з тексту опису проблеми фрагментів коду.

Таким чином, використання моделей трансформерів у поєднанні з інструментами, такими як GitHub, дозволяє значно підвищити ефективність обробки баг-репортів, зменшити навантаження на команди розробників і прискорити процес виправлення дефектів. Це є важливим кроком у напрямку автоматизації процесів у сфері розробки програмного забезпечення.

Список використаних джерел

1. Hanmin Qin and Xin Sun. Classifying bug reports into bugs and non-bugs using LSTM. ACM International Conference Proceeding Series (2018), 16-19. Issue: https://doi.org/10.1145/3275219.3275239
2. Saniat Javid Sohrawardi, Iftekhar Azam, and Shazzad Hosain. A comparative study of text classification algorithms on user submitted bug reports. 2014 9th International Conference on Digital Information Management, ICDIM 2014 (2014), 242–247. Issue: https://doi.org/10.1109/ICDIM.2014.6991434
3. K. Herzig, S. Just and A. Zeller. «It's not a bug, it's a feature: How misclassification impacts bug prediction,» 2013 35th International Conference on Software Engineering (ICSE), San Francisco, CA, USA, 2013, pp. 392-401. Issue: https://doi.org/10.1109/ICSE.2013.6606585
4. M.L. Siddiq and J.C.S. Santos. «BERT-Based GitHub Issue Report Classification,» 2022 IEEE/ACM 1st International Workshop on Natural Language-Based Software Engineering (NLBSE), Pittsburgh, PA, USA, 2022, pp. 33-36, doi: 10.1145/3528588.3528660.

УДК 621.396

Левківський Н.В., Бабарика А.О.

РОЛЬ ЕКВІВАЛЕНТІВ АНТЕН У ПІДВИЩЕННІ БЕЗПЕКИ СИСТЕМИ ЗВ’ЯЗКУ

Забезпечення надійного зв’язку в сучасних умовах є критично важливим завданням, особливо в умовах ведення бойових дій, протидії засобам радіоелектронної боротьби (РЕБ) та ускладненої електромагнітної обстановки. Одним із методів підвищення стійкості систем зв’язку є використання еквівалентів антен, що дозволяє оцінювати та покращувати характеристики реальних антенних систем без необхідності їхнього фізичного застосування. Еквіваленти антен є важливим компонентом у забезпеченні

безпеки системи зв’язку. Окрім того, радіосистеми потребують постійної перевірки на працездатність. Сучасні УКХ радіосистеми не мають внутрішніх протоколів тестування вихідного тракту.

Для вирішення задач прихованості радіомереж від систем радіоелектронної розвідки противника та перевірки вихідних трактів УКХ радіостанцій актуальною задачею є розробка пристрою, який може вимірювати потужність вихідного тракту радіостанції без розповсюдження радіохвиль в просторі. Для вирішення цієї задачі розроблено пристрій,
який забезпечить вимірювання потужності радіостанцій, використовуючи термоелектр
ичний елемент Пельтьє та навантажувальний резистор [1].

Основними компонентами апаратної реалізації пристрою є:

– термоелектричний елемент TEC1-12706, що виконує роль датчика теплової енергії;
– навантажувальний резистор 50 Ом 150 Вт, який поглинає потужність радіостанції;
– антенний подовжувач, що з'єднує радіостанцію з резистором;
– алюмінієвий радіатор, який забезпечує охолодження системи;
– термопрокладка, що стабілізує температуру датчика;
– мультиметр, який вимірює напругу на виході елемента Пельтьє, що корелює з поданою потужністю.

Сигнал передається з радіостанції на резистор через антенний подовжувач, нагріваючи його [2]. В результаті нагрівання одна сторона елемента Пельтьє створює різницю потенціалів, яку можна виміряти мультиметром і використати для визначення потужності.

Нормування шкали рівнів потужності проведено емпіричним методом шляхом подачі на вихід еталонної радіостанції різних рівнів потужності, що відповідало зміні напруги на виході елемента Пельтьє. Отримані в результаті значення напруги на виході елемента Пельтьє дали змогу розробити шкалу рівнів потужності вихідного тракту радіостанції.

Список використаних джерел

1. Василенко Т. Системи вимірювання потужності радіостанцій: монографія / Т. Василенко. – Дніпро: Радіотехнічні дослідження, 2022. – 184 с..
2. Rachok R., Katerynchuk I., Prokopenko Y., Strelbitskyi M., Babaryka A., Basarab O. Separate Issues of the Rational Construction of a Wireless Sensor Radio Network. *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv. Ukraine, 2024. P. 121-124. doi: 10.1109/TCSET64720.2024.10755682.

Лейба В.О., Любішин Б.В.

ПРОБЛЕМИ ФОРМУВАННЯ СИГНАЛІВ ІЗ ЗАДАНИМ КОЕФІЦІЄНТОМ ГАРМОНІК

Для повірки аналізаторів спектра та вимірювачів нелінійних спотворень формують сигнали із заданим (точно відомим коефіцієнтом гармонік). Але при формуванні сигналів виникають певні труднощі, тому що коефіцієнт гармонік, будучи інтегральним параметром сигналу, незмінний до його форми за умови рівності амплітуд перших гармонік та середньоквадратичних значень вищих гармонік.

Сигналів із заданим коефіцієнтом гармонік може бути нескінченно багато. Це, з одного боку дає можливість використовувати як вимірювальні сигнали з нормованим коефіцієнтом гармонік сигнали прямокутної, трикутної або синусоїдальної форми.

Але, з іншого боку, це призводить до невизначеності вибору вимірювального сигналу, що породжує суперечки про його найкращу форму.

Однозначної відповіді питанню, якою має бути форма сигналу немає, так як форма не обмежується самим визначенням коефіцієнта гармонік.

Пошук оптимальної форми повинен проводитися виходячи з мети вимірювального сигналу, наприклад, з урахуванням вимоги узгодження спектра сигналу, з діапазоном робочих частот вимірювання засобу вимірювання. Недотримання цієї вимоги спричиняє появу додаткових похибок виміру, які неможливо чи досить складно оцінити. Тому оптимальним вважається такий вимірювальний сигнал, спектр якого повністю знаходиться в діапазоні робочих частот засобів вимірювань, що повіряється. Не один сигнал, а цілий ряд оптимальних вимірювальних сигналів так як кількість гармонік та його співвідношення може бути різними.

Поряд із оптимальними, у вимірювальній практиці знаходять застосування інших сигнали, формування яких може здійснюватися більш простими засобами. Загальний недолік відомих вимірювальних сигналів – те, що коефіцієнт гармонік в них визначається ставленням, наприклад, середньоквадратичних значень напруги другої та першої гармонік, або через відношення рівня обмеження синусоїдального сигналу до його амплітудного значення.

Точне завдання відносин змінних напруг залежить від похибки ділення використовуваних цієї мети дільників. Дані пристрої дуже трудомісткі у виготовленні та громіздкі, незручні для автоматизації їх виготовлення. Тому розглядається спосіб завдання коефіцієнта гармонік, не через відношення напруги, а через відношення тривалостей інтервалів часу. Похибка вимірювання та відтворення інтервалів часу вже сьогодні досягає часткою пікосекунд, і немає принципових обмежень щодо її подальшого зниження.

УДК 621.391

Литвин А.В., Вакуленко Д.М.

НАПРЯМКИ МОДЕРНІЗАЦІЇ ШИРОКОСМУГОВИХ МЕРЕЖ ЗВ’ЯЗКУ ТИПУ MANET

Досвід ведення сучасних збройних конфліктів, зокрема російсько-української війни, продемонстрував критичну необхідність суттєвого збільшення пропускної здатності як у традиційних каналах зв'язку, так і у каналах радіозв'язку, організованих широкосмуговими режимами станцій від провідних світових виробників, таких як L3 HARRIS та SILVUS. Практичне застосування радіостанцій SILVUS для організації прив'язки окремих підрозділів у ході проведення спеціальних операцій на території противника дозволило забезпечити швидкісну та надійну передачу даних по каналах радіозв'язку в умовах підвищеної складності.

Відомо, що пропускна здатність каналу безпосередньо корелює зі смугою пропускання радіоканалу, що є фундаментальним фактором для покращення якості передачі голосу, підвищення швидкості передачі даних, збільшення кількості доступних каналів та зменшення чутливості до різного роду перешкод. У контексті сучасних військових комунікацій, де надійність та ефективність обміну інформацією мають виняткове значення, оптимізація цього параметру набуває особливої актуальності.

Провідна американська технологічна компанія L3 HARRIS впровадила інноваційну форму сигналу (TSM-X) у радіостанціях серії FALCON IV, що дозволило досягти значного збільшення пропускної здатності та розширення діапазону смуги

пропускання. Зазначена форма сигналу гарантує стабільне функціонування мережі з потенційною підтримкою до 200 вузлів при використанні єдиного частотного каналу, що є вирішальним фактором для успішного проведення тактичних операцій у несприятливих умовах. Теоретичні та практичні дослідження підтверджують, що така технологія забезпечує оптимальне співвідношення між ефективністю використання спектру та стійкістю до навмисних і ненавмисних завад.

Компанія SILVUS імплементує технологію Mobile Networked MIMO (MN-MIMO), яка представляє собою інтеграцію кодованого ортогонального мультиплексування з частотним розділенням каналів (COFDM), технології множинного входу та множинного виходу Multiple Input Multiple Output (MIMO) та мобільних спеціальних мереж (MANET). Це технологічне рішення забезпечує цифровий зв'язок з безпрецедентними показниками продуктивності та адаптивності.

COFDM реалізує принцип ортогонального частотного мультиплексування шляхом перетворення широкосмугового радіоканалу на сукупність паралельних вузькосмугових піднесучих. Ця технологія забезпечує ефективну передачу даних та підвищену стійкість до багатопроменевого поширення і селективних частотних завмирань. Зокрема, при застосуванні в каналах з частотно-селективними завмираннями OFDM суттєво знижує рівень міжсимвольної інтерференції за рахунок паралельної передачі вузькосмугових підканалів.

Просторове мультиплексування в технології MIMO дозволяє системі передавач/приймач суттєво збільшити пропускну здатність без додаткового використання смуги пропускання або підвищення потужності передачі. Застосування технології MIMO в умовах радіоелектронного протиборства надає значні переваги з точки зору підвищення завадостійкості та інформаційної безпеки завдяки можливості просторової селекції сигналів. Ефективність мультиплексування характеризується лінійним збільшенням пропускної здатності, пропорційно до кількості антен передавача або приймача (залежно від того, яка з цих величин менша).

Розширення смуги пропускання в УКХ радіозв'язку шляхом впровадження нових форм сигналу та технології MIMO надає мережам типу MANET можливість динамічно адаптувати свою топологію відповідно до відносного переміщення вузлів. Це дозволяє максимізувати швидкість передачі даних та підвищити надійність зв'язку між окремими хостами телекомунікаційної мережі.

Аналіз досвіду застосування мереж MANET в умовах інтенсивного радіоелектронного протиборства демонструє, що здатність до самоорганізації та оптимізації маршрутизації є критично важливими характеристиками для забезпечення безперервності зв'язку. Алгоритми маршрутизації в MANET, такі як OLSR (Optimized Link State Routing), AODV (Ad-hoc On-demand Distance Vector) та DSR (Dynamic Source Routing), забезпечують гнучке встановлення та підтримку маршрутів між вузлами мережі, що особливо важливо в умовах динамічного бойового простору [1].

Слід зазначити, що інтеграція технологій SDR (Software Defined Radio) з мережами MANET відкриває додаткові можливості для адаптивного керування параметрами радіосистеми, включаючи динамічну зміну смуги пропускання, модуляції та потужності передачі, залежно від зовнішніх умов. Це забезпечує оптимальний компроміс між дальністю зв'язку, швидкістю передачі даних та енергоефективністю.

Перспективними напрямками подальшої модернізації широкосмугових мереж зв'язку типу MANET є:

– впровадження технологій когнітивного радіо для адаптивного використання доступного спектру та мінімізації інтерференції з іншими системами [2];

– розробка удосконалених алгоритмів маршрутизації з урахуванням енергетичних обмежень та вимог до якості обслуговування (QoS);

– інтеграція методів штучного інтелекту для прогнозування стану каналів та оптимізації параметрів передачі;

– вдосконалення методів захисту інформації та протидії радіоелектронному придушенню.

Таким чином, комплексна модернізація широкосмугових мереж зв'язку типу MANET з використанням інноваційних технологій формування сигналів та просторового мультиплексування дозволяє досягти істотного підвищення ефективності тактичних комунікацій у складних умовах сучасного бойового простору.

Список використаних джерел

1. Романюк В.А., Степаненко Є.О., Панченко І.В., Восколович О.І. Літаючі самоорганізуючі радіомережі. *Збірник наукових праць Військового інституту телекомунікацій та інформатизаці*ї. 2017. №1 С. 104-114.
2. Vasylyshyn V., Stoliar O. Efficiency improvement of radio communication systems with OFDM based on cognitive radio technology. *Стан та перспективи розвитку інфокомунікацій в сучасних умовах:* зб.тез доп. наук. конф., м.Харків, 22 лист. 2024. С.79.

УДК 621.391

Литвин А.В., Пеньковський О.Л.

ЗАСТОСУВАННЯ ГІБРИДНИХ МЕТОДІВ РОЗШИРЕННЯ СПЕКТРУ В СУЧАСНИХ ЗАСОБАХ РАДІОЗВ'ЯЗКУ

У контексті сучасних викликів, пов'язаних з ускладненням електромагнітної обстановки та посиленням інтенсивності радіоелектронного протиборства, актуалізується проблематика забезпечення стійкості засобів радіозв'язку. Російсько-українська війна продемонструвала затребуваність та ефективність технологій розширення спектру для протидії засобам радіоелектронного придушення. Одним із перспективних напрямів вирішення зазначеної проблеми є розробка та впровадження гібридних методів розширення спектру, що поєднують переваги різних підходів.

У фундаментальній основі комбінованих методів розширення спектру закладено принцип синергії двох або більше базових методів, спрямований на нівелювання притаманних їм недоліків при одночасному підсиленні переваг. Результати багатьох досліджень підтверджують, що ефективність гібридизації методів розширення спектру істотно перевищує показники окремих методів за умов складної радіоелектронної обстановки.

До найбільш перспективних компонентів гібридних систем слід віднести:

– метод розширення спектру прямої послідовності (DSSS);
– технологію стрибкоподібної зміни частоти (FHSS);
– ортогональне частотне мультиплексування (OFDM);
– метод лінійної частотної модуляції (LFMCW).

Парадигма інтеграції DSSS та OFDM полягає у застосуванні псевдовипадкової послідовності для модуляції субносійних частот OFDM-сигналу.

Експериментальні дослідження демонструють, що застосування даної гібридної конфігурації забезпечує підвищення коефіцієнта завадостійкості на 15-20% порівняно з класичними реалізаціями OFDM при дії направлених завад типу «білий шум» [3]. Додатковими перевагами є оптимізація частотного ресурсу та зниження ймовірності ідентифікації сигналу засобами радіотехнічної розвідки.

При практичній імплементації гібридних методів розширення спектру необхідно врахувати низку технічних аспектів:

– забезпечення точної синхронізації псевдовипадкових послідовностей між

передавальним та приймальним пристроями, що є критичним для систем з dsss-компонентом;

– оптимізація обчислювальної архітектури з огляду на підвищені вимоги до процесорної потужності;

– дотримання енергоефективності шляхом адаптивного регулювання параметрів передачі;

– імплементація алгоритмів адаптації до змінних умов поширення сигналу та характеристик завад.

Оптимальний баланс між завадостійкістю та енергоефективністю досягається при використанні адаптивних алгоритмів, що корегують базис розширення DSSS відповідно до спектральних характеристик завад [4].

Стратегічним напрямом розвитку комбінованих методів розширення спектру є інтеграція технологій штучного інтелекту для забезпечення автоматичної адаптації параметрів системи до змін радіоелектронної обстановки [5]. Сучасні дослідження засвідчують, що застосування методів машинного навчання для оптимізації параметрів гібридних методів розширення спектру потенційно здатне підвищити ефективність використання радіочастотного ресурсу на 25-30% [6].

Таким чином, синтез технологій DSSS та OFDM представляє собою ефективне рішення для забезпечення високої швидкості передачі даних із одночасним досягненням високої стійкості до завад та багатопроменевого поширення сигналу. Запропонований метод інтегрує переваги обох підходів та створює передумови для розбудови захищених систем радіозв'язку з мінімальною вразливістю до засобів радіоелектронного придушення.

Список використаних джерел

1. Torrieri D. Principles of Spread-Spectrum Communication Systems. Springer, 4th Edition, 2022.
2. Скляр Б. Цифровий зв'язок: теоретичні основи та практичне застосування. Техносфера, 2020.
3. Agrawal P., et al. «Hybrid Spread Spectrum Techniques for Military Communications». Military Communications Conference (MILCOM), pp. 312-317, 2023.
4. Zhang Y., Huaping L. «Performance Analysis of DSSS-OFDM in Jamming Environment». IEEE Transactions on Communications, vol. 71, no. 4, pp. 2567-2581, 2023.
5. Chen X., Wang J. «Artificial Intelligence in Anti-jamming Communications: A Survey». IEEE Surveys & Tutorials, vol. 25, no. 1, pp. 431-459, 2023.
6. Jonsson E. «Machine Learning for Adaptive Spectrum Management in Hybrid Spread Spectrum Systems». International Journal of Wireless Information Networks, vol. 31, no. 1, pp. 78-93, 2024.

Лютий А.О.

ІННОВАЦІЙНЕ РОЗГОРТАННЯ БАЗОВИХ СТАНЦІЙ НА БАГАТОСМУГОВИХ ВУЛИЦЯХ ІЗ ПІДТРИМКОЮ МУЛЬТИЗВ'ЯЗКУ МІЖ ТА ВСЕРЕДИНІ RAT, З ВИКОРИСТАННЯМ МІЛІМЕТРОВИХ І СУБМІЛІМЕТРОВИХ ХВИЛЬ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕРЕЖІ

Щоб зменшити вплив перешкод, спричинених динамічним блокуванням шляхів поширення в міліметрових (mmWave) системах, 3GPP запропонувала мультизв'язок, за якого обладнання користувача (UE) одночасно підключається як до базової станції (BS) у діапазоні до 6 ГГц, так і до mmWave BS. Ми

розглядаємо один із найскладніших перспективних сценаріїв розгортання – розгортання на багатосмугових вулицях із мультизв'язком як усередині RAT, так і між ними.

Технології безпроводового зв'язку в міліметровому діапазоні (mmWave) відіграють ключову роль у розвитку сучасних мобільних мереж, сприяючи їх переходу до стандартів п'ятого покоління (5G) і шостого в подальшому. Хоча процес стандартизації нової радіотехнології (NR) майже завершений 3GPP, однією з основних дослідницьких задач залишається оптимізація систем NR для різних сценаріїв розгортання.

Завдяки роботі в широкій доступній смузі пропускання, системи міліметрових хвиль здатні забезпечити надзвичайно високу пропускну здатність на повітряному інтерфейсі, що робить їх ідеальними для ресурсоємних додатків. Це включає в себе такі сервіси, як доповнена та віртуальна реальність, потокові ігри та відео високої роздільної здатності. Однак такі системи мають значну вразливість до блокування сигналу між базовою станцією (БС) і користувацьким обладнанням (UE). Це блокування може бути спричинене не лише великими статичними об'єктами (наприклад, будівлями), а й меншими динамічними перешкодами, такими як людські тіла або транспортні засоби [1,2]. Дослідження показують, що загасання сигналу через людське тіло може перевищувати 15 дБ, а при перешкодах, спричинених транспортними засобами, втрати досягають 40 дБ. Унаслідок цього зв'язок між UE та БС тимчасово втрачатися, що призводить до відключень.

Щоб компенсувати такі перебої, 3GPP запропонував механізм багатозв'язності (multi-connectivity), який дозволяє UE підтримувати одночасні з'єднання з кількома базовими станціями та динамічно перемикатися між ними у разі втрати сигналу. Окрім підтримки мультизв'язності всередині однієї технології радіодоступу (RAT), 3GPP також передбачає можливість одночасної роботи з кількома RAT. Наприклад, UE може підтримувати декілька активних з'єднань із різними базовими станціями mmWave, а також додаткове підключення до мікрохвильової БС у діапазоні до 6 ГГц, яка покриває ту ж саму територію. У цьому випадку, навіть якщо щільність розміщення БС mmWave недостатня для мінімізації ризику відключень, користувацький трафік може бути тимчасово переадресований на БС в діапазоні до 6 ГГц, яка значно менш чутлива до блокування сигналу.

Такий підхід допомагає підвищити надійність з'єднання та забезпечити стабільність обслуговування навіть у складних міських умовах, де наявність численних перешкод є неминучою.

Розглянемо спільну систему міліметрових хвиль і sub-6 ГГц, показану на рис. 1, з декількома БС мілметрового діапазону в зоні покриття однієї БС sub-6 ГГц. У розглянутих умовах вуличного розгортання передбачається, що БС міліметрового діапазону встановлюються по обидва боки вулиці, наприклад, на ліхтарних стовпах або стінах будівель.

На рис. 1 видно вуличне розгортання БС де відстань між БС з міліметровими хвилями вздовж однієї сторони становить d, і вони розташовані по різні боки, утворюючи рівнобедрені трикутники, тобто зсунуті на половину відстані d між двома послідовними БС з міліметровими хвилями. Потужність, що випромінюється БС мм-хвиліта БС до 6 ГГц, вважається постійною і дорівнює $P_{T,N}$ та $P_{T,L}$, відповідно.

Вважається, що вулиця має N смуг руху, де N - парне число. Напрямок руху «верхніх» і «нижніх» $N/2$ смуг протилежний. Ширина кожної смуги постійна і дорівнює w. Для визначення характеристик відмов, які є вхідною інформацією для процесу обслуговування дорожнього руху на БС мм-хвилі та до 6 ГГц, випадковим чином позначено транспортний засіб у дорожньому русі. Цей транспортний засіб називається *позначеним* транспортним засобом. Швидкість позначеного транспортного засобу приймається рівною v_U. Висота БС, пов'язаної з позначеним транспортним засобом, є постійною, h_U . Швидкість інших транспортних засобів вважається

постійною, v_B . У цьому дослідженні не враховано «товщину» транспортних засобів, представляючи їх як двовимірні об'єкти (прямокутники) у площині, перпендикулярній до площини дороги і розташованій на центральній лінії кожної смуги. Довжина та висота є дискретними випадковими величинами і характеризуються кумулятивними функціями розподілу (CDF), *FL,B (x) та FH,B (x)*, відповідно. Центри сторін прямокутника організовують пуассонівський процес з інтенсивністю λB .



Рисунок 1 – Вуличне розгортання базових станцій до 6 ГГц/ммХвилі.

У розглянутому розгортанні шлях поширення сигналу прямої видимості (LoS) між БС з міліметровими хвилями і UE, встановленими на транспортних засобах, може бути заблокований іншими транспортними засобами. За результатами вимірювань перешкод на частотах mmWave, передбачається, що блокування лінії зв'язку автомобілями призводить до додаткового погіршення якості на 30 дБ.

Модель поширення UMi 3GPP в міських забудовах, а також втрат на блокування дозволяє виділити три зони навколо БС з міліметровими хвилями (рис. 1). У першій зоні, визначеній радіусом *RB* , втрати при поширенні є такими, що UE не відчуває умов відключення, навіть коли він заблокований. У другій зоні, обмеженій радіусами *RB* та *RO* , *RO* > *RB* , UE відчуває відключення тільки тоді, коли шлях LoS заблокований. Нарешті, відключення відбувається навіть у неблокованих умовах для UE, розташованих далі, ніж *RO*. Ці радіуси можуть бути розраховані за допомогою моделі поширення та припущення про додаткові втрати 30 дБ, спричинені блокуванням.

Список використаних джерел

1. Коляденко Ю.Ю., Лютий А.О. Модель систем зв‘язку 6G за умов спільного використання міліметрових та субміліметрових радіохвиль. Міжнародна науково-практична

конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» 14 березня 2024 року, м. Харків. С. 172 -174. https://nangu.edu.ua/uploads/files/Zbirnyk%20tez%20MNPK%2014.03.2024.pdf
2. М. Гапеєнко та ін., «Про часові ефекти мобільних блокаторів у міських сценаріях стільникового зв'язку міліметрового діапазону», *IEEE Transactions on Vehicle Technology*, vol. 66, no. 11, pp. 10124-10138, Листопад 2017.

УДК 621.396

Майборода І.М.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СУПУТНИКОВИХ ТЕРМІНАЛІВ НА ОСНОВІ RIS ТЕХНОЛОГІЇ

Досвід російсько-української війни показав, що, в першу чергу, широкосмуговий доступ до інтернету забезпечує можливість швидкої передачі інформації для військових. У багатьох були очікування, що повномасштабне вторгнення обмежить його роботу. Натомість - супутниковий інтернет Starlink забезпечив нам постійний обмін інформацією між різними підрозділами Сил оборони України.

Мережа супутників на низькій навколоземній орбіті (LEO) від таких компаній, як Starlink та Eutelsat OneWeb, обіцяє забезпечити зв’язок у будь-якій точці світу. Але для встановлення зв’язку із супутниками, які постійно перебувають у русі та швидкого перемикання між ними, для підтримки надійного зв’язку потрібні передові антенні технології. Отже, компанія Greenerwave розробила RIS (Reconfigurable Intelligent Surfaces) технологію дешевих і енергоефективних супутникових терміналів для доступу в інтернет на основі «інтелектуальних поверхонь, що реконфігуруються». Технологія використовує штучний інтелект та знижує вартість енергоспоживання терміналів у 10 разів у порівнянні з традиційними способами.

Запропонований радикально новий підхід до побудови наземних терміналів передбачає використання технології метаматеріалів та «інтелектуальних поверхонь, що реконфігуруються» для формування і зміни напряму радіопроменів. Це дозволяє створювати високоефективні антени зі значно меншими витратами в порівнянні з традиційними фазованими антеними решітками, де потрібне використання складної і дорогої електроніки.

Термінал, заснований на RIS, складається з безлічі невеликих регульованих відбивних блоків, які працюють узгоджено, змінюючи напрямок та властивості променя, коли він відбивається від поверхні. Оскільки в антені використовується набагато простіша електроніка, то технологія більш рентабельна та енергоефективна, особливо для використання в додатках, де вона критично важлива, наприклад на транспортних засобах, у тому числі на літаках.

В основі підходу щодо створення терміналів полягають фундаментальні дослідження метаматеріалів, тобто штучно створених структур, які демонструють електромагнітні властивості, які зазвичай не зустрічаються в природних матеріалах. Зокрема, використовується двовимірний метаматеріал, що є поверхнею, яка складається з великої кількості мініатюрних елементів, що відбивають, електричний опір яких можна індивідуально перемикати між високим і низьким рівнями. Це дозволяє точно контролювати фазу радіохвиль, відбитих від кожного елемента.

Але незважаючи на простоту апаратної реалізації, що здається, для точного налаштування RIS необхідні складні алгоритми. Greenerwave використовує спеціальне програмне забезпечення та цифрових «двійників» на основі штучного інтелекту для моделювання поведінки антени та розрахунку оптимальних параметрів.

Таким чином, RIS технологія відкриває нові перспективи для використання супутникового інтернету. Вже сьогодні велика супутникова компанія Intelsat веде роботи щодо створення спеціалізованого термінала на основі тієї ж RIS технології. Також окрім супутникового зв'язку, в Greenerwave бачать потенціал використання своєї розробки і для мереж 5G та 6G, оскільки низьке енергоспоживання може зацікавити телекомунікаційні компанії.

УДК 623.7

Максюта Д.В., Книш Д.В., Порохончук О.М.

АКТУАЛЬНІ НАПРЯМКИ РОЗВИТКУ РАДІОЕЛЕКТРОННИХ СИСТЕМ ДЛЯ СИЛОВИХ СТРУКТУР УКРАЇНИ

Розвиток радіоелектронних систем для силових структур значною мірою визначається сучасними викликами, такими як повномасштабна військова агресія проти України, кібервійна, асиметричні загрози, високі вимоги до захищеності зв'язку та технологічності сучасних систем озброєння. Аналіз публікацій з відкритих джерел свідчить про актуальність та перспективність зазначених нижче напрямків розвитку радіоелектронних систем.

1. Розвиток засобів захищеного зв'язку та управління:

– цифровізація та інтеграція інформаційних технологій, завершення переходу від аналогових до цифрових систем обробки та передачі сигналів, створення єдиного інформаційного простору для всіх рівнів управління;

– використання програмно керованих радіосистем (SDR), які спрямовані на забезпечення гнучкості та адаптивності радіозв'язку, наприклад проєкт ESSOR (European Secure Software-defined Radio), що має військове застосування;

– розробка стійких до перешкод систем зв'язку (Frequency Hopping, Spread Spectrum, MIMO- та MANET (Mobile Ad-Hoc Networks)-технологій) з підвищеною пропускною здатністю, динамічним вибором частот для уникнення перешкод, підвищення безпеки та надійності передачі даних, зменшення ймовірність перехоплення сигналу та інтерференції з іншими радіосигналами;

– використання квантової криптографії для передачі даних з обмеженим доступом, зниження ризиків кіберзагроз, яка дозволяє виявити будь-які спроби перехоплення інформації, контролюючи стан квантової системи, адже сам факт спостереження за такими системами призводить до зміни стану їх квантових частинок;

– системи зв'язку з автоматичним шифруванням, які забезпечують надійний захист даних та конфіденційність комунікацій в умовах зростаючої мобільності та розвитку нових технологій;

– системи з малою помітністю (Low Probability of Intercept, LPI) для забезпечення безпечної та конфіденційної передачі даних, особливо в військовій сфері за рахунок своїх технічних характеристик, які роблять їх майже нездатними до виявлення стандартними радіоприймачами;

– мережі типу Mesh Network для автономного обміну даними, які не мають єдиного центрального вузла, кожен пристрій у мережі може спілкуватися безпосередньо з будь-яким іншим пристроєм, а оптимальні маршрути для передачі даних визначаються такими мережами автоматично з урахуванням, в тому числі, поломок або перешкод;

– побудова мережевих архітектур зв'язку типу FANET (Flying Ad-Hoc Networks) між дронами та наземними пунктами управління, які дозволяють підвищити ефективність, покращити якість, зменшити втрати даних, оптимізувати розподіл ресурсів, забезпечити зв'язок у віддалених районах, використовувати дрони для

інспекції інфраструктури, моніторингу та доставки вантажів в небезпечних умовах, зменшуючи ризики для людей.

2. Подальший розвиток, з урахуванням сучасних реалій, радіоелектронної розвідки (РЕР) та радіоелектронної боротьби (РЕБ):

– автоматизація управління системами РЕБ та РЕР з можливістю аналітики великих масивів радіоданих для прогнозування загроз, інтеграція штучного інтелекту, створення когнітивних радіосистем для автоматичного аналізу сигналів в системах РЕР;

– створення мобільних комплексів РЕБ для придушення зв'язку противника самонавчальних систем, які адаптуються до радіоелектронного середовища в реальному часі;

– розробка систем раннього виявлення атак дронів та радіоперехоплення, комплексів активного захисту від високоточного озброєння, перешкоджання наведенню боєприпасів на радіо- та лазерних каналах.

3. Продовження освоєння міліметрового діапазону хвиль та 5G технології:

– використання 5G для забезпечення надійного, широкосмугового зв'язку на полі бою;

– використання радарів міліметрового діапазону для високоточних систем виявлення цілей.

4. Використання для сучасних радіолокаційних систем:

– радарів з активними фазованими антеннними решітками (Active Electronically Scanned Array, AESA);

– пасивних радарів для виявлення цілей без випромінювання власного сигналу.

5. Підвищення енергетичної автономності:

– використання енергоефективних технологій для забезпечення роботи радіоелектронних систем;

– інтеграція з джерелами альтернативної енергії.

Розвиток цих напрямів дозволить суттєво підвищити ефективність силових структур та їхню спроможність діяти в умовах сучасних загроз.

Фактом успішного розвитку, наприклад систем РЕБ, в Україні служить станція «Покрова», існування якої було офіційно анонсовано наприкінці 2023 року. «Покрова» діє за методом GPS-спуфінгу проти безпілотників типу «Shahed-131/136».

Наприкінці 2023 року в межах проєкту Brave1 українські розробники представили мобільний комплекс пеленгаторів ETEP, який дозоляє виявляти ворожі сигнали радіостанцій, дронів та РЕБ, ефективніше використовувати власні безпілотні системи, формуючі більш безпечні маршрути.

Нещодавно був анонсований проект «Атлас», що розробляється в Україні компанією-виробником Kvertus. Зазначена система передбачає комбіноване використання системи РЕР «Азимут» та системи РЕБ «Міраж». Основне призначення «Атлас» масштабний захист військ та військових об'єктів від дронів противника уздовж лінії фронту. При цьому система «Міраж» це мобільний, а «Атлас» – мережевий комплекс із стаціонарними та мобільними вузлами. Система РЕР «Азимут» призначається для виявлення та аналізу радіосигналів, які випромінюються або приймаються БпЛА. Після виявлення сигналу «Азимут» проводить аналіз сигналу та його джерела, і передає інформацію на систему РЕБ «Міраж» для подальшого подавлення.

В 2025 році командувач Сил безпілотних систем під час інтерв'ю заявив про близьку перспективу знищення ударних дронів за допомогою українського лазерного комплексу «Тризуб». Зазначений комплекс має ефективно збивати «шахеди» та розвідувальні дрони.

Колектив Наукового центру Повітряних Сил Харківського національного університету імені Івана Кожедуба приймає активну участь в дослідженні, аналізі,

оцінці та розробці технічних рішень, спрямованих на удосконалення існуючих та створення нових зразків радіотехнічних систем озброєння, актуальність яких постійно зростає в умовах динамічних змін в способах та методах застосування противником засобів повітряного нападу, удосконалення його власних радіотехнічних систем.

Серед напрямків досліджень Наукового центру Повітряних Сил:

– удосконалення систем РЕБ, в тому числі апаратури для спуфінгу, інтегрування з системами виявлення, цілевказання та відображення інформації для ефективної боротьби з системами наведення засобів повітряного нападу противника, які використовують GPS-системи поєднанні з інерційними системами наведення в комбінації з апаратурою подавлення перешкод, орієнтованою на істотне зниження ефективності систем РЕБ України;

– розробка компактних засобів виявлення дронів противника для своєчасного та автоматизованого попередження про небезпеку, активації засобів ураження, як елементів, що реалізують активний методу захисту військової техніки;

– розробка засобів протиповітряної оборони та способів їх застосування з метою фізичного знищення або максимальної нейтралізації небезпеки від засобів повітряного нападу противника до досягнення ними цілі,

– розробка інноваційних зразків озброєння на нових фізичних принципах (надпотужних НВЧ генераторів, лазерної зброї і т.ін.).

УДК 623.55.02

Малюк В.Г.

ВПЛИВ ПАРАМЕТРІВ МОДЕЛІ АКТИВНОГО РАДІОМАСКУВАННЯ КАНАЛУ ЗВ’ЯЗКУ VHF/UHF ДІАПАЗОНУ НА ОБЛАСТЬ РОЗМІЩЕННЯ ГЕНЕРАТОРА РАДІОПЕРЕШКОД

Сучасні засоби радіоконтролю забезпечують високоефективне сканування, перехоплення сигналів, їх виявлення та аналіз, на підставі чого дається оцінка дій і намірів противника. Це призводить до необхідності зниження ефективності засобів радіоспостереження за допомогою активних і пасивних засобів радіоелектронної боротьби [1, 2, 3]. Одним із пасивних способів зниження ефективності радіоспостереження є розрахунок зони електромагнітної доступності (ЕМД) систем мобільного радіозв’язку за межами якої потужність сигналу передавача недостатня для прийому радіостанцією спостереження противника. Якщо такий приймач знаходиться в зоні ЕМД, то можна застосувати активне придушення корисного радіосигналу в місці розташування радіоприймача спостереження противника шляхом розміщення джерела навмисних радіоперешкод. При цьому робота такого спеціального генератора радіоперешкод повинна забезпечувати дотримання умов електромагнітної сумісності (ЕМС) та засобів його радіообміну.

У роботі [1] запропоновано простий і ефективний спосіб визначення меж зони можливого розміщення генератора радіоперешкод для захисту засобів мобільного радіозв'язку UHF/VHF діапазону від прослуховування радіоприймачем противника. Методика враховує наявність зон ЕМД систем мобільного радіозв'язку та радіус дії генератора радіоперешкод.

Схема активного захисту каналу мобільного радіозв'язку наведена на рис. 1.

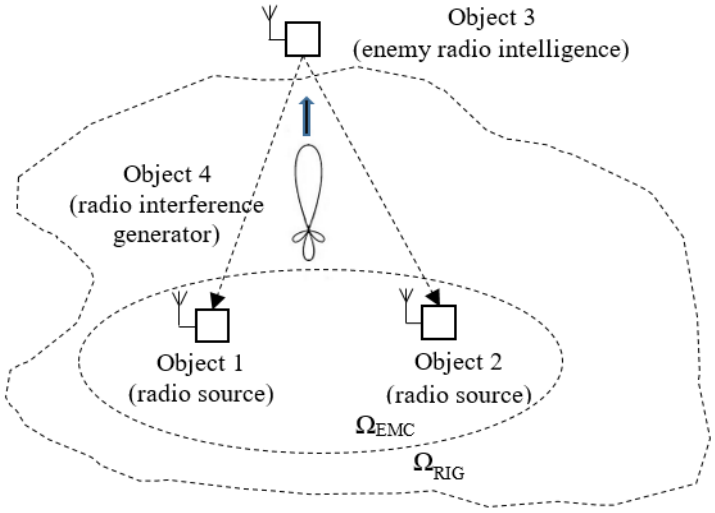


Рисунок 1 – Схема активного захисту каналу мобільного радіозв'язку

Модель містить об'єкти з такими параметрами:

Об'єкти 1 і 2 – наземний засіб радіозв'язку UHF/VHF діапазону, для якого відомі потужність передавача, чутливість приймача та цифрована нормована діаграма спрямованості (ДС).

Об'єкт 3 - радіоприймач наземного спостереження противника, для якого відома, чутливість. Передбачається, що радіоприймач має неспрямований антенний пристрій.

Об'єкт 4 – наземний генератор адитивної радіоперешкоди UHF/VHF діапазону, для якого відомі потужність передавача та цифрована нормована діаграма спрямованості (ДС).

Для забезпечення активного захисту каналу мобільного радіозв'язку у [1] розраховується зона можливого розміщення генератора радіоперешкод Ω_E, з якої виключається область Ω_{EMC}, де не виконуються умови ЕМС.

Метою даної роботи є дослідження пливу таких параметрів моделі активного радіомаскування, як частота і потужність генератора радіоперешкод на розміри зони розміщення Ω_E.

Розрахунки проводились для трьох випадків поєднання типів ДС антен об'єктів 1 і 2 радіоканалу мобільного зв'язку (рис. 1) побудованого на радіозасобах MTP3000 Series [10]:

1) неспрямовані ДС із зонами ЕМД, наведеними на рис. 2a;
2) комбіновані ДС із зонами ЕМД, наведеними на рис. 2b;
3) спрямовані ДС із зонами ЕМД, наведеними на рис. 2c.



a) b) c)

Рисунок 2 – Варіанти поєднання типів ДС антен об'єктів 1 і 2

На рис.2 присутня умовна горизонтальна лінія фронту, що розділяє зону Ω_E на дві частини. Верхня частина Ω_E над лінією фронту, де знаходиться приймач

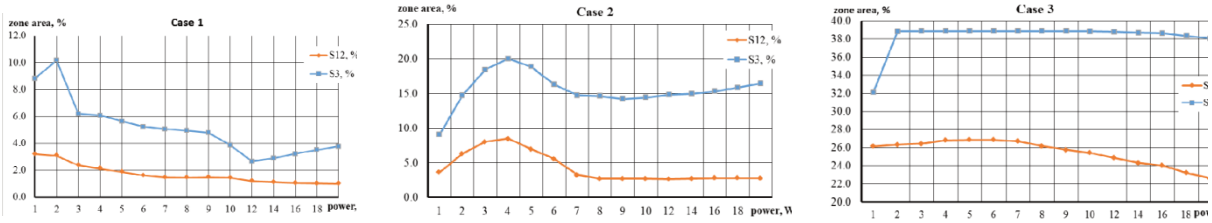
спостереження противника (об’єкт 3), позначається як S_3. Нижня частина Ω_E під лінією фронту, де розташовані об’єкти 1 і 2, позначається як S_{12} і використовується для розміщення генератора радіоперешкод з точки зору безпеки.

Випадок 1 (рис. 3a). Площа зони S_{12} становить 3,2 % від усієї площі оперативної карти Ω, що в 2,75 рази менше площі S_3 = 8,83 %. При збільшенні потужності генератора в межах від 1 до 20 Вт розмір зони S_3 перевищує площу зони S_3 у 2,8-3,8 рази.

Випадок 2 (рис. 3b). Площа зони S_{12} становить 3,63 % від усієї площі оперативної карти Ω, що в 2,5 рази менше площі S_3 = 9,06 %. При збільшенні потужності генератора в межах від 1 до 20 Вт розмір зони S_3 перевищує площу зони S_3 у 0,6-2,5 рази.

Випадок 3 (рис. 3c). Площа зони Ω_E = 53,44 % від усієї площі операційної карти Ω, а площа S_{12} = 21,32 %, що значно більше розмірів площ у попередніх. При збільшенні потужності генератора в межах від 1 до 20 Вт розмір зони S_3 перевищує площу зони S_3 у 1,2-1,7 разів.

Вплив частоти радіосигналу на форму та розміри зони розміщення. У діапазоні VHF (136...174 MHz) частота радіосигналу не впливає на форму та розміри зони розміщення для всіх випадків 1, 2 та 3 (рис.4a). Для розрахунків у діапазоні UHF (403...527 MHz) отримані наступні результати.



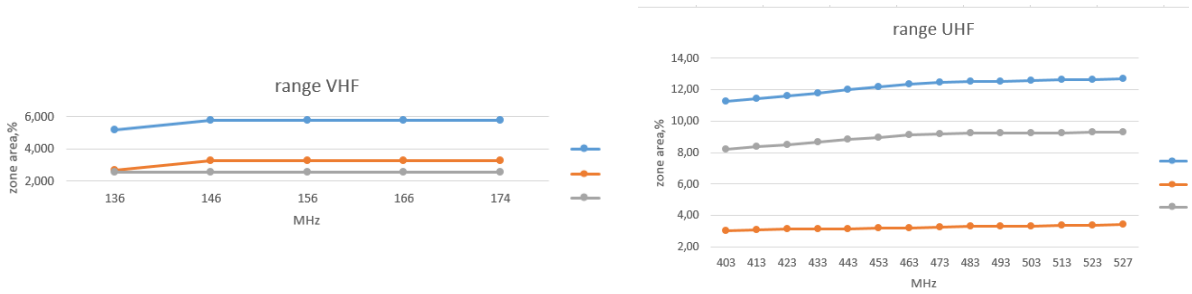
a) b) c)

Рисунок 3 – Залежність розмірів зон S_{12} і S_3 від потужності генератора радіоперешкод

Випадок 1. У міру зростання частоти радіосигналу зменшуються розміри зон ЕМД об'єктів радіоканалу, що призводить до зміни форми та збільшення площі зони розміщення Ω_E на 11% (рис.4б)..

Випадок 2. Відносне збільшення площі зони розміщення Ω_E становить 6%.

Випадок 3. У міру зростання частоти радіосигналу форма зони розміщення практично не зазнає змін. Відносне збільшення площі зони розміщення Ω_E становить 5%.



a) b)

Рисунок 4 – Залежність розмірів зон S_{12} і S_3 від частоти генератора радіоперешкод

Висновки.

1. Найбільш впливовим параметром моделі активного радіомаскування каналу зв'язку VHF/UHF діапазону на область розміщення генератора радіоперешкод є потужність генератора.

2. Найбільш переважний варіант організації роботи радіоканалу, який відкриває широкі можливості для його активного захисту за допомогою генератора радіоперешкод, – це наявність спрямованих антенних пристроїв в обох радіозасобів каналу мобільного зв'язку, взаємно орієнтованих один на одного.

Список використаних джерел

1. V. Maliuk, S. Horielyshev, O. Iohov, O. Novykova, V. Olenchenko, I. Sydorenko, K. Tkachenko. Method of Calculating the Boundaries of the Active Protection Mobile Radio Zone. Advances in Military Technology Vol. 19, No. 1, 2024, pp. 189-204 DOI 10.3849/aimt.01880
2. V. Maliuk, O. Iohov, S. Horielyshev, V. Olenchenko, A. Oleschenko, O. Novykova, K. Tkachenko. Bounds Calculation Method Of Electromagnetic Availability Zone Of Radio Emission Source. *Advances in Military Technology* Vol. 17, No. 2, 2022, pp. 341-356. DOI 10.3849/aimt.01739
3. Iohov O., Maliuk V., Horielyshev S., Tkachenko K., Herasimov S. Development of a Method for Boundary Determination of the Noise-resistant Area of the UHF/VHF Band. Advances in Military Technology, 2020, vol. 15, no. 2. pp. 231-246. DOI 10.3849/aimt.01376

Мартинюк І.М., Погребняк Т.Д., Шматов Є.М.

ЗАСОБИ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ В ОСВІТНЬОМУ ПРОЦЕСІ ПІДГОТОВКИ МАЙБУТНІХ ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

Повномасштабна війна стала величезним викликом для освітньої галузі, з'явились нові фактори впливу, які суттєво вплинули на освітній процес. Але попри всі страшні виклики, ракетні обстріли, людські трагедії, вища освіта в Україні існує і розвивається, в тому числі військова. Пошкодження матеріально-технічної бази та значної кількості приміщень ЗВО (ВВНЗ) України викликають потребу у використанні нових інформаційно-комунікативних технологій у навчанні курсантів (студентів) дистанційно. Сучасні інформаційні технології дають змогу підвищити та вдосконалити ефективність освітнього процесу.

Дослідження результатів використання засобів імітаційного моделювання у військовій сфері вказують на значне підвищення якості освітнього процесу. Відповідно до класифікації НАТО LVC засоби імітаційного моделювання поділяють на три основних види:

– реальні – суб'єкти використовують зразки тренувального озброєння та військової техніки в полігонних умовах обстановки;

– віртуальні – суб'єкти використовують віртуальні зразки одиниць озброєння та військової техніки або їх компоненти;

– конструктивні – комп'ютерні імітаційні програми та системи, у яких відбувається управління віртуальними моделями особового складу, озброєння та військової техніки в умовах динамічної електронної обстановки (бойових дій, навколишнього середовища та ін.). Вибір засобу чи тренажеру (реального, віртуального або конструктивного) залежить від форми підготовки (індивідуальна, колективна), рівнів застосування

(тактичний, оперативний, стратегічний), навчальних цілей тренування, можливостей навчально-матеріальної та технічної бази, локацій підготовки тощо. Закордонний досвід свідчить про результативність комплексного застосування систем засобів імітаційного моделювання під час заходів бойової підготовки військ (сил), освітнього процесу тощо. Розвиток використання таких засобів у підготовці військових фахівців ЗС України пов'язаний із наявністю, доцільністю та результативністю їх запровадження під час індивідуальної та колективної підготовки.

Мультимедійні тренажерні системи і комплекси відіграють особливу роль у процесі дистанційного навчання: використання засобів мультимедіа для повторення, узагальнення та систематизації знань допомагає створити конкретне, наочно-образне уявлення про предмет, явище чи подію, поглиблення знань, формування професійних навичок та компетентностей. Мультимедійні тренажери (симулятори) знайшли широке застосування при навчанні – застосуванні та управлінні складними видами військової техніки та озброєння, в тому числі інженерної техніки. Інтерактивні технології навчання з інженерної техніки сприяють ефективному розвитку у кожного курсанта здібності логічно мислити, розуміти роботу механізмів та агрегатів, вмінню використовувати здобуті знання на практиці, формування таких умінь, як аналіз, порівняння, виділення головного, а також критичне мислення та здатність приймати відповідальні рішення.

Отже використання інноваційних технологій в підготовці майбутніх військовослужбовців забезпечить ЗС України висококваліфікованими кадрами, які зможуть підвищити обороноздатність нашої держави.

Матвєєв Г.А., Казмірчук Р.В.

ДОСВІД ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВИХ ЦІЛЯХ

Якщо період з 2020 по 2021 рр. характеризувався в основному масовим збором та аналізом даних, то початок повномасштабного вторгнення російської федерації на територію України ознаменував епоху «польової обкатки» інтелекті програмних засобів, заснованих на штучному. Сьогодні активно використовуються передові цифрові технології на основі штучного інтелекту, далі – ШІ, що здатні надавати значний вплив на перебіг різних збройних конфліктів, зокрема, російсько-української війни.

Такі програмні інструменти, як Palantir AI, Primer AI та Clearview AI, що застосовуються в рамках російсько-української війни, демонструють трансформацію методів ведення бойових дій. Водночас широкий спектр застосування програмних засобів на основі ШІ знаходиться в «сірій зоні» міжнародного законодавства у сфері інформаційної безпеки, де міжнародне співтовариство тільки починає робити перші кроки у спробі врегулювати безконтрольний збір даних та надати застосуванню нових технологій штучного інтелекту більш прозорого характеру. Відсутність налагодженого міжнародного регуляторного механізму щодо розробників технологій ШІ сприяє наданню приватним організаціям та їх замовникам в особі урядів інформації, що має конфіденційний характер на глобальному рівні, що може бути використано із корисливою метою.

Передові технології дистанційного ведення бою.

Сучасні технології дистанційного ведення бою значною мірою вплинули поточний характер ведення бойових дій. Супутники, БПЛА, кібернетичні можливості та штучний інтелект із самого початку російсько-української війни перебували в центрі особливої уваги іноземних збройних сил та приватних технологічних корпорацій. Так, голова

програми міжнародної безпеки та оборонної політики американської корпорації RAND Джим Мітр заявив, що «ми справді бачимо в режимі реального часу, як розвивається ситуація в Україні, тому існують комерційні компанії, які поспішають на допомогу». При цьому, за словами представника міністерства оборони США Сашка Бейкера, Україна виявила «творчий підхід до інтеграції можливостей» Сполучених Штатів та інших союзників.

Справді, багато в чому завдяки високому ступеню проникнення супутникових технологій на території нашої держави і стала можлива «повномасштабна цифровізація війни», що дозволяє в режимі реального часу здійснювати збір та аналіз даних з метою подальшого прийняття рішень. Невеликі комерційні безпілотники також стали важливою частиною протистояння, дозволяючи військам займатися збором розвідувальної інформації, коригувати вогонь артилерії та авіації або використовувати дрони як барражуючі боєприпаси.

Технології ШІ стали «третьою революцією у озброєнні» після винаходу пороху та ядерної зброї.

Ряд міжнародних експертів відзначає сталу серед західних країн практику: для більшості апаратно-програмних засобів військового призначення на основі ШІ на першому етапі розробляються їхні цивільні прототипи, які надалі адаптуються для військових потреб, що дозволяє суттєво знижувати час та вартість створення військових систем зі штучним інтелектом.

Нижче розглянемо програмні інструменти, які є технологією подвійного призначення, що дозволяє порушувати питання про етичність їх використання у кожному конкретному випадку на прикладі американської компанії, розробника програмного забезпечення аналізу даних для організацій Palantir AI.

Один із яскравих прикладів використання технологій штучного інтелекту в Україні – однойменна комплексна розробка американської корпорації Palantir Technologies Inc., що спеціалізується на розробці програмного забезпечення для аналізу даних та розвідувальної роботи. Ця система включає платформу для інтеграції, управління та аналізу даних з різних джерел з метою обробки великих обсягів інформації та надання інтелектуальних інструментів аналізу даних, які допомагають оператору приймати обґрунтовані рішення.

Одразу після початку повномасштабного вторгнення російської федерації на територію України генеральний директор IT-корпорації Palantir Алекс Карп став першим із представників великого приватного бізнесу, який відвідав офіс президента у Києві з метою запропонувати послуги Palantir Technologies, і з того моменту програмні рішення компанії почали активно впроваджуватись у систему управління Збройними Силами.

Комплекс Palantir AI, що надається на безоплатній основі Україні, має широкий спектр функцій, спрямований насамперед на усунення «туману війни»:

– використання захищеного каналу зв'язку з метою оперативного обміну розвідданими між спецслужбами держав;

– надання доступу до об'єднаної бази супутникових знімків різних постачальників, включаючи Maxar, Airbus, ICEYE, Capella та Національне управління океанічних та атмосферних досліджень США, що надає тепловізійні зображення, що реєструють застосування артилерії. Palantir AI здатний отримувати дані з понад 300 супутників із областю фокусування до 3 метрів;

– аналіз інформації, що дозволяє обчислити найімовірніше розташування військ противника. В результаті кожної дії цифрові дані піддаються оновленню і коригуються системою з метою більш точного прогнозування;

– використання широкосмугового зв'язку, що надає компанія Starlink, яка налічує понад 2,5 тис. супутників на навколоземній орбіті;

– можливість застосування сторонніх програмних засобів.

Зворотний бік ефективності системи Palantir AI — відсутність етичних принципів використання цієї технології у зв'язку з її універсальністю. Ця технологія може бути задіяна в різних сферах громадської діяльності, надаючи оператору можливість застосовувати Palantir AI, зокрема, у порушення міжнародних гуманітарних норм.

Так, у 2019 р. програмне забезпечення Palantir AI використовувалося Імміграційним та митним управлінням США з метою цифрового профілювання іммігрантів у рамках жорсткої політики Дональда Трампа, що багатьма співробітниками Palantir Technologies було сприйнято як зраду місії компанії «працювати заради загального блага».

У результаті корпорація зіткнулася із сильним тиском з боку активістів із захисту цивільних прав, які закликали припинити співпрацю із федеральним управлінням.

Крім того, у 2014 р. в рамках виконання замовлення для Агентства національної безпеки Palantir Technologies розробила систему, що надає співробітникам АНБ доступ до електронних листів, записів телефонних дзвінків, текстових повідомлень та даних з камер спостереження.

Застосування системи Palantir AI викликає побоювання щодо потенційних ризиків, які вона може представляти для міжнародної інформаційної безпеки, зокрема:

– здатність Palantir AI обробляти та аналізувати величезні обсяги даних, включаючи чутливу та особисту інформацію, що загрожує збереженню приватності та конфіденційності даних;

– враховуючи той факт, що Palantir AI часто використовується урядовими організаціями та службами розвідки, існує потенційна ймовірність зловживання функціоналом та порушення громадянських свобод;

– алгоритми машинного навчання, що використовуються Palantir AI для аналізу даних можуть бути упередженими або містити помилки, що може призвести до неправильних висновків та рішень.

Оскільки перехід громадянського суспільства та театрів військових дій у цифрове середовище набуває все більш масового характеру, можна з великою часткою впевненості стверджувати, що ця тенденція продовжить розвиватися в прискорених темпах, а держави продовжуватимуть приділяти значну увагу цим розробкам.

Алгоритмічний збір зображень практично з будь-якої цифрової платформи дозволяє технологічним компаніям скористатися поточною нестабільною геополітичною обстановкою для розширення своєї діяльності, відкинувши конфіденційність персонального та державного значення на другий план.

Розглядаючи застосування технологій штучного інтелекту в ході російсько-Української війни в рамках зазначених програмних інструментів, можна зробити висновок про трансформацію методів ведення бойових дій, що відбувається, завдяки використанню нових комплексних цифрових розробок.

Впровадження програмних засобів на основі штучного інтелекту дозволяє операторам виключати необхідність надсилання даних до спеціалізованого аналітичного центру для подальшої обробки фахівцями, значно скорочуючи час ухвалення рішення на місцях. Особливо примітним є той факт, що історично військові технології створювалися переважно спеціалізованими підприємствами військово-промислового комплексу, але зараз значна частина інструментів випускається компаніями приватного сектору, які раніше не мали ділових відносин з урядами країн у рамках військового співробітництва.

Широкий спектр застосування програмних засобів на основі ШІ знаходиться в «сірій зоні» міжнародного законодавства у сфері інформаційної безпеки, де міжнародне співтовариство лише починає робити перші кроки у спробі врегулювати безконтрольний збір даних та надати застосуванню нових технологій штучного інтелекту більш прозорий характер. Відсутність налагодженого міжнародного регуляторного механізму щодо розробників технологій ШІ сприяє наданню приватним організаціям та їх замовникам в особі урядів інформації, що має конфіденційний

характер на глобальному рівні, що може що може бути використано із корисливою метою.

Так, 18 липня 2023 р., виступаючи на першому в історії засіданні Ради Безпеки ООН на тему штучного інтелекту, Генеральний секретар ООН Антоніу Гутерріш закликав міжнародне співтовариство терміново вжити заходів для контролю за розвитком цієї «незвичайної технології» та створити на базі ООН орган, який міг би сформулювати глобальний союз. Він зазначив, що і військові, і невоєнні варіанти застосування штучного інтелекту можуть мати серйозні наслідки для глобального миру та безпеки. Він також попередив, що застосування ШІ з метою вчинення тероризму, злочинів та кібератак матиме вкрай серйозні наслідки для глобальної безпеки.

Медовкін В.В., Дядюн С.В.

ДОСЛІДЖЕННЯ БЛОКЧЕЙН-РІШЕНЬ ДЛЯ ПРОЗОРОГО УПРАВЛІННЯ ФІНАНСАМИ

Сучасна фінансова система стикається з низкою проблем, пов'язаних із недостатньою прозорістю операцій, високими транзакційними витратами і вразливістю централізованих систем. Блокчейн-технології пропонують революційний підхід до вирішення цих проблем, забезпечуючи незмінність записів, децентралізацію та автоматизацію процесів за допомогою смарт-контрактів.

Дане дослідження спрямоване на комплексний аналіз потенціалу блокчейн-технологій у сфері фінансового управління з акцентом на забезпечення прозорості, безпеки та ефективності операцій. Актуальність теми зумовлена зростаючим інтересом до децентралізованих фінансових систем як з боку ринку, так і з боку регуляторів, при цьому існує нестача науково обґрунтованих підходів до оцінювання їх реальної ефективності. Сучасна фінансова система стикається з низкою проблем, включно з високими транзакційними витратами, недостатньою прозорістю операцій і вразливістю централізованих систем до різних видів атак. Блокчейн-технологія пропонує інноваційний підхід до вирішення цих проблем завдяки своїм фундаментальним властивостям: децентралізації, незмінності записів і можливості виконання самовиконуваних смарт-контрактів. У даній роботі проведено порівняльний аналіз різних блокчейн-платформ (Ethereum, Solana, Polygon, Hyperledger), досліджено особливості функціонування смарт-контрактів у фінансовій сфері, а також систематизовано наявні рішення на основі технології розподіленого реєстру.

Практична значущість даної роботи полягає у формуванні рекомендацій щодо вибору оптимальних блокчейн-рішень для різних завдань фінансового менеджменту, а також у розробці методології оцінки ефективності таких систем. Дослідження дають змогу визначити найперспективніші напрями розвитку блокчейн-технологій у фінансовому секторі та виявити ключові бар'єри, що перешкоджають їх широкому впровадженню. Особливий акцент зроблено на аналізі можливостей інтеграції блокчейн-рішень з наявними фінансовими системами та сервісами, що являє собою одне з найскладніших завдань при впровадженні цієї технології. Розглянуті питання енергоефективності різних блокчейн-платформ, що особливо актуально в контексті глобальних екологічних цілей. Результати роботи можуть становити інтерес як для фінансових організацій, що розглядають можливість впровадження блокчейн-рішень, так і для розробників подібних систем, а також для регуляторних органів, зацікавлених у формуванні ефективних механізмів контролю за новими фінансовими технологіями.

В процесі проведення дослідження виконано такі задачі:

– проведено теоретичний аналіз функціонування різних блокчейн-платформ у контексті фінансового управління;

– систематизовано та класифіковано наявні блокчейн-рішення для управління фінансами;

– виявлено ключові проблеми та обмеження застосування блокчейн-технологій у фінансовій сфері;

– досліджено регуляторні аспекти та питання відповідності блокчейн-рішень нормативним вимогам;

– розроблено систему критеріїв і метрик для оцінки ефективності блокчейн-рішень у сфері фінансового управління;

– сформовано прогноз розвитку блокчейн-технологій у фінансовому секторі та рекомендації щодо їх впровадження.

Основні результати дослідження:

– виконана комплексна класифікація наявних блокчейн-рішень для фінансового управління;

– виявлено ключові переваги і обмеження різних блокчейн-платформ:

1. Ethereum: гнучкість у розробці смарт-контрактів, але висока вартість транзакцій;
2. Solana: висока швидкість транзакцій, але централізована модель валідаторів;
3. Polygon: масштабованість та низькі комісії, але залежність від мережі Ethereum;
4. Hyperledger: висока безпека та можливість приватного управління, але відсутність відкритої екосистеми;

– розроблено систему метрик для оцінювання ефективності блокчейн-рішень, включаючи швидкість обробки транзакцій, енергоефективність, безпеку даних та відповідність регуляторним вимогам;

– сформовано прогноз розвитку блокчейн-технологій у фінансовому секторі, зокрема активний розвиток CBDC (центральних банківських цифрових валют) та інтеграцію DeFi-рішень у традиційні фінансові інститути;

– зроблено рекомендації щодо подолання бар'єрів впровадження блокчейн-рішень у фінансові системи, включаючи вдосконалення регуляторних механізмів та підвищення рівня довіри до технології серед користувачів.

Дане дослідження робить внесок у розуміння потенціалу та обмежень блокчейн-технологій у сфері фінансового управління. Результати роботи можуть бути використані фінансовими інститутами, розробниками блокчейн-рішень, а також регуляторними органами для формування ефективних стратегій впровадження та регулювання блокчейн-систем у фінансовому секторі.

Метешкін К.О., Шевченко В.А., Маслій Л.О.

МОДЕЛЮВАННЯ ДАНИХ І ЗНАНЬ У КОНЦЕПЦІЇ КОЛЕКТИВНОГО РОЗУМУ В.І. ВЕРНАДСЬКОГО

Вчення академіка В.І. Вернадського про еволюційний розвиток біосфери Землі на даний час актуальне як ніколи, у зв’язку з бойовими діями на території України. У своєму вченні В.І. Вернадський називає людство геологічною силою, яка має значний вплив на природу, тобто на біосферу Землі. Він стверджує, що біосфера неспроможна досягти стану ноосфери, доки на Землі відбуваються війни. Разом з тим, результати науково-технічної революції, зокрема інформаційних технологій та штучного інтелекту, показують, що людство досягло межі створення ноосферного інтелекту. Таке твердження ґрунтується на розвитку теоретико-методологічних засад ноогеоматики, які складають методи, моделі та методики створення, інтелектуальних кадастрових систем. В їх основу покладено результати аналізу Державного земельного кадастру, розглянутого з урахуванням побудови гіпотетичної ноосфери В.І. Вернадського, і

навіть концептуальної моделі центру обробки кадастрової інформації [1,2].

На жаль, багато хто помиляється у розумінні терміну «штучний інтелект», розуміючи при цьому розробку моделей знань у вигляді продукційних правил, семантичних мереж і фреймів. І хоча такі моделі припускають логічний висновок, що можна інтерпретувати як деяку інтелектуальну здатність. На рисунку 1 проілюструємо взаємозв'язок інтелектів, тобто здібності людини чи групи людей вирішувати широке коло задач з різним рівнем узагальнення. Наприклад, інтелект В.І. Вернадського дозволяв вирішувати, як елементарні задачі лише на рівні біохімічних реакцій, так і розробку вчення про еволюційний розвиток біосфери в ноосферу – задача планетарного масштабу.

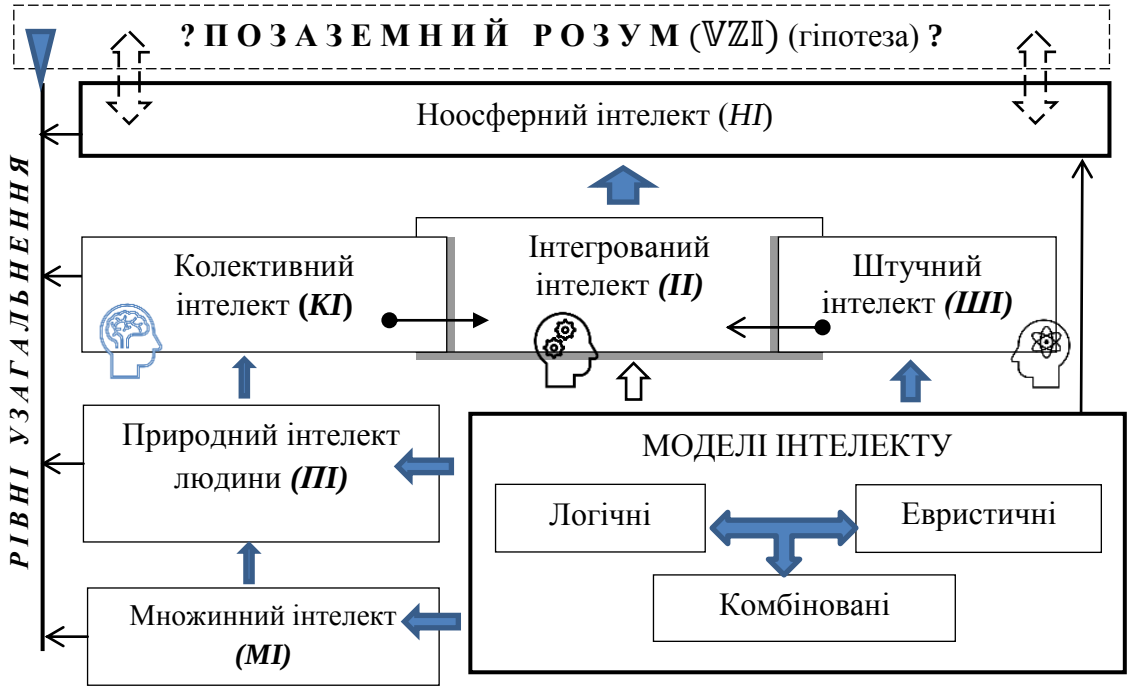


Рисунок 1 – Схема, що ілюструє взаємозв'язок інтелекту на різних рівнях його узагальнення

Ієрархію людського інтелекту за В.І. Вернадським (НІ) визначимо як сукупність множинного інтелекту (МІ) [3], природного інтелекту людини (ПІ), колективного інтелекту (КІ), інтегрованого інтелекту (ІІ) та штучного інтелекту (ШІ), (ІІ+ШІ), згідно формули:

$$\Big(\Big(\big((\text{МІ} \subset (\text{ЕІ})\big) \subset \text{КІ}\Big)\Big) \subset \text{НІ}\Big) \Leftrightarrow \mathbb{VZI}, \qquad (1)$$

$$MI = \{\rho_i\},\ \text{i} = \overline{1,9}.$$

Різні варіанти інтелектуальних здібностей можна записати, використовуючи або формалізм Декарта:

$$MI^1 \supseteq (\rho_1 \times \rho_2),$$
$$MI^2 \supseteq (\rho_1 \times \rho_2 \times \rho_3),$$
$$\dots$$
$$MI^9 \supseteq (\rho_1 \times \rho_2 \times \rho_3 \times \dots \times \rho_9), \qquad (2)$$

або використовуючи закон композиції на підмножинах башти множин:

$$MI = \left(\left(\left(\left(\left(\left(\left((\rho_1 \top \rho_2) \top \rho_3\right) \top \rho_4\right) \top \rho_5\right) \top \rho_6\right) \top \rho_7\right) \top \rho_8\right) \top \rho_9\right), \quad (3)$$

де $(\rho_1)-$ натуралістичний музичний, $(\rho_2)-$ логіко-математичний, $(\rho_3)-$ лінгвістично-вербальний, $(\rho_4)-$ екзистенційний, $(\rho_5)-$ міжособистісний, $(\rho_6)-$ внутрішньо-особистісний, $(\rho_7)-$ тілесно-кінестетичний, $(\rho_8)-$ візуально-просторовий(ρ_9).

На рисунку 1 абревіатурою $\mathbb{VZI}$ позначений позаземний розум, який необхідно розуміти як гіпотезу, сформульовану в теорії палеоконтактів [4].

Високий рівень узагальнення даних та знань обумовлює складність створення ноосферного інтелекту. Якщо у відомих інтелектуальних системах, таких як експертні системи, системи підтримки прийняття рішень та інші при побудові баз даних та знань використовуються відомі моделі, такі як реляційні, ієрархічні, мережеві тощо, то моделі даних, що використовуються на високому рівні узагальнення, повинні представлятися кластерами, які мають нечітку структуру. Відомі моделі знань, такі як продукційні правила повинні бути на високому рівні узагальнення системи таких правил. Натомість, моделі знань, засновані на семантичних мережах мають бути їх ієрархією, тобто. ієрархічними семантичними мережами фрагмент, яких показаний рисунку 2. Особливість таких мереж показаних на рисунку, у тому, що кожна вершина (вузол) семантичної мережі має власну структуру. Фреймові структури подання знань позбавлені недоліків, пов'язаних зі складністю подання даних і знань за рахунок використання приєднаних й спеціальних процедур, які у спеціальній літературі називаються «демони». Разом з тим, і цей метод представлення знань не дозволяє повною мірою реалізувати ноосферний інтелект, створення якого вимагає великої кількості даних (інформації), а також попередньої побудови моделей, що відображають ті чи інші сторони або властивості об'єктів, процесів та явищ.

Тому пропонується при створенні ноосферного інтелекту на нижньому рівні його ієрархії, використовувати традиційні методи та моделі представлення даних та знань. Отримані результати, як вихідні дані, використовувати на черговому етапі моделювання, інтерпретуючи при цьому високий рівень узагальнення. Зауважимо, що величезна кількість процесів та явищ, які відбуваються на Землі, є складними, слабоструктурованими, розмитими (нечіткими) різного ступеня достовірності тощо.

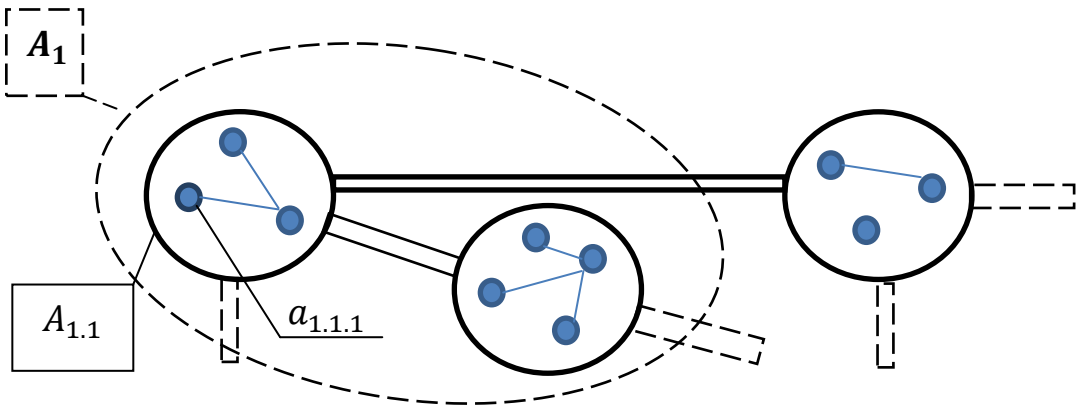


Рисунок 2 – Фрагмент структури ієрархічної семантичної мережі

Ці обставини зумовлюють використання при моделюванні методів і теорій метаматематики таких формалізмів, як категорії, функтори, конуси морфізмів тощо. Даний математичний апарат дозволяє не лише вивчати процеси земельного адміністрування, як це показано у дисертації [5], але й досліджувати та будувати

нейронні мережі різних унікальних конструкцій, які могли б вирішувати задачі та проблеми у різних предметних галузях.

Список використаних джерел

1. Маслій Л.О., Метешкін К.О., Кухар М.А. Категорна модель центру обробки кадастрової інформації // Автомобільні дороги і дорожнє будівництво. 2024. Випуск 116. Частина 2. С. 104–114.
2. Метешкін К.О., Пілічева М.О, Маслій Л.О. Державний земельний кадастр у ноосферній концепції В. І. Вернадського // Комунальне господарство міст. Серія: Технічні науки та архітектура. – № 173. – Том 6. – 2022. – С. 86-90.
3. Gardner Howard E. Multiple Intelligences: The Theory in Practice. Basic Books, 1993. 320 p.
4. Вікіпедія Вільна енциклопедія : палеоконтакти. URL: https://uk.wikipedia.org /wiki/%D0%9F%D0%B0%D0%BB%D0%B5%D0%BE%D0%BA%D0%BE%D0%BD%D1%82%D0%B0%D0%BA%D1%82 (дата звернення: 17.02.2025)
5. Кухар М.А. Моделі комп'ютерної підтримки прийняття рішень системи земельних відносин в Україні : дис. … канд. техн. наук : 05.13.06. Харків, 2018. 155 с.

Мокоївець В.І., Бокачов С.В., Томчук О.А., Федоров О.Ю.

ВЗАЄМОДІЯ ЗАСОБІВ АВТОМАТИЗАЦІЇ ПУНКТІВ УПРАВЛІННЯ СУХОПУТНИХ ВІЙСЬК ТА ІНШИХ СКЛАДОВИХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

З поглибленням процесів інформатизації всіх галузей життєдіяльності людства різко розширилися можливості з підвищення ефективності управлінської діяльності. Не залишаються осторонь від процесу автоматизації управлінської діяльності і військові формування сектору безпеки і оборони України, які традиційно були фаворитом апробації на предмет використання новітніх технологій для досягнення мети їх застосування.

Загальний порядок застосування складових частин сектору безпеки і оборони України залежить від особливостей правового режиму, під час якого вони залучаються до виконання завдань. Правовий режим надзвичайного стану передбачає надання військовому командуванню повноважень, необхідних для відвернення загрози та забезпечення безпеки і здоров'я громадян, нормального функціонування органів державної влади та органів місцевого самоврядування. У випадку введення правового режиму воєнного стану, здійснення відповідних заходів покладається безпосередньо на військове командування та військові адміністрації.

Порядок взаємодії військового командування та військових адміністрацій з центральними органами виконавчої влади щодо забезпечення додержання правового режиму воєнного стану, а також оперативного підпорядкування їм органів і підрозділів інших складових сектору безпеки і оборони України визначається Верховним Головнокомандувачем ЗСУ. Старшому військовому командиру надаються повноваження, які необхідні для забезпечення виконання покладених завдань. В цих умовах він може приймати у своє підпорядкування підрозділи (органи) інших складових сектору безпеки і оборони України та здійснювати управління їх службовою і бойовою діяльністю, використовуючи багаторівневу вертикаль військових пунктів управління як базу системи управління угруповання військ (сил), які залучаються до виконання визначених завдань.

Вагомою складовою силового блоку держави є Сухопутні війська Збройних Сил України, які зазвичай складають основу міжвидового, а часто й міжвідомчого,

угруповання військ (сил). Вертикаль пунктів управління загальновійськових формувань утворює організаційну основу забезпечення стійкого управління застосуванням різнорідних сил і засобів. Тому на розвитку матеріальної бази пунктів управління саме Сухопутних військ Збройних Сил України зосереджуються чималі інтелектуальні та матеріальні ресурси держави.

Розуміючи важливість та перспективність забезпечення систем управління військами (силами) сучасними засобами, створеними на основі новітніх інформаційних технологій, військове керівництво держави приділяє значну увагу створенню вітчизняної військової АСУ. Однією із важливих її складових повинна стати АСУ Сухопутних військ Збройних Сил України. Вона повинна функціонувати в єдиному інформаційному середовищі системи керівництва збройними силами і за своїм функціональним призначенням відповідати покладеним на Сухопутні війська завданням та умовам їх виконання.

Будучи самостійною видовою, певною мірою замкнутою системою, АСУ Сухопутних військ повинна легко адаптуватись до загальної структури Збройних Сил України завдяки утвореним вертикалям співпідпорядкованих об'єктів управління. Функціонування відповідних вертикалей повинно регламентуватись ієрархією відповідних ланок управління, для чого в системі повинні чітко виділятись підсистеми оперативно-стратегічного, оперативно-тактичного і тактичного рівнів.

Підсистема оперативно-стратегічного рівня забезпечує зв'язок із стратегічною ланкою військового управління і відповідає за загальне планування і керівництво підготовкою та застосуванням Сухопутних військ. Вона повинна бути сумісна не тільки з елементами системи вищого штабу, але й безперешкодно співпрацювати із АСУ інших видів Збройних Сил України, а також мати можливість поєднуватись із засобами органів управління інших військових формувань та правоохоронних органів.

Рівень оперативно-тактичний покриває інформаційне середовище, яке забезпечує діяльність посадових осіб в ланці оперативне командування – бригада і відповідає за детальне планування і управління з'єднаннями і військовими частинами в ході їх підготовки і безпосереднього застосування. Інформаційні вертикалі, які пронизують горизонталь оперативно-тактичного рівня щільно пов'язують її як із оперативно-стратегічним, так і тактичним рівнями. Крім того, забезпечується сумісність із підрозділами інших видів Збройних Сил України, а також органами і підрозділами інших військових формувань та правоохоронних органів.

Підсистема тактичного рівня є основним компонентом АСУ Сухопутних військ. Вона відповідає за аналітичне забезпечення управлінської діяльності посадових осіб в ланці бригада – батальйон (підрозділ), впритул до окремого вогневого засобу і навіть окремого військовослужбовця. Важливість її полягає в тому, що вона уявляє собою той самий «кінцевик», від якого у всі ланки управління різних рівнів надходить більша частка інформації та відбувається реалізація інтелектуального продукту, створеного з використанням засобів АСУ.

З огляду на те, що керівництво підготовкою і веденням бойових дій з'єднаннями і військовими частинами Сухопутних військ здійснюється з різних пунктів управління, які оснащені локальними комп'ютерними мережами, системами передачі інформації та її захисту, дуже актуально постає питання інформаційної сумісності між собою засобів автоматизації управління всіх рівнів та приналежності. Підґрунтям такої сумісності повинна стати уніфікація і стандартизація типових програмних, технічних та інформаційно-лінгвістичних засобів базових технологій.

Досвід показує, що намагання поєднати в загальну систему вже існуючі різнорідні комплекси і засоби, які створювалися для виконання окремих, часто не пов'язаних між собою завдань, не завжди призводить до позитивного результату, потребує багато часу і вимагає значних фінансових затрат. Альтернативою такому шляху повинен стати

комплексний підхід до створення АСУ Сухопутних військ, інтегрованої в загальну систему управління Збройних Сил України.

З огляду на те, що пункти управління Сухопутних військ у певних умовах правового режиму, що застосовується в Україні або на окремих її територіях, фактично є організаційно-матеріальною основою функціонування системи управління міжвідомчого угруповання військ (сил), засоби автоматизації процесу управління, які використовуються на них, повинні бути здатні взаємодіяти з аналогічними засобами органів управління інших складових сектору безпеки і оборони держави.

Таким чином, ефективність функціонування загальної системи управління угруповання військ (сил) у значній мірі забезпечуватиметься максимальною сумісністю засобів автоматизації процесу управління всієї вертикалі пунктів управління Сухопутних військ Збройних Сил України та інших складових сектору безпеки і оборони держави на основі застосування єдиних інформаційних технологій в управлінській та службово-бойовій діяльності органів управління та військових частин і підрозділів.

УДК 351.74/76

Мордвинцев М.В., Хлєстков О.В.

ОПТИМІЗАЦІЯ ОПЕРАТИВНОЇ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ ЗА ДОПОМОГОЮ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Сучасні системи відеоспостереження відіграють ключову роль у забезпеченні громадської безпеки та підвищенні ефективності роботи правоохоронних органів. Їх впровадження дозволяє здійснювати постійний моніторинг публічних місць, оперативно реагувати на правопорушення та запобігати злочинам. Завдяки технологічному прогресу, відеоспостереження стало невід'ємною частиною стратегії забезпечення правопорядку в багатьох країнах світу.

Досвід держав Європейського Союзу та Сполучених Штатів Америки демонструє, що інтеграція відеоспостереження з аналітичними платформами на основі штучного інтелекту сприяє зниженню рівня злочинності та підвищенню розкриття правопорушень. Такі системи дозволяють автоматично розпізнавати обличчя, номерні знаки транспортних засобів та аналізувати підозрілу поведінку, що забезпечує швидке виявлення та затримання правопорушників. Наприклад, у Лондоні розгалужена мережа камер відеоспостереження допомагає поліції ефективно контролювати ситуацію на вулицях міста та оперативно реагувати на інциденти [1].

Запропонована автоматизована система відеодокументування переміщень об'єктів поєднує відеозаписи з даними геолокації мобільних пристроїв або GPS-навігаторів [2]. Це дозволяє створювати детальні звіти про маршрути пересування осіб чи транспортних засобів, що є надзвичайно корисним під час розслідування злочинів або пошуку зниклих осіб. Такий підхід забезпечує більш точне відтворення подій та допомагає встановити хронологію дій підозрюваних.

Основні компоненти системи включають:

1. **Панорамне відеоспостереження**: забезпечує широкий огляд території для загального моніторингу ситуації. Використання високоякісних камер з широким кутом огляду дозволяє охоплювати великі площі та виявляти потенційні загрози на ранніх етапах.

2. **Цільове відеоспостереження**: фокусується на конкретних об'єктах або особах для детального аналізу. Це може включати використання камер з високою роздільною здатністю та функцією масштабування для отримання чітких зображень підозрюваних

або транспортних засобів.

3. **Індивідуальне відеодокументування**: використовує персональні мобільні камери або IP-камери для збору даних у реальному часі. Такий підхід дозволяє правоохоронцям фіксувати події безпосередньо під час патрулювання або проведення спеціальних операцій, що підвищує прозорість та об'єктивність їхніх дій.

Інтеграція цих компонентів з існуючими базами даних правоохоронних органів та застосування алгоритмів штучного інтелекту дозволяє автоматизувати процеси виявлення та відстеження підозрілих осіб, що значно підвищує ефективність оперативної роботи. Наприклад, система може автоматично порівнювати обличчя, зафіксовані на камерах, з базою даних розшукуваних осіб та негайно повідомляти відповідні служби у разі збігу.

Впровадження таких систем також сприяє підвищенню довіри громадськості до правоохоронних органів. Прозорість дій поліції, забезпечена відеозаписами, допомагає уникати неправомірних звинувачень та покращує взаємодію між населенням та правоохоронцями. Крім того, наявність камер відеоспостереження діє як стримуючий фактор для потенційних правопорушників, оскільки підвищує ймовірність їх виявлення та затримання.

Висновки. Впровадження сучасних систем відеоспостереження та їх інтеграція з аналітичними інструментами є ключовим фактором у підвищенні ефективності роботи правоохоронних органів. Це сприяє не лише своєчасному реагуванню на правопорушення, але й їх запобіганню, що в цілому покращує рівень громадської безпеки та довіру населення до правоохоронних структур. Використання передових технологій, таких як штучний інтелект та геолокаційні дані, дозволяє створювати комплексні системи моніторингу, які забезпечують більш глибокий аналіз ситуацій та підтримують прийняття обґрунтованих рішень у сфері забезпечення правопорядку.

Список використаних джерел

1. Жадан, Д.О., Мордвинцев, М.В. і Пашнєв, Д.В. (2024) «Відстеження протиправних дій за допомогою систем відеоспостереження: огляд сучасного стану досліджень», Право і безпека, 92(1), с. 78-89. doi: 10.32631/pb.2024.1.07.
2. Спосіб відеодокументування переміщень об'єкта за допомогою системи відеофіксації: пат. 73635 Україна: МПК12 G08G1/00 № 201209091; заявл. 24.07.2012; опубл. 25.09.2012, Бюл. № 18. 4 с.

УДК 004.03/04

Нелінь Д.П., Максюта Д.В., Книш Д.В.

АНАЛІЗ ПЕРСПЕКТИВ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ В СЛУЖБОВІЙ ДІЯЛЬНОСТІ СИЛОВИХ СТРУКТУР

Потенціал розвитку електронних комунікаційних мереж для силових структур є значним як в Україні, так і на міжнародному рівні. Основні напрями розвитку включають:

– покращення стійкості мережі – розробка технологій та інфраструктури, які забезпечують надійний зв’язок навіть в умовах атаки або руйнування інфраструктури;

– інтеграція новітніх технологій – впровадження новітніх радіотехнологій та гігабітного підключення для забезпечення широкосмугового доступу;

– міжнародне співробітництво – підтримка міжнародних проектів та технічної допомоги для покращення інфраструктури;

– підвищення інституційної спроможності – розвиток регуляторного середовища та інституційних можливостей для ефективного управління електронними комунікаціями.

Ці заходи спрямовані на забезпечення безперебійного зв’язку, підвищення ефективності силових структур та покращення загальної безпеки.

Як відомо найбільш поширеними прикладами електронних комунікаційних мереж, що використовуються, в тому числі, в службовій діяльності силових структур є:

– електронна пошта (Email) – використовується для офіційного листування, обміну інформацією між підрозділами та іншими організаціями, а також для надсилання важливих документів та звітів;

– месенджери – дозволяють швидко обмінюватися інформацією, координувати дії під час оперативних заходів, надсилати текстові повідомлення, фото та відео. Приклади: Telegram, Signal (з високим рівнем безпеки);

– соціальні мережі – використовуються для комунікації з громадськістю, поширення інформації про розшукові заходи, а також для збору інформації від громадян. Платформи як Facebook та Twitter можуть бути корисними для інформування громадськості та отримання зворотного зв'язку;

– відеоконференції – допомагають проводити наради, обговорення, тренінги та координаційні зустрічі без необхідності фізичної присутності. Zoom, Microsoft Teams та Google Meet використовуються для відеоконференцій;

– блоги та форуми – використовуються для обговорення професійних тем, обміну досвідом, вирішення питань та отримання консультацій від колег з інших регіонів чи країн;

– хмарні сервіси – забезпечують безпечне зберігання та обмін файлами, дозволяють спільно працювати над документами в реальному часі. Google Drive, Dropbox та OneDrive можуть використовуватися для зберігання доказів, звітів та інших важливих файлів;

– електронні платіжні системи – можуть використовуватися для управління бюджетами, здійснення закупівель та інших фінансових операцій в онлайн-режимі.

Використання цих систем, серед іншого, на мобільних телефонах допомагає оптимізувати робочі процеси, підвищує оперативність та точність дій, а також покращує комунікацію та співпрацю як всередині силових структур, так і з зовнішніми партнерами. В Україні існує кілька законодавчих актів, які регулюють використання мобільних телефонів силовими структурами. Основні з них включають:

– статут внутрішньої служби Збройних Сил України (стаття 143), який визначає порядок користування мобільними телефонами військовослужбовцями;

– Закон України «Про електронні комунікації» (№ 1089-IX від 16.12.2020), який регулює правові та організаційні основи державної політики у сферах електронних комунікацій;

– Закон України «Про основи кібербезпеки», який забезпечує захист інформаційних систем та даних від кіберзагроз.

Цими законодавчими актами встановлюються, за певних умов, істотні обмеження на використання мобільних телефонів для забезпечення безпеки та захисту важливих даних, які юридично унеможливлюють використання як електронних комунікаційних мереж зокрема, так і мобільних пристроїв взагалі. Додатковою проблемою є той факт, що після тимчасового захоплення деяких регіонів України російські військові перенаправили інтернет-трафік через свої мережі. Це дозволяє їм як моніторити інформацію, так і масово поширювати свою пропаганду.

Тому для вирішення протиріччя між зростаючою необхідністю в використанні комунікаційних мереж та вимогами безпеки уповноваженими службами в Україні вживаються певні заходи. Так, наприклад, Державна служба спеціального зв’язку та захисту інформації України в 2022 році надала рекомендації як безпечніше користуватися зв’язком та мати доступ до месенджерів, соціальних мереж,

українських ЗМІ, в тому числі у тимчасово окупованих районах та на прилеглих до цих районів територіях.

Серед рекомендацій, які є корисними як для силових структур, так і для цивільних є використання VPN-сервісу для приховування власної інтернет-активності, електронної переписки. Доцільним є перехід всіх силових структур на однотипні електронні адреси, наприклад в Збройних Силах України для службової електронної переписки використовуються адреси «*.@post.mil.gov.ua».

Також у 2024 році Міністерство оборони України, враховуючи актуальність питання «цифровізації» певних питань службової діяльності, почало впровадження технології Mobile Device Management для захисту особистих телефонів військових. Технологію називають військовим аналогом App Store чи Play Маркет. Подібні методи підвищення кіберзахисту військовослужбовців використовуються і в армії Сполучених Штатів. Продовженням цього напрямку є впровадження в службову діяльність певної категорії посадових осіб пристроїв для забезпечення захищеного та конфіденційного зв'язку – криптофонів. З появою нових захищених девайсів і гаджетів в Україні з'являється та розвивається спеціалізоване та надзвичайно корисне програмне забезпечення. Прикладом такого програмного забезпечення служить добре відома в підрозділах сил оборони України бойова система управління тактичної ланки «Кропива», створена групою волонтерів «Армія SOS». Зазначена система дозволяє спростити та істотно прискорити певні тактичні розрахунки, автоматизувати окремі завдання з управління на рівні батальйону (дивізіону), роти (батареї), взводу, окремої одиниці техніки, допомагає об'єднувати засоби розвідки, управління та вогневого ураження в єдине інформаційне поле. Як зазначають автори цього проекту, за класифікацію, прийнятою в країнах НАТО, «Кропива» відноситься до систем типу C2 (commandandcontrol). «Кропива» має низку технологічних бонусів для військових як на полі бою, так і під час навчань: доступ до електронної карти місцевості, обмін даними (в тому числі текстовими повідомленнями) з іншими абонентами системи, розв'язання окремих розрахункових завдань, забезпечення взаємодії та передачі даних із засобів розвідки, радарними та звукометричними комплексами в автоматичному режимі.

В Науковому центрі Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба свого часу було розроблено спеціалізоване програмне забезпечення (СПЗ) «Віраж-планшет». Зазначене СПЗ знайшло широке використання як в Повітряних Силах України, так і в інших силових структурах. На даний час «Віраж-планшет» може встановлюватись на пристрої навіть на платформі «Android». Можливості автоматизації процедур контролю, збереження та видачі інформації про повітряну обстановку, відображення переміщення повітряних цілей у реальному часі, передачі інформації за допомогою радіомодемів на відстань до кількох кілометрів обумовили широке поширення СПЗ «Віраж-планшет» як для виконання бойових завдань, так і для навчальних.

Таким чином, електронні комунікаційні мережі для силових структур є критично важливими, адже вони забезпечують швидку та надійну комунікацію між структурними підрозділами, що є ключовим для успішного виконання бойових, спеціальних службових завдань. Аспектами, які підкреслюють вимоги до зв'язку та електронних комунікаційних мереж, зокрема, для силових структур є:

– безпека – використання зашифрованих каналів та спеціальних технологій для захисту від радіоелектронної розвідки;

– ефективність – швидка передача важливих даних та координація дій між підрозділами;

– надійність – забезпечення стабільного зв'язку навіть у важких умовах, таких як зони боїв або віддалені райони;

– технологічний прогрес – впровадження новітніх технологій, таких як Mobile

Device Management, для захисту особистих телефонів військових.

УДК 681.5.015

Ненич Д.О.

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОГО РЕГУЛЯТОРА ТЕМПЕРАТУРИ ДЛЯ ДОСЛІДНИЦЬКИХ ТА ПРОМИСЛОВИХ ЗАСТОСУВАНЬ

Сучасні наукові дослідження та технологічні процеси потребують високоточного контролю температури для забезпечення стабільності експериментальних умов і ефективності промислового обладнання. У доповіді представлено розробку інтелектуального регулятора температури для дослідницьких і промислових застосувань, який забезпечує точне підтримання температурного режиму та можливість лінійного збільшення температури із заданою швидкістю. Запропоноване рішення поєднує сучасні технології зв'язку (Wi-Fi, Bluetooth) для дистанційного керування та моніторингу. Описано технічну реалізацію системи, її можливості та перспективи подальшого розвитку, а також розглянуто архітектуру програмного інтерфейсу для інтеграції з іншими інформаційними системами.

Контроль температури є критично важливим у багатьох наукових та інженерних галузях, зокрема при дослідженні теплофізичних властивостей матеріалів, випробуванні електронних компонентів та керуванні технологічними процесами. Зростаючі вимоги до точності регулювання температури стимулюють розробку нових рішень, що базуються на сучасних електронних компонентах і засобах зв’язку.

Метою роботи є розробка інтелектуального регулятора температури, який забезпечує: точне підтримання заданої температури; можливість програмованої зміни температури; дистанційне керування через Wi-Fi або Bluetooth; модульну архітектуру для легкого розширення функціоналу; інтеграцію з іншими інформаційними системами через API.

Технічна реалізація. Система складається з таких основних компонентів:

– мікроконтролер Arduino UNO - забезпечує обробку даних та підтримку бездротового зв’язку;
– димер на симісторах - дозволяє плавне регулювання потужності нагріву;
– нагрівач великої потужності;
– термопара типу К - забезпечує точні вимірювання температури до +1300 °С;
– модулі Wi-Fi та Bluetooth - забезпечують дистанційне керування та моніторинг.

Програмний інтерфейс. У програмній реалізації системи керування було використано бібліотеку PID_v1, розроблену Бреттом Борегардом [1], для створення об’єкту PID-регулятора. Програмна реалізація створення об’єкту PID-регулятор, запропонована Бреттом Борегардом, передбачає використання об’єкто-орієнтованої парадигми програмування. Програмна частина системи включає наступні компоненти:

– вбудоване програмне забезпечення (Firmware), написане на C/C++ (Arduino IDE);
– реалізацію PID-регулятора для підтримки стабільної температури;
– підтримку протоколів MQTT та HTTP для обміну даними.

Веб-інтерфейс та API:

– використання Node.js (Express) для розробки серверного API;
– RESTful API для налаштування параметрів та отримання даних;
– WebSocket для реального часу моніторингу температури;
– Frontend на React.js для візуалізації даних та керування регулятором.

Мобільний застосунок:

– розробка на Flutter для кросплатформеності (Android/iOS);

– Bluetooth та Wi-Fi керування пристроєм;
– графічний інтерфейс для налаштування та моніторингу.

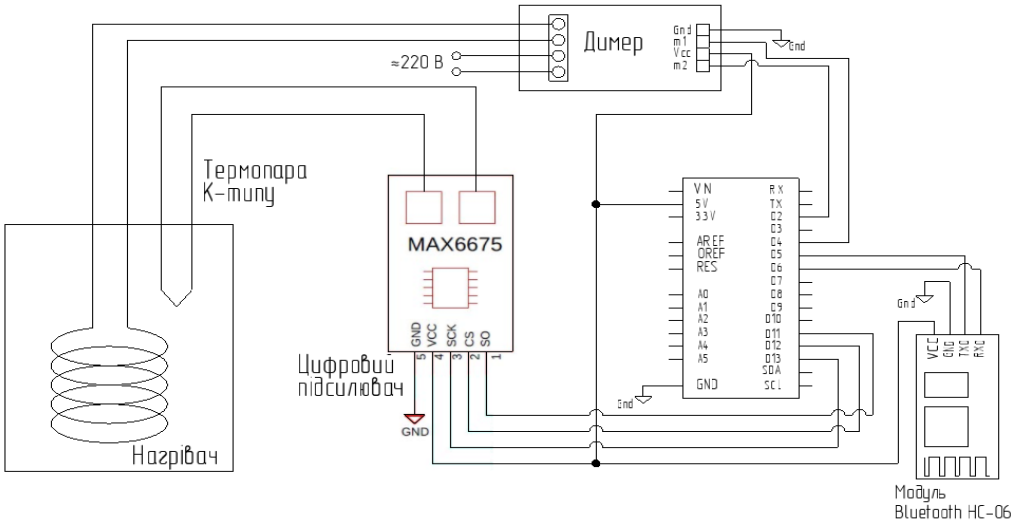


Рисунок 1 – Загальна схема пристрою

Інтеграція з хмарними сервісами:
– підключення до Firebase для збереження логів;
– використання AWS IoT Core або Google Cloud IoT для розширеної аналітики.

Перспективи розвитку. Подальший розвиток проекту включає:
– розширення можливостей програмного забезпечення для точного контролю швидкості нагріву;
– використання алгоритмів машинного навчання для прогнозування оптимальних режимів роботи;
– розробку мобільного застосунку для зручного керування;
– інтеграцію альтернативних засобів зв'язку (LoRa, ZigBee, 5G);
– автоматичне коригування параметрів регулювання на основі історичних даних.

Висновки. Запропонований інтелектуальний регулятор температури є перспективним рішенням для дослідницьких і промислових застосувань. Його модульна архітектура, можливість дистанційного керування та розширюваний програмний інтерфейс роблять систему ефективним інструментом у сфері температурного контролю. Запропонована система забезпечує лінійну зміну керованої величини і може бути застосована для системи керування температури. Інтеграція з хмарними сервісами та використання алгоритмів машинного навчання значно підвищують можливості системи, роблячи її адаптивною до змінних умов експлуатації.

Список використаних джерел

1. Beauregard B. Arduino-PID-Library [Електронний ресурс] / Brett Beauregard – Режим доступу до ресурсу: https://github.com/br3ttb/Arduino-PID-Library.

Нещадін О.В.

ДОСВІД ЗАСТОСУВАННЯ ІНТЕРАКТИВНИХ ТЕХНОЛОГІЙ НАВЧАННЯ ЩОДО ПРИЙНЯТТЯ РІШЕНЬ СПЕЦІАЛІСТАМИ ІНЖЕНЕРНОЇ ПІДТРИМКИ

З початком широкомасштабного вторгнення, після розгортання чисельності сил оборони до теперішнього кількісного складу, гостро постали питання пов'язані з обсягами підготовки значно більшої кількості військ, в тому числі і офіцерів, штабів.

Інженерні бойові операції (дії) є невизначеними та непередбачуваними, є комплексними намаганнями – боротьбою між людською волею протидіючих сторін. Командири стикаються з мислячим та адаптивним противником. Вони ніколи не можуть з певністю передбачити як буде діяти та протидіяти противник, або яким чином розвиватимуться події. Навіть дії їх сил важко передбачити через такі фактори, як, наприклад, людські помилки та наслідки стресу. Офіцери, які розуміють динаміку змін у часі, ураховуючи невизначеність щодо противника та своїх сил, краще пристосовані для прийняття ефективних рішень.

Відповідно є нагальна необхідність використання у підготовці військовослужбовців інтерактивних технологій, особливо під час проведення командно-штабних навчань, що суттєво скорочує час та витрату ресурсів.

Так, у Національній академії Сухопутних військ України імені гетьмана Петра Сагайдачного активно використовуються система імітаційного моделювання бойових дій (ІМБД) на базі програмного забезпечення JCATS та програма ситуаційної обізнаності «DELTA».

Дані продукти дозволяють на високому рівні, швидко і якісно провести аналіз місцевості району бойових дій (АОО – area of operation), району інтересу (АІ – area or interest) та району впливу (АОІ – area of influence), відповідно:

– підготувати оцінку району бойових дій (ЕВА) у вигляді висновків з аналізу місцевості за факторами ОАКОС;

– скласти МСОО – узагальнений об’єднаний оверлей перешкод;

– визначити висоти та зони проведення інженерної розвідки місцевості, противника та об’єктів, оптимальні шляхи для маневру сил, засобів та ділянки місцевості для виконання заходів загальної інженерної підтримки.

У цілому використання програми ситуаційної обізнаності «DELTA» дозволяє: організувати виконання заходів інженерної підтримки з показом зон:

– видимості (невидимості), що можуть бачити наші сили;

– показати танкодоступні ділянки місцевості, що вплине на правильне та ешелоноване планування Системи інженерних загороджень, визначати координати (особливо встановлених загороджень); організувати виконання заходів з фортифікаційного обладнання місцевості (смуги відповідальності) та пунктів управління, підготовки та утриманні рокадних та фронтальних шляхів у смузі відповідальності та визначити місця розташування пунктів польового водопостачання та заготівлі лісоматеріалів (дерев’яних конструкцій).

За допомогою програми ситуаційної обізнаності «DELTA» військовослужбовці дуже швидко відпрацьовують оцінку району бойових дій за усіма факторами, наприклад, зона бойових дій включає райони, окуповані противником, який може поставити під загрозу виконання завдання. Противник у районі АОІ описується за схемою:

– Close-air support – підтримка з повітря;
– Artillery;
– Rotary Wing (Літальні апарати);
– Reserve Forces.

Відпрацювання зони бойових дій за вище вказаною схемою на програмах ситуаційної обізнаності дозволяє візуалізувати отриману інформацію.

Раніше оцінку рельєфу здійснювали вручну по топографічній карті із з’ясуванням певних висот та побудовою ліній видимості (невидимості), що займало час.

Важливим елементом оцінки району бойових дій є складання об’єднаного оверлею перешкод, який передбачає в основному аналіз місцевості за військовими аспектами ОАКОС. У ході оцінкі перешкод (Obstacles) відпрацьовуються покроково оверлеї перешкод: водних перешкод з підйомом шляхів; рослинності та рельєфу (піднімаються контуром зеленого та коричного кольорів відповідно); інфраструктури (населених

пунктів – піднімаються контуром чорного кольору), при об'єднанні (накладанні) яких отримується об'єднаний оверлей перешкод (Combined Obstacle Overlay, COO).

Оцінка району бойових дій за допомогою інтерактивних програм вирішує багато питань планування та організації бойових дій.

Умови спостереження – це умови погоди та місцевості, які дозволяють як своїм військам, так й військам противника, бачити особовий склад, озброєння, військову техніку та ключові аспекти оперативного середовища (відмічаються у програмі).

Ділянки вогневого ураження – це райони, які можна накрити вогнем засобів озброєння з окремо взятої позиції, так само відображаються у програмі ситуаційної обізнаності.

Ділянки вогневого ураження безпосередньо пов'язані із можливостями спостереження.

Умови ведення вогню прямою наводкою – це умови місцевості, які дозволяють своїм військам вести вогонь униз по схилу, при цьому війська та техніка не проецируються на фоні неба зі сторони противника.

Найбільш вигідними позиціями є: бойові гребні передніх схилів; топографічні гребні; природні рубежі та райони, що забезпечують добрий огляд та обстріл підступів до них – усе це досить швидко з'ясовується у програмного продукті «DELTA».

Результатами оцінки району бойових дій є доцільно вибрані вогневі позиції зазвичай на зворотних схилах поблизу топографічного гребня.

При цьому для того, щоб визначити віддалену межу спостереження, необхідно зіставити найбільші висоти панівного рубежу з висотами попереду розташованої місцевості й визначити рубіж, за яким місцевість не проглядається з панівного рубежу, – це і буде гранично віддалена межа спостереження.

З'ясування ключових точок місцевості та характеристик підступів шляхів або імовірно доступних напрямків (avenue of approach – AAs) за допомогою програм ситуаційної обізнаності надалі візуалізує ситуативну схему дій противника або наших дій.

Шляхові підходи (AAs) – це повітряний або наземний маршрут атакуючої сили (підрозділів) заданого розміру (ешелону), що веде до його цілі або до ключової місцевості. Ідентифікація AAs важлива, оскільки маневр, залежить від наявних шляхів. Під час наступальних операцій оцінка AAs призводить до вибору найкращих обраних варіантів згідно мети командира та визначення геопросторів, доступних для дій бойових елементів. Під час опрацювання AAs необхідно враховувати наступальні можливості сил та шляхи, які підтримують рух. Для розробки AAs використовуються результати оцінки перешкод (COO).

Оформлення AAs на МСОО здійснюється через визначення мобільних коридорів, їх категоруванням (за розміром: взвод, рота, батальйон і т.д.) та групуванням мобільних коридорів у форму шляху підступу.

Коридори мобільності (mobility corridors) – це зони, де є можливість рухатись через обмеження місцевістю. Сам коридор мобільності порівняно не містить перешкод і дозволяє військовим силам скористатися принципами масовості та швидкості. Коридори мобільності зазвичай співпадають у напрямку доріг.

У наступі висновки з оцінки шляхів підступу дозволяють визначити найкращий маршрут своїх сил для досягнення цілі, а також шляхи відступу противника (OPFOR – opposing force) або переміщення його резервів.

В обороні необхідно визначити які шляхи сприяють наступу військ противника та напрямки, що підтримують рух своїх резервів.

Аналіз району бойових дій на програмних продуктах «DELTA», «КРОПИВА» дозволяє швидко і раціонально розробляти варіанти дій виконання бойових завдань, визначати ефекти встановлення загороджень.

Особливостями застосування інтерактивних технологій є їх одночасне використання у комплексі.

Навчання військовослужбовців здійснюється одночасно на декілька продуктах програмного забезпечення, при цьому задіються платформа дистанційного навчання MOODLE та БПЛА, за допомогою яких проводиться практичне уточнення прийнятого рішення (рекогносцировка). Відповідно військовослужбовці у режимі реального часу можуть оцінювати обстановку, приймати рішення та віддавати накази через програму «DELTA», використовуючи стрім БПЛА та транслюючи необхідну інформацію через платформу дистанційного навчання MOODLE уточнювати своє рішення, накази, контролювати та коригувати дії відповідного персоналу.

З метою закріплення навчальних матеріалів, розширення світогляду, забезпечення тренованості та бойової злагодженості підрозділів, досягнення необхідного рівня тактичної підготовки командирів і штабів широко використовуються засоби імітаційного моделювання (ЗІМ), військові тренажерні системи (ВТС), від індивідуальних до тактичних.

Таким чином, використання інтерактивних технологій дозволяють в автоматичному режимі виявляти помилкові дії тих, хто навчається, і формувати відповідні рекомендації щодо їх усунення. Надають можливість організувати керований процес вироблення у військовослужбовців стійких навичок бойової роботи, приводить до прийняття ними оптимальних рішень, забезпечує найбільш ефективне застосування зразків ОВТ у різних умовах обстановки.

УДК 004.738

Нікора І.В., Богдановська К.Д.

МОДЕЛІ ОЦІНКИ ПРОПУСКНОЇ ЗДАТНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ ПІД ВПЛИВОМ КІБЕРНЕТИЧНИХ АТАК

Пропускна здатність інформаційно-комунікаційної мережі визначається як ключовий показник, що характеризує її здатність передавати дані від одного вузла до іншого протягом певного часового інтервалу. Пропускна здатність розглядається як об'єм даних, який мережа може обробити та передати, визначений в бітах чи байтах на секунду. це є критично важливим для оцінки ефективності мережі.

Важливо розуміти, що пропускна здатність може бути визначена різними способами, включаючи загальну пропускну здатність мережі та пропускну здатність окремих її компонентів. Зокрема, розглядається пропускна спроможність каналів передачі даних, комутаційних вузлів та інших ключових елементів мережі. Застосування спеціального програмного забезпечення MATLAB дозволяє моделювати різні випадкові процеси, за допомогою статистичних пакетів MATLAB можна обчислити характеристики різних розподілів та їх комбінацій, дозволяє створювати та аналізувати марківських ланцюги за допомогою спеціалізованих функцій, надає потужні засоби для візуалізації результатів аналізу, такі як графіки розподілів, графіки залежностей між величинами тощо. Використання теорії графів є потужним інструментом для моделювання та аналізу систем зі складною структурою взаємозв'язків між її елементами. В контексті аналізу пропускної здатності мережі, граф використовуємо для відображення взаємозв'язків між вузлами та лініями зв'язку.

Модель оцінки резервної пропускної здатності визначає, як ефективно мережа може перерозподіляти свої ресурси та використовувати резервні шляхи під час збоїв або кібератак, враховується швидкість виявлення і реагування на події.

Застосування в контексті кібернетичного впливу дозволяє аналізувати, наскільки швидко та ефективно мережа може відновити свою пропускну здатність після кібератаки, враховуючи резервні маршрути та заходи безпеки.

На основі аналізу ризиків та потенційних загроз розробимо стратегію захисту для нашої інформаційно-комунікаційної мережі, основними принципами цієї стратегії є перевірка і виявлення загроз та реагування на загрози. Етап перевірка та виявлення загроз включає ретельний моніторинг та аналіз активності в мережі з метою виявлення будь-яких потенційних загроз безпеці. Для цього використовуються різноманітні інструменти, включаючи системи виявлення інтрузій, аналіз логів подій та відповідні алгоритми машинного навчання, що дозволяє виявляти незвичайну або підозрілу активність в мережі, таку як несподівані спроби доступу або атаки на вузли. Крім того, системи моніторингу виявляють аномальні патерни з'єднань , які можуть свідчити про кібернетичні загрози, такі як DDoS-атаки або спроби перехоплення даних. Аналіз логів подій дозволяє відслідковувати дії користувачів та виявляти надмірну або підозрілу активність.

Після виявлення загрози настає етап реагування, який включає швидку та ефективну реакцію на потенційну кібернетичну атаку. В залежності від характеру загрози та її впливу на мережу, модель включає методи відключення атакованих вузлів або послаблення їх підключень якщо виявлено, що певний вузол піддається атакам або є джерелом незвичайної активності, його можуть відключити від мережі або обмежити його доступ, і метод швидкого переключення на резервний канал зв'язку якщо пропускна здатність певного каналу зв'язку знижується через атаку або перевантаження, система може автоматично переключитися на резервний канал зв'язку для забезпечення неперервності та збереження пропускної здатності мережі.

УДК 621.396.96

Олексенко О.О., Карлов В.Д., Ковальчук А.О.

ПРОПОЗИЦІЇ ЩОДО СТВОРЕННЯ ТА УДОСКОНАЛЕННЯ СИСТЕМ ДИСТАНЦІЙНОГО НАВЕДЕННЯ ЗАСОБІВ МАЛОКАЛІБЕРНОЇ ЗЕНІТНОЇ АРТИЛЕРІЇ

В задачах автоматизації управління та наведення засобів стрілецького озброєння, зенітної артилерії, та пускових установок ракетної техніки, знайшли широке застосування електромеханічні приводи обертання, які призначені для забезпечення дистанційного автоматичного розвороту вогневого засобу ураження на заданий азимут та кут місця. Однією із задач є дослідження можливості застосування дистанційного керування малокаліберною зенітною артилерією при стрільбі по повітряним і наземним цілям. Наприклад, маючи автоматизовану система збору, обробки, та відображення інформації про повітряну обстановку, її можливо використовувати для цілевказівки та завчасного наведення засобів малокаліберної зенітної артилерії в напрямку на повітряну ціль. Особливо це актуально при використанні засобів малокаліберної зенітної артилерії для боротьби з маловисотними, малорозмірними цілями та цілями, що мають велику швидкість.

Метою проведених досліджень є розробка функціональної структури системи дистанційного керування кутовим положенням засобів малокаліберної зенітної артилерії з осучасненою елементною базою та дослідження якості її функціонування шляхом комп'ютерного моделювання. За участю працівників Харківського національного університету Повітряних Сил імені Івана Кожедуба розроблено декілька варіантів систем дистанційного керування стрілецькою зброєю та засобами

малокаліберної зенітної артилерії. Системи дозволяють дистанційно керувати наведенням на наземну або повітряну ціль та веденням вогню по дротовій лінії чи по радіолінії за допомогою виносного пульту та монітору. Дистанційне керування працює на сучасних мікроконтролерах з відповідним програмним забезпеченням, живлення установок здійснюється автономно, а виконавчими елементами системи є крокові електричні двигуни із зворотнім зв'язком, які здійснюють наведення стволів в горизонтальній та вертикальні площині. Така конструкція дозволяє значно підвищити точність стрільби та дає суттєву економію боєприпасів, і оператор знаходиться в безпечному місці.

В якості сучасних датчиків кута повороту (енкодерів) – електромеханічних пристроїв, за допомогою яких можна визначити положення осі (валу), найбільш прийнятні з точки зору надійності безконтактні абсолютні цифрові енкодери, які бувають оптичні і магнітні. Саме використання сучасних цифрових датчиків кута повороту дозволяє покращити точність вимірювання кутового положення та зменшити фізичні розміри обладнання системи обертання. На заміну класичних електричних двигунів постійного струму запропоновані до використання так звані крокові двигуни, які вже довгий час використовуються в системах позиціонування і також мають певні переваги та простоту технічної реалізації в системах наведення малокаліберної зенітної артилерії. Динамічні та статичні характеристики аналого-цифрової системи обертання в значній мірі визначаються можливостями механічної частини, в першу чергу крокових двигунів, а кількість необхідного обладнання значно зменшується та осучаснюється. Для аналізу якості функціонування електромеханічної системи обертання пропонується використання програмної оболонки SIMULINK пакету прикладних програм MATLAB. Аналіз отриманих результатів дозволяє швидко оцінювати характеристики обертання та змінюючи параметри елементів оцінити їх влив на характеристики обертання.

За результатами проведених досліджень запропоновані осучаснені варіанти функціональних структур аналого-цифрових електромеханічних слідкуючих систем для дистанційного керування азимутальним положенням малокаліберної зенітної артилерії, та реалізовано в експериментальних і дослідних зразках представниками Харківського національного університету Повітряних Сил імені Івана Кожедуба, які вже показали свою ефективність на полі бою.

УДК 004.8: 004.056

Оленченко В.Т.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНЬОМУ ПРОЦЕСІ

Термін «Штучний інтелект» належить англійському математику, логіку і криптографу Алану Тьюрингу. Вперше він його використав у науковій статті під назвою «Обчислювальні машини та інтелект», опублікованій 1950 року у філософському журналі «Mind». В ній Тюрінг запропонував тест для визначення категорії співрозмовника – людина чи комп'ютер. **К**омп'ютер розглядався як система, що наділена інтелектуальними процесами, характерними для інтелекту живої людини – уміння узагальнювати, аналізувати та обробляти інформацію, набиратися досвіду, робити висновки та пропонувати дії.

Інакше кажучи штучний інтелект (ШІ) – це сукупність алгоритмів та інструментів машинного навчання, що спроможні миттєво обробляти інформацію: виявляти її закономірності, формалізувати та оптимізувати її, надавати пропозиції та готові рішення.

Ознаки штучного інтелекту містять пошукові алгоритми мережі інтернет та інші додатки. Однак, з листопаду 2022, з відкриттям доступу до сервісу ChatGPT, ШІ все більше втручається у процеси життєдіяльності людини.

Не оминув ШІ і освітній процес.

На поточний момент, освітяни використовують ШІ для вирішення широкого кола завдань:

– підготовку планів та методичних розробок для проведення занять, а також розроблення на їх основі презентацій та тестів різного рівня складності для перевірки знань;

– перевірки – аналізу та оцінювання – звітних матеріалів здобувачів освіти;

– підготовку індивідуальних завдань за профілем та, за необхідності, їх персоналізацію;

– розроблення вихідних даних та сценаріїв проведення практичних занять;

– генерування ідей, пошук креативних та цікавих підходів до навчання та інших.

Усе це спрямоване на стимуляцію пізнавального процесу у здобувачів освіти.

Разом з тим спостерігаються і негативні наслідки використання ШІ:

– в процесі відпрацювання поставлених завдань (у тому числі тестів) стає проблематичним визначення рівня знань здобувачів освіти;

– процес прийняття рішення повністю перекладається на ШІ і в критичній ситуації (без доступу до сервісів ШІ) ті хто навчаються не можуть або бояться взяти на себе відповідальність;

– у здобувачів освіти зникає потреба у підвищенні свого рівня знань – адже є прямий доступ до бази даних ШІ.

Висновок. При всій привабливості застосування ШІ в освітньому процесі, як то оптимізація часу на підготовку до занять, креативності і таке інше, має і ряд істотних вад його використання. Необхідно дотримуватися балансу між використанням ШІ у процесі навчання і традиційних методів освіти.

Паламарчук Н.А., Процюк Ю.О., Мартинюк В.В., Кугот О.Л.

АНАЛІЗ АЛГОРИТМІВ (МЕТОДІВ) РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ, ЯКІ БАЗУЮТЬСЯ НА КОМП'ЮТЕРНОМУ БАЧЕННІ ДЛЯ ІДЕНТИФІКАЦІЇ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

З кожним днем ведення бойових дій все більше території України стає забрудненою вибухонебезпечними предметами (ВНП), на розмінування якої підуть десятиліття. Використання новітніх технологій розмінування, таких як механізоване розмінування, роботизовані системи (комплекси), безпілотні літальні апарати (БпЛА) з різними датчиками типів для виявлення та знешкодження ВНП є дуже актуальним.

Ці технології дозволяють здійснювати віддалене управління засобами розмінування та убезпечують операторів від випадкового спрацювання ВНП, але не виключають їхньої присутності у роботі цих систем. Для вирішення задач з ідентифікації зображень ВНП, БпЛА або інші роботизовані системи доцільно обладнувати відповідними пристроями на кшталт камери з високою роздільною здатністю, тепловізора, автоматизованої системи зйомки тощо, які б дозволили з певною ймовірністю розпізнавати виявлені об'єкти за їхніми характерними локальними ознаками (формою/зображенню, матеріалом виготовлення корпусу, температурою корпусу, тощо) та класифікувати їх без участі оператора (людини) [1, 2].

Проведений аналіз сучасних та перспективних технологій робототехніки, їх реалізація з використанням штучного інтелекту, надає можливість застосовувати дескриптори особливих (ключових, контрольних) точок зображення на основі навчання

нейронної мережі з описом методів SIFT, SURF, ORB та BRISK. Одним з найбільш розвинених алгоритмів для глибинного навчання з ідентифікацією зображень та відео є згорткові нейронні мережі (Convolutional Neural Network, CNN), які адаптовані для обробки зображень і спроєктовані з припущенням, що на вхід подається еталонне зображення. На відміну від стандартних нейронних мереж, шари у згорткових нейронних мережах є тривимірними, а нейрони одного шару зв'язані тільки з певною областю наступного шару. Це дозволяє вибудувати певні характеристики в архітектуру, спрямовану на поліпшення класифікації зображень.

Структурні методи розпізнавання об'єктів, що засновані на локальних ознаках зображення, набули популярності та широко застосовуються в сучасних системах комп'ютерного зору. Вони базуються на визначенні множини особливих (контрольних) точок (далі – контрольні точки) та їхньому описові у вигляді числового чи бінарного вектора – дескриптора, який відображає властивості зображення для локальних околиць цих точок. Зазначене дає можливість програмі працювати із візуальними образами подібно людині. Значення дескриптора є незмінним стосовно зміщення, повороту, масштабування об'єктів на зображенні, при цьому кількість утворених дескрипторів, що формують опис, повинна бути достатньою для прийняття рішення відносно ідентифікації. Розпізнавання полягає в обчисленні міри релевантності між описами об'єкта та еталона, образи яких задані у вигляді множин дескрипторів та оптимізації значень цієї міри для бази еталонних зображень [3-5].

Для обробки зображень з метою їх ідентифікації використовують ряд алгоритмів (методів), які базуються на комп'ютерному баченні. До основних з них належать:

1. SIFT (Scale Invariant Feature Transform) – алгоритм застосовується для аналізу зображень з подальшим виявленням, описуванням та зіставлянням локальних ознак (точок) у зображеннях та створенні дескриптора. Для побудови простору зображень метод SIFT використовує фільтр Гауса, де обчислюється різниця Гауса, а саме попіксельне віднімання зображень в одній октаві. Октаву формують зображення одного масштабу, розмиті фільтром Гауса з різним радіусом розмиття. На цьому етапі забезпечується інваріантність до масштабування, далі визначаються екстремуми, які записуються в список потенційних контрольних точок.

Переваги: інваріантність щодо рівномірного масштабування спрямування та зміни освітлення; часткова інваріантність щодо афінного спотворення. Недоліки: вимогливість до обчислювальної потужності та ліцензійність.

2. SURF (Speeded up Robust Features) – подібний до алгоритму SIFT, але працює за допомогою матриці Гессе, яка досягає свого екстремуму в точках максимальної зміни градієнту яскравості. Градієнт яскравості обчислюється за допомогою фільтрів Хаара. Метод добре виявляє плями, кути, краї, але не інваріантний відносно масштабу. Після знаходження контрольних точок формуються дескриптори.

Переваги: інваріантність відносно повороту, різниці яскравості; можливість виявлення багатьох об'єктів на заданому зображенні. Недоліки: складність реалізації та не дуже швидка робота.

3. FAST (Features from Accelerated Segment Test) – алгоритм детектування контрольних точок на зображеннях, заснований на швидкому алгоритмі перевірки великої кількості пікселів навколо потенційної контрольної точки. Визначає потенційні контрольні точки, шукаючи точки, у яких інтенсивність значно вища або нижча від інтенсивності центрального пікселя. Після вибору центрального пікселя, алгоритм перевіряє інтенсивності пікселів навколо центрального пікселя в чотирьох напрямках. Якщо знайдено стійкий або більше швидких переходів із темного до світлого або зі світлого до темного, центральний піксель вважається контрольною точкою.

Переваги алгоритму: швидкість детектування контрольних точок; ефективність виявлення контрольних точок на складних зображеннях з великою кількістю деталей;

простота реалізації. Недоліки: чутливість до шуму та текстур, до орієнтації; не є інваріантним до масштабу; відсутність можливості генерації дескрипторів.

4. BRIEF (Binary Robust Independent Elementary Features) – алгоритм створення локальних дескрипторів для обробки зображень, який використовується для виявлення та опису контрольних точок на зображеннях. Основна ідея методу полягає в тому, щоб створити короткі, бінарні дескриптори, які можуть швидко порівнюватися для відповідності між зображеннями.

Переваги: швидкість порівняння зображень через використання бінарних дескрипторів та прості порівняння пікселів; ефективність в обробці великих обсягів даних; простота реалізації; малий обсяг пам’яті, що дозволяє ефективно зберігати та обробляти багато дескрипторів одночасно. Недоліки: низька робучість; низька точність збігу; чутливість до шуму.

5. ORB (Oriented FAST and Rotated BRIEF) – алгоритм, який обчислює орієнтацію ключової точки зображення та бінарне узгодження з вже отриманих орієнтацій. Є ефективним варіантом SIFT та SURF, який забезпечує порівняну ефективність та швидкість. ORB розроблений на базі детектора контрольних точок і дескриптора.

6. BRISK (Binary Robust Invariant Scalable Keypoints) – продовження алгоритмів SIFT і SURF, але з подальшим удосконаленням складових FAST. BRISK складає дескриптор шляхом об’єднання результатів порівняльних тестів яскравості, враховуючи зазначений масштаб та розташування кожної контрольної точки, щоб забезпечити інваріантність до обертання та одержати адаптовано нормалізовані дескриптори. Дескриптор BRIEF забезпечує ідентифікацію однакових ділянок зображення, отриманих з різних точок зору.

Переваги: вища швидкодія завдяки спрощенню процесу обробки, побудови і використання дескриптора бінарного типу; можливість виявлення вищих контрольних точок на зображенні та досягнення стійкості до геометричних перетворень [2-5].

Порівняльний аналіз характеристик зазначених алгоритмів наведено в таблиці.

Таблиця – Порівняльний аналіз характеристик алгоритмів

Найменування алгоритму / Характеристика	SIFT	SURF	FAST	BRIEF	ORB	BRISK
Швидкість	висока	висока	висока	висока	середня	середня
Інваріантність до масштабу	відсутня	відсутня	відсутня	відсутня	наявна	наявна
Інваріантність до обертання	відсутня	відсутня	відсутня	відсутня	наявна	наявна
Витримка до шуму	висока	висока	низька	середня	висока	висока
Діапазон освітленості	середній	широкий	високий	середній	високий	високий
Діапазон детектованого кута	великий	широкий	середній	середній	великий	великий
Робоча пам’ять	середня	висока	низька	низька	середня	середня
Навчальна складність	висока	висока	низька	середня	середня	середня
Простота реалізації	середня	середня	висока	висока	середня	середня
Ресурсоємність	низька	висока	низька	низька	середня	середня
Відносна надійність	висока	висока	висока	середня	висока	висока

Аналіз методів ідентифікації зображень показав, що при розпізнаванні ВНП за зображеннями доцільно використовувати комбінування алгоритмів ORB та BRISK, вони дозволяють враховувати спотворення кольору, погане освітлення, наявність шумів та різних проекцій зображень, мають вищу швидкодію, побудовані по бінарному типу, що спрощує процес обчислення та знижує затрати. Характерними локальними ознаками ВНП, за якими можливе їх розпізнавання та класифікація є форма/зображення, матеріал виготовлення корпусу, його температура. Виявлення та розпізнавання за кожною окремою ознакою чи їх сукупністю може бути реалізоване в окремій чи комплексній роботизованій системі. Зазначене потребує подальших досліджень, первинно, щодо формування бази даних еталонних зображень та навчання нейронної мережі для ідентифікації різних типів ВНП.

Список використаних джерел

1. Невлюдов І.Ш., Янушкевич Д.А., Толкунов І.О., Попов І.І., Іванець Г.В. Обґрунтування необхідності створення робототехнічних комплексів для гуманітарного розмінування. Scientific Journal «Problems of Emergency Situations». Серія: Civil Security. Вип. 2 (38). С. 17–38. DOI: 10.52363/2524-0226-2023-38-2 (дата звернення: 10.03.2025).
2. Процюк Ю.О., Драглюк О.В., Паламарчук Н.А., Куцаєв П.В. Підходи до формування бази даних зображень в системі ідентифікації вибухонебезпечних предметів для подальшого навчання нейронної мережі. Збірник наукових праць ВІТІ «Системи і технології зв'язку, інформатизації та кібербезпеки». 2024. № 5, С. 119 – 128. URL: https://journal.viti.edu.ua/downloads/MITIT_5_2024.pdf.
3. Єремеєв О., Васильєва І., Макарічев В., Рубель О., Лі Ф., Чернова Г., Коваленко Б., Ворзель Б., Лукін В. Деякі аспекти обробки багатоканальних даних дистанційного зондування з використанням нейромереж. Prospective global scientific trends: Informatics, Architecture, Innovative technology, Ecology: Monographic series «European Science». 2023. No. sge19-02. P. 7–60. URL: https://desymp.promonograph.org/index.php/sge/article/view/sge19-02-001.
4. Szeliski R. Computer vision: algorithms and applications. Springer Science & Business Media. 2010. URL: https://vim.ustc.edu.cn/_upload/article/files/d4/87/71e9467745a5a7b8e80e94007d1b/4cd69b21-85d3-43ba-9935-fd9ae33da82b.pdf (дата звернення: 14.03.2025).
5. Gorokhovatskyi, Volodymyr; Tvoroshenko, Iryna. Image classification based on the Kohonen network and the data space modification. 2020. URL: https://ceur-ws.org/Vol-2608/paper76.pdf (дата звернення: 10.03.2025).

Паламарчук С.А., Паламарчук Н.А., Чередниченко О.Ю., Побережець Т.В.

ПРОБЛЕМАТИКА ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Завдання захисту інформації та кіберзахисту в інформаційно-комунікаційних системах (далі – ІКС, система) завжди актуальні, основні з них це санкціонований вхід, надання користувачам доступу до ресурсів ІКС та повноважень на обробку інформації, захист мережевих сервісів, відмовостійкість, тощо. Згідно [1], доступ до інформації в ІКС надається лише ідентифікованим та автентифікованим користувачам, ці процедури дозволяють визначити і перевірити користувача та за певними атрибутами надати доступ до ресурсів (сервісів, в т.ч. і хмарних) та інформації. Ідентифікація та автентифікація – це перша лінія оборони, «прохідна» інформаційного простору ІКС

(організації, відомства), яка є сполучним сегментом завдань захисту інформації та кіберзахисту.

Проблематика захисту інформації та кіберзахисту для різних систем більше ніж очевидна, фактично, рф 8 років вела гібридну війну і кількість кібератак постійно росла. Деякі приклади: атака на енергосистему з виведенням її з ладу (грудень 2015); атаки на мережі Міністерства фінансів, Держказначейства та Пенсійного фонду України, знищили важливі бази даних (грудень 2016); наймасовіша кібератака в історії NotPetya, вразила ~80 % підприємств України, зокрема, аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці, Кабінету міністрів України та низки ЗМІ (виведено з ладу ~10% комп'ютерів) (червень 2017); атаки проти системи «Вибори» під час виборів президента, коли з'явилися помилкові результати виборів; злам застосунку «Дія» (січень 2022) і злив персональних даних 13 млн. користувачів; атака на мережу Viasat, спричинила перебої зв'язку в Україні і деяких країнах ЄС, атаки на сайти (державні реєстри) Національних інформаційних систем та Міністерства юстиції України (грудень 2024) та ін. [3, 4].

З огляду на зазначене, резонансною є думка автора [4], згідно якої саме факт успішності останньої кібератаки на державні реєстри засвідчив, що відповідні ризики були певною мірою недооцінені, висновків і уроків з 2022 року зроблено не було. Весь час, вже впродовж «великої війни», замість зосередження на питаннях захисту наявних державних інформаційних ресурсів (першочергово тих, де обробляються дані громадян, зокрема військовозобов'язаних, чинних військовослужбовців, працівників правоохоронних органів), відбувається «шалена цифровізація», побудована на безвідповідальному ставленні до безпеки (формальному виконанні). Безпека – це не те, що роблять в оснащених «за всі гроші світу» «ситуаційних центрах», створених «за стандартами НАТО». Десятки чи сотні модернових кіберцентрів, збір даних про злами з мільярда джерел та ін. масштабні дії – принципово нічого не змінюють, якщо культура вимог до їх захисту та кібербезпеки відсутня, або ігнорується. Безпека – це не стан, а постійний, динамічний процес, який має починатися, коли виникає ідея автоматизувати (цифровізувати) якийсь процес та з якісного проектування системи, її захисту [4].

Загалом, ті підходи, що застосовуються зараз відображають тенденції формального (послабляючого) ставлення до проєктування та створення систем (що підтверджується і особистим досвідом супроводження створення відомчих ІКС), а саме:

– «демонструється» факт слабкої участі «Замовника-Споживача» у формуванні вимог до систем та їх захисту, слабкої уяви, які функції потрібно автоматизувати, а також, хибності враження, що «програмне забезпечення це і є ІКС»;

– технічні завдання на створення ІКС практично не містять суттєвих системних вимог (до функціоналу системи, спеціального програмного забезпечення, захисту інформації, інформаційної взаємодії), які потрібно було б перевіряти на різних етапах випробувань;

– відсутності принципового підходу з боку «Замовника-Споживача» до проведення випробувань та приймання етапів робіт, низької якості експлуатаційної документації;

– нерідко має місце відсутність взаємоузгодженості між проектними рішеннями при створені ІКС та комплексної системи захисту інформації (далі – КСЗІ) в ній, відсутність взаємодії між розробниками ІКС, КСЗІ та програмного забезпечення, тощо [2, 5].

Загалом, десятиліттями спостерігаючи за породженням різних трактувань щодо створення КСЗІ зазначимо, що не на створення системи захисту потрібно акцентувати увагу, і оперувати складністю процесу, а на створення «захищеної» ІКС, адаптуючись до викликів сьогодення та світових практик, які необхідно узгоджувати з національним законодавством, а не приймати «шляхом прямого перекладу». Потребують змін і підходи до всіх видів забезпечення: нормативного, організаційного, кадрового та технічного. Ніхто не є противником прогресу, адже зручними є державні е-послуги та

ін. «новинки» сьогодення але це має бути продуманий продукт зі стійкою безпекою [4, 5].

Сказане підтверджує думку [2] (і здоровий глузд), що первинно мають створюватися захищенні системи, в яких кожна функція системи «користувач/процес-інформація» повинна перекриватися інтегрованими послугами безпеки. І в доповнення, беззаперечним є те, що базовою умовою забезпечення кіберзахисту є створення захищеної ІКС у відповідності до вимог законодавства та визначених стандартів із захисту інформації (інформаційної безпеки), згідно з якими відпрацьовуються вимоги до конкретної системи та враховуються особливості обробки інформації в ній. При цьому, завдання захисту інформації та кіберзахисту відрізняються, вони не є взаємозамінними. Слід чітко розуміти, що в межах захисту інформації основним є забезпечення визначених властивостей інформації (конфіденційності, цілісності та доступності). Тоді як, в межах кіберзахисту основним є забезпечення штатного режиму функціонування системи, керованості системою, в тому числі, щодо доступу до визначеної інформації, реєстрації подій, своєчасного виявлення та реагування на загрози (атаки) та їх нейтралізації [2, 5].

Узагальнюючи зазначене, необхідність захисту інформації та кіберзахисту як професійного напрямку буде лише зростати. Інформація давно стала зброєю у війні, її потрібно не лише добувати, а первинно захищати те, що маємо. І як би гостро не стояла потреба в автоматизації інформаційних процесів, наданні адміністративних он-лайн послуг та ін. «цифровізації», питаннями безпеки нехтувати небезпечно, прикладів цього більше ніж достатньо.

Список використаних джерел

1. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Каб. Міністрів України від 29.03.2006 № 373 : станом на 21 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 07.03.2025).
2. Паламарчук Н., Паламарчук С., Черниш Ю., Мальцева І. Підходи до забезпечення кіберзахисту інформаційно-комунікаційних систем державних установ. *Збірник тез-доповідей V МНПК «Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану»*. Одеса, 20 жовт. 2023 р. С. 235–236. URL: https://sites.google.com/vaodesa.mil.gov.ua/confvaodesa.
3. Ткач В.О., Паламарчук С.А., Паламарчук Н.А., Чередниченко О.Ю., Цимбал І.В. Російсько-українська кібервійна. *Збірник тез-доповідей Всеукраїнської науково-практичної конференції «Актуальні проблеми кібербезпеки».* Київ, 27 жовт. 2022 р. С. 26–29. URL: https://duikt.edu.ua/uploads/p_2121_20358827.pdf?file=p_2121_20358827.pdf.
4. Дімітрієв О. Уроки кібератаки: як уникнути повторення? URL: https://interfax.com.ua/news/blog/1037217.html (дата звернення: 10.03.2025).
5. Паламарчук Н.А., Паламарчук С.А., Мартинюк В.В., Чередниченко О.Ю. Сучасні парадигми захисту інформації для державних установ. *Матеріали IV Міжнародної науково-технічної конференції «Системи і технології зв'язку, інформації та кібербезпеки: актуальні питання і тенденції розвитку».* Київ: ВІТІ, 28 лист. 2024 р. С. 110-111. URL: https://mitit.mil.gov.ua/page/science (дата звернення: 07.03.2025).

УДК 004.934.2

Пастушенко М.О., Пастушенко М.С., Романюк В.А., Файзулаєв Т.А.

АНАЛІЗ ВПЛИВУ НОРМАЛІЗАЦІЇ ГОЛОСОВОГО СИГНАЛУ СИСТЕМИ АВТЕНТИФІКАЦІЇ НА ЯКІСТЬ ФОРМАНТНИХ ДАНИХ

Сучасне життя і діяльність, як окремої людини, так і більшості організацій пов'язана з використанням інформаційних телекомунікаційних систем (ІТС). На жаль, сучасні ІТС в даний час схильні, як правило, до зовнішнього впливу, що призводить до порушення їх роботи. Одним із бар'єрів для запобігання зовнішньому впливу є системи автентифікації. Останнім часом для цього використовуються біометричні ознаки користувача, зокрема і його голос. Як відомо, за критерієм ефективність/вартість голосові системи автентифікації (ГСА) є найбільш перспективними [1]. Однак, сучасні ГСА має помилки першого та другого вище необхідних. Тому є актуальним наукове завдання зниження рівня зазначених помилок та, в першу чергу, за рахунок удосконалення процедур цифрової обробки голосового сигналу користувача.

Процедури цифрової обробки голосового сигналу включають:

– виділення ділянок голосового сигналу (виключення пауз між словами);
– за необхідності сегментацію сигналу;
– придушення шумів та перешкод;
– оцінку ознак користувача, які включені до шаблону;
– формування шаблону користувача та його використання для розміщення в базі системи автентифікації (етап реєстрації), або порівняння зі зразками бази шаблонів (на етапі автентифікації користувача).

При цьому на етапах цифрової обробки рекомендується проводити нормалізацію даних. Цілі нормалізації різні: вирівнювання енергії оброблюваного сигналу, придушення шумової складової, якісна оцінка ознак шаблону [3], приведення до безрозмірних величин ознак шаблону та ін.

Особливу роль серед ознак займають формантні дані, які включають формантні частоти, рівень спектральної потужності, ширину спектру формант та огинаючу спектру аналізованого сигналу. Термін форманта позначає певну частотну область, в якій внаслідок резонансу посилюється деяке число гармонік частоти основного тону, виробленого голосовими зв'язками, тобто в спектрі звуку форманта є областю посилених частот, що досить виразно виділяється.

Таким чином, під формантами розуміються частотні резонанси (полюси передаточної функції) мовної акустичної системи користувача в системи автентифікації. При цьому найбільш важливий параметр − частота форманти, визначається геометричною конфігурацією мовного тракту. У процесі промови довжина мовного тракту змінюється, тому змінюються й формантні дані.

У цій роботі досліджується вплив нормалізації голосового сигналу користувача на характеристики формантних даних.

Голосні негаразд важливі у розпізнаванні промови, але мають значення у розпізнаванні промовця [2]. Відомо, що голосні містять більшість періодичних частин мови. Отже, голосні мають більшу інформацію про резонанс мовного тракту, саме про частоті основного тону та формант. Тож у роботі проводитимемо аналіз, використовуючи українську фонему «о», яку вимовляє жінка. Частота дискретизації сигналу становила 64 кГц.

Серед методів нормалізації можна виділити: пікову, за середньоквадратичним значенням, нормалізацію за заданою нормою та ін. У цих дослідженнях використовуватимемо нормалізацію за заданою нормою, при якій рівень норми дорівнює максимальному значенню на ділянці, що аналізується.

На відміну від відомих підходів, вихідна фонема при аналізі не розбивалася при аналізі на сегменти і становила приблизно 200 мс. Такий підхід дозволив більш якісно і просто виділяти формантні дані. Форма амплітудного спектру аналізованого сигналу після нормалізації не змінюється, у якому досить просто виділяються перші шість формант. Починаючи з сьомої форманти, виникають складнощі з їх виділенням.

Відповідно до плану проведення дослідження, було проведено нормалізацію вихідного сигналу на інтервалі аналізу та, від отриманих результатів, було розраховано амплітудний спектр.

Проаналізуємо вплив нормалізації на формантні дані. Насамперед слід зазначити, що амплітудний спектр нормалізованого сигналу переміщається в позитивну область, а саме, значно підвищується спектральний рівень потужності кожної форманти. Таким чином, при розрахунку огинаючої спектра, остання, зрушуватиметься по осі «у» в позитивну область приблизно на 30 дБ. Однак, її характер не змінюється.

Проведений аналіз формантних частот від їхнього номера. Для перших шості формант аналіз свідчить про майже лінійну залежність частоти формант від їх номера. Зауважимо, що нормалізація не впливає на частоту визначених формант.

Нормалізація істотно впливає величину ширини спектра формант. Ширина спектру формант, як правило, визначається за будь-яким рівнем від максимального значення. У дослідженнях ця величина становила 0.8. Тут слід зауважити, що ширина спектра багато в чому залежить від форми спектра формантного сигналу і здатності розрахованого спектру (точність розрахунку). У цьому випадку вона становила 4 Гц. Більшість формантних частот для нормалізованого сигналу мають більшу ширину спектра. Тому за практичної реалізації доцільно оцінювати ширину спектра формант для ненормалізованого сигналу. Це дозволить точніше оцінити ширину спектра формантних частот.

Список використаних джерел

1. Пастушенко М.О., Пастушенко М.С., Петраченко М.О. До питання оцінки ефективності біометричних систем. *Електронний науковий журнал «Проблеми телекомунікацій»*. 2023. С. 37–44. URL:https://pt.nure.ua/wp-content/uploads/ 2023/12/123_ Pastushenko_biometric_.pdf.
2. Beigi H. Fundamentals of Speaker Recognition / H.Beigi // NY: Springer, 2011.– 942 p. DOI:10.1007/978-0-387-77592-0
3. Pastushenko M., Krasnozheniuk Ya., Zaika M. Investigation of Informativeness and Stability of Mel-Frequency Cepstral Coefficients Estimates based on Voice Signal Phase Data of Authentication System User. *International Conference «Problems of Infocommunications. Science and Technology» (PIC S&T'2020)*, 2020,**:** Kharkiv, Ukraine, pp. 467-472. **DOI:** 10.1109/PICST51311.2020.9468083.

УДК 004.934.2

Пастушенко М.С., Романюк В.А., Файзулаєв Т.А.

АНАЛІЗ ВПЛИВУ ЧАСТОТИ ДИСКРЕТИЗАЦІЇ ГОЛОСОВОГО СИГНАЛУ СИСТЕМИ АВТЕНТИФІКАЦІЇ НА ЯКІСТЬ ФОРМАНТНИХ ДАНИХ

Питання забезпечення безпеки особистих даних, інформаційних та обчислювальних ресурсів багато в чому пов'язані з процедурами автентифікації. В даний час все ширше з цією метою використовуються біометричні ознаки користувача. Особливо зручними у цьому плані є голосові системи автентифікації (ГСА), які з погляду ефективність/вартість є найперспективнішими [1]. Сучасні ГСА мають істотний

недолік – високий рівень помилок 1 та 2 роду, які не відповідають сучасним вимогам. Відомо, що усунути цей недолік можна за рахунок удосконалення процедур цифрового оброблення голосового сигналу.

Процедури цифрової обробки голосового сигналу включають:

– реєстрацію та дискретизацію голосового сигналу;
– виділення ділянок голосового сигналу (виключення пауз між словами);
– за необхідності сегментацію сигналу;
– придушення шумів та перешкод;
– оцінку ознак користувача, які включені до шаблону;
– формування шаблону користувача та його використання для розміщення в базі системи автентифікації (етап реєстрації), або порівняння зі зразками бази шаблонів (на етапі автентифікації користувача).

При цьому на етапах цифрової обробки рекомендується проводити дискретизацію із частотою 8 або 16 кГц. Частота 8 кГц суперечить відомій вимогі щодо частоти дискретизації Найквіста, за якою найвища частота корисного сигналу дорівнює половині або менше частоти дискретизації. Оскільки відомо [2],що ознаки користувача розміщуються в голосовому сигналі до частоти 8 кГц.

Мета цієї роботи оцінити вплив частоти дискретизації на якість оцінки формантних даних. Відомо, що особливу роль серед ознак займають формантні дані, які включають формантні частоти, рівень спектральної потужності, ширину спектру формант та огинаючу спектру аналізованого сигналу. Термін форманта позначає певну частотну область, в якій внаслідок резонансу посилюється деяке число гармонік частоти основного тону, виробленого голосовими зв'язками, тобто в спектрі звуку форманта є областю посилених частот, що досить виразно виділяється.

Як означено вище, у цій роботі досліджується вплив частоти дискретизації голосового сигналу користувача на характеристики формантних даних. У роботі будемо проводити аналіз, використовуючи українську фонему «о», яку вимовляє жінка. Останнє зумовлено тим, що голосні фонеми є важливими щодо користувача системи автентифікації. Частота дискретизації сигналу становила 64 кГц.

Використання фонеми з частотою дискретизації 64 кГц дозволяє організувати «чистий» експеримент, використовуючи процедури проріджування даних. Процедури проріджування дають можливість отримати додаткові послідовності для аналізу з частотами 32, 16 і 8 кГц.

На відміну від відомих підходів, вихідна фонема при аналізі не розбивалася при аналізі на сегменти і становила приблизно 200 мс. Такий підхід дозволив більш якісно та просто виділяти формантні дані. Форма та характер амплітудного спектру аналізованого сигналу для різної частоти дискретизації не змінюється, у якому досить просто виділяються перші шість формант. Починаючи з сьомої форманти, виникають складнощі з їх виділенням.

Відповідно до плану проведення дослідження, була проведена обробка аналізованої послідовності при різній частоті дискретизації.

Аналіз отриманих результатів дозволяє зробити висновок, що вимоги до частоти дискретизації істотно залежить від складності процедур наступної обробки [3]. І друге, навіть найпростіші процедури обробки (швидке перетворення Фур'є) показують неприйнятність застосування частоти дискретизації 8 кГц.

Список використаних джерел

1. Пастушенко М.О., Пастушенко М.С., Петраченко М.О. До питання оцінки ефективності біометричних систем. *Електронний науковий журнал «Проблеми телекомунікацій»*. 2023. С. 37–44. URL:https://pt.nure.ua/wp-content/uploads/2023/12/123_ Pastushenko_biometric_.pdf.
2. Beigi H. Fundamentals of Speaker Recognition / H.Beigi // NY: Springer, 2011.– 942 p.

DOI:10.1007/978-0-387-77592-0
3. Pastushenko M., Krasnozheniuk Ya., Zaika M. Investigation of Informativeness and Stability of Mel-Frequency Cepstral Coefficients Estimates based on Voice Signal Phase Data of Authentication System User. *International Conference «Problems of Infocommunications. Science and Technology» (PIC S&T'2020)*, 2020,**:** Kharkiv, Ukraine, pp. 467-472. **DOI:** 10.1109/PICST51311.2020.9468083.

Пащетник О.Д., Живчук В.Л., Петлюк І.В.

АНАЛІЗ ВИКОРИСТАННЯ АРХІТЕКТУРНОГО ПІДХОДУ ДЛЯ ПРОЄКТУВАННЯ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМ ЗА СТАНДАРТАМИ НАТО

У відповідності до методології архітектурного підходу (АП), який викладено в документі Міністерства Оборони (МО) США «DoDAF 2.0 Department of Defense Architecture Framework» («Еталонна модель побудови архітектури інформаційних систем МО США»), формування єдиного інформаційного простору для учасників бойових операцій (дій) повинно здійснюватися у відповідності до мережецентричної концепції, шляхом створення систем, що мають сервіс-орієнтовану архітектуру (СОА).

Відомо, що даний підхід використовують збройні сили країн-членів НАТО для проєктування інформаційних (автоматизованих) систем управління. Також він сформульований і представлений у міжнародних стандартах IEEE Std 1471-2000 і ISO/IEC 42010:2011. Основними концепціями (поняттями) стандарту є: система, цільове призначення, середовище, архітектура, архітектурний опис, представлення, модель.

Згідно методології АП, проєктування великих програмних систем повинно починатися із визначення цих концепцій (понять) в контексті призначення і задач, для вирішення яких ці системи створюються. Ключовими поняттями такого підходу є архітектура, тобто фундаментальна організація системи та архітектурний опис, що включає в себе представлення різних аспектів архітектури. Погляди включають архітектурні елементи та відносини між елементами, керовані через метамодель.

Архітектурний опис такої системи містить в собі чотири типи подання:

– функціональне (включає опис функцій і процесів управління, органів управління, що описують ці процеси, а також інформацію, що циркулює в системі управління);

– системне (це набір графічних і текстових моделей, що описують програмне, технічне і інформаційне забезпечення автоматизованої системи);

– у відповідності з технічними стандартами (визначає порядок і процедури розробки автоматизованої системи);

– загально-архітектурне (містить інформацію, що відноситься до архітектури інформаційних (автоматизованих) систем в цілому, межі і контекст її застосування).

Завдяки застосуванню архітектурного підходу забезпечуються унікальна та одноманітна ідентифікація всіх компонентів, що входять в дану систему, можливість їх безшовної інтеграції і безконфліктної взаємодії. Це досягається тим, що всі архітектурні документи логічно і формально зв’язані, що гарантує цілісність, працездатність і безперебійність описаної архітектури.

В результаті застосування даного підходу будуть забезпечені:

– безшовна інтеграція і сумісність новостворених і модернізованих засобів інформаційних (автоматизованих) систем управління із існуючими компонентами системи управління Збройних Сил України;

– підвищення оперативності під час розроблення та впровадження систем і засобів в існуючі структури засобів інформаційних (автоматизованих) систем управління

військами та зброєю.

Базова архітектура НАТО, що забезпечує керівництво для опису систем зв'язку та інформаційних систем через архітектури, визначена в документі Ради штабу НАТО з консультацій, командування та управління AC/322-B(2028)0002 (NATO Architecture Framework. Version 4 (NAFv4), January 2018).

УДК 004.49

Першин О. В., Клабан І. Ю., Кулабухов О.М.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ТА ПРОДУКТИВНОСТІ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ

З поширенням використання мережевих технологій зростає актуальність питання ефективності певних систем виявлення вторгнень. Актуальність даного питання також обумовлюється проблемою вибору більш ефективної в конкретних ситуаціях системи виявлення вторгнень в мережу, вирішення якої і є основною ціллю роботи.

В роботі проводиться дослідження систем виявлення вторгнень Snort і Suricata які були розгорнуті на операційних системах Linux, FreeBSD, а також віртуальна машина з операційною системою Ubuntu з ядром Linux 5.4 яка розгорнута на гіпервізорі VMWare ESXI.

Обидві системи виявлення піддавалися інтенсивному трафіку на обох протоколах. Для отримання більш точних результатів усі тести були проведені з різними розмірами пакетів (1470 біт, 1024 біт , 512 біт) для TCP і UDP. Тестування проводилося при швидкостях 250 Мбіт/с, 500 Мбіт/с, 750 Мбіт/с та 1.0 Гбіт/с.

Для забезпечення валідності тестів та точності порівняння систем Snort і Suricata використовувалося одне й те ж саме середовище передачі даних та були розгорнуті на ідентичних машинах для обох систем

Під час оцінювання були згенеровані мережеві атаки для оцінки продуктивності обох систем виявлення у умовах інтенсивного і змішаного трафіку. Аналіз проведених досліджень показав , що обидві програми показують досить високий рівень надійності на програмних забезпеченнях Linux та FreeBSD, розгорнутих на фізичних машинах. Однак на Linux 5.4, розгорнутому на VMWare ESXI Suricata показує втрати пакетів в межах сорока відсотків.

УДК 623.364.4

Поплавець С.І.

ДЕЯКІ ПОГЛЯДИ ДО ФОРМУВАННЯ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ РАДІАЦІЙНОЇ ТА ХІМІЧНОЇ ОБСТАНОВКИ

Для оцінки та прогнозування можливих загроз використовуються інформаційні моделі, які дозволяють аналізувати джерела забруднення, їх поширення та потенційний вплив. В якості вхідних даних взяті: джерела забруднення (АЕС, хімічні підприємства, військові об'єкти); метеорологічні умови (вітер, температура, вологість); географічні характеристики місцевості; данні моніторингу (радіаційний фон, концентрація хімічних речовин). В результаті аналізу та обробки вхідної інформації в інформаційних моделях радіаційної та хімічної обстановки отримані вихідні дані, які дозволяють оцінити масштаб загрози, спрогнозувати її розвиток та визначити заходи реагування.

При створенні інформаційної моделі радіаційної обстановки [1] та розробці сценаріїв наслідків руйнування об’єктів, пов’язаних з радіаційною небезпекою [2], використовуються вихідні дані з методик прогнозування та оцінки радіаційної обстановки після аварій на атомних електростанціях [3, 4]. Алгоритми моделі враховують обсяг вихідної інформації, яка включає дані про виявлення та оцінку радіаційної обстановки за допомогою методів прогнозування та результатів радіаційної розвідки.

Аналогічно, на основі методик прогнозування масштабів забруднення після руйнування хімічно небезпечних об’єктів (ХНО) [5-7], розроблено алгоритми інформаційної моделі хімічної обстановки, які застосовуються для довгострокового та аварійного прогнозування.

Моделювання атмосферної дисперсії враховує дифузійні процеси поширення радіонуклідів та небезпечних хімічних речовин у повітрі після руйнування радіаційних об’єктів та ХНО [8]. Для цього використовуються комп’ютерні програми та алгоритми, які імітують розповсюдження забруднювачів. Фактори, що впливають на масштаби поширення забруднюючих речовин, об’єднані в одну групу для спрощення та оптимізації вихідних даних, які використовуються для моделювання забруднення навколишнього середовища після руйнування радіаційних та хімічно небезпечних об’єктів. Для розрахунку зони розсіювання викидів від стаціонарних джерел застосовується емпірично-статистичний метод.

В якості моделей розповсюдження забруднення використовуються: Гауссові моделі розповсюдження (для локальних викидів), лагранжеві моделі частинок (відстеження руху забруднювачів), CFD-моделювання (обчислювальна гідродинаміка для складних випадків). Моделі дисперсії застосовуються для передбачення розподілу концентрацій забруднюючих речовин під час розробки сценаріїв наслідків руйнування радіаційно небезпечних об’єктів та ХНО. Ці моделі інтегровані в алгоритми інформаційних систем, які описують радіаційну та хімічну обстановку.

Список використаних джерел

1. Поплавець С.І. Гишко Г.Б., Овчаров О.В. Формування інформаційної моделі радіаційної обстановки для генерування сценаріїв наслідків руйнування радіаційно-небезпечних об’єктів. Scientific Collection «InterConf», (41): with the Proceedings of the 7th International Scientific and Practical Conference «Scientific Horizon in The Context of Social Crises» (February 6-8, 2021). Tokyo, Japan: Otsuki Press, 2021. P. 1206–1212. ISBN 978-4-272-00922-0.
2. Поплавець С., Гузченко С., Воробйов О., Авраменко О., Шумейко В. Можливий підхід щодо визначення раціонального складу сил та засобів радіаційного, хімічного, біологічного захисту для виконання заходів в умовах радіоактивного та хімічного зараження. Журнал наукових праць. Соціальний розвиток і безпека. К. : НУОУ. 2022. Вип. 12, № 5. С. 130—146. https://doi.org/10.33445/sds.2022.12.5.12.
3. Методика прогнозирования и оценки последствий разрушений (аварий) атомных електростанций и предприятий химической промышленности. М. : Воениздат, 1991. 92 с.
4. Кузьменко Л.Ф., Блеко А.М., Бацовский О.В. Методика оцінки обстановки при аваріях на ПНО та екологічної обстановки на військовому об’єкті : метод. посіб. К.: НАОУ, 2001. С. 23–35.
5. Про затвердження Методики прогнозування наслідків виливу (викиду) небезпечних хімічних речовин при аваріях на промислових об’єктах і транспорті /спільний наказ МНС України, Мінагрополітики, Мінекономіки, Мінекології № 73/82/64/122 від 27.03.2001 р. [електронний ресурс]. Режим доступу до сайту:http://zakon5.rada.gov.ua/laws/show/z0326-0.
6. Про затвердження Методики прогнозування наслідків виливу (викиду) небезпечних

хімічних речовин під час аварій на хімічно небезпечних об’єктах і транспорті [Текст]: наказ Міністерства внутрішніх справ України від 29 лист. 2019 року № 1000. К., 2019. 67 с.
7. Поплавець С.І. Гишко Г.Б., Лазебник С.В. Формування інформаційної моделі хімічної обстановки для генерування сценаріїв наслідків руйнування хімічно-небезпечних об’єктів. Debats scientifiques et orientations prospectives du developpement scientifique: collection de papiers scientifiques «ΛΌГОΣ» aves des matériaux de la l conference scientifique et pratique international (Vol. 2), Paris, 5 février 2021. Vinnytsia-Paris: Plateforme scientifique européenne & La Fedeltà, 2021. P. 123–130. https://doi.org/10.36074/logos-05.02.2021.v2.
8. Поплавець С.І. Гишко Г.Б., Колмогоров О.В. Інтегрування дифузійних процесів розповсюдження радіонуклідів та небезпечних хімічних речовин до інформаційних моделей хімічної та радіаційної обстановки. Scientific Collection «InterConf», (42): with the Proceedings of the 1st International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (February 19-20, 2021). Rome, Italy: Dana, 2021. P. 1115–1126. ISBN 978-88-32012-34-7. DOI 10.51582/interconf.19-20.02.2021.

Попов М.О.

ВИЗНАЧЕННЯ КООРДИНАТ РОЗВІДУВАЛЬНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ РАДІОЛОКАЦІЙНИМИ СТАНЦІЯМИ РАДІОТЕХНІЧНИХ ВІЙСЬК ТА МЕРЕЖЕЮ SDR ПРИЙМАЧІВ

Досвід російсько-української війни також показав, що велику небезпеку для підрозділів сил оборони України, об’єктів критичної інфраструктури тощо представляють розвідувальні безпілотні літальні апарати (БпЛА). Розвідувальні БпЛА є складними цілями для існуючих радіолокаційних станцій (РЛС) та на екранах індикаторів РЛС не спостерігаються. Факторами, які ускладнюють радіолокаційну розвідку розвідувальних БпЛА, є:

– мала дальність виявлення існуючого парку РЛС, отже, і малий час перебування цілей у зонах виявлення;

– вплив кутів закриття на виявлення цілей, особливо в лісистій місцевості;

– відсутність, як правило, попередніх цілевказівок по розвідувальних БпЛА.

Існуючі способи підвищення якості ведення радіолокаційної розвідки РЛС радіотехнічних військ (РТВ) і підвищення точності визначення координат повітряних об’єктів і цілей в сучасних умовах полягають в наступному:

– висування та розгортання окремих радіолокаційних взводів (зведених радіолокаційних підрозділів) на небезпечних напрямках;

– вибір позицій РЛС з найменшими кутами закриття;

– створення смуг виявлення маловисотних цілей на небезпечних напрямках за рахунок розгортання відповідних РЛС виявлення маловисотних цілей;

– застосування РЛС з кращими можливостями щодо виявлення маловисотних цілей;

– видача інформації про розвідувальні БпЛА споживачам з мінімальною дискретністю;

– використання інформації візуального спостереження від частин (підрозділів) першого ешелону;

– організація інформаційної взаємодії щодо поєднання інформації, яка добувається шляхом радіоперехоплення, та радіолокаційної інформації.

Основними недоліками існуючих способі підвищення якості ведення радіолокаційної розвідки РЛС РТВ і підвищення точності визначення координат

розвідувальних БпЛА є:

– висока вартість сучасних зразків озброєння і військової техніки (ОВТ);

– тривалий час на розробку на впровадження нових зразків ОВТ;

– складність побудови радіолокаційного поля (висока інтенсивність заходів щодо нарощування радіолокаційного поля, пов'язаних зі зміною позицій призначення для радіотехнічних підрозділів (виведення з під удару тощо);

– великі ресурсні витрати на забезпечення підвищення енергетики окремих РЛС;

– низька точність визначення координат розвідувальних БпЛА при використанні інформації візуального спостереження від частин (підрозділів) першого ешелону;

– нестійке супроводження БпЛА рухомими радіовисотомірами.

Отже, для усунення зазначених недоліків між можливостями існуючих засобів радіолокації і способами визначення координат розвідувальних БпЛА та вимогами до точності визначення координат розвідувальних БпЛА виникає актуальним питанням застосування мережі Software Defined Radio (SDR) приймачів.

Попова Н.О., Попов М.О., Нелінь Д.П.

АНАЛІЗ ЗАСТОСУВАННЯ СУПУТНИКОВОГО ЗВ'ЯЗКУ У СУЧАСНІЙ ВІЙНІ

Системи Starlink надали українській армії стратегічну перевагу на фронті. І наразі їм немає альтернативи.

На теперішній час проєкт американської компанії Space X Starlink відіграє важливу роль у сучасній війні, забезпечуючи високошвидкісний супутниковий зв'язок навіть у віддалених або зруйнованих районах. Його застосування під час війни в Україні продемонструвало ефективність у військових операціях.

Основні способи використання Starlink у війні:

– зв'язок для військових;

– збір розвідувальних даних за допомогою безпілотних літальних апаратів;

– швидка передача даних і розвідки;

– коригування артилерії;

– координація підрозділів сил оборони;

– надійний зв'язок у зонах ведення бойових дій та регіонах, де зруйнована інфраструктура.

Забезпечення зв'язку для цивільних організацій:

– робота критичної інфраструктури (медична допомога, енергетика, транспорт);

– можливість оперативного реагування на надзвичайні ситуації;

– підтримка інформаційної безпеки, запобігання кібератакам;

– доступ до незалежних джерел інформації, обхід цензури;

– можливість ведення інформаційної війни та контрпропаганди.

Поряд з багатьма позитивними аспектами, існують певні виклики та ризики, а саме:

– виникнення залежності від однієї компанії (Space X);

– існування можливості подавлення противником зв'язку та застосування кібератак;

– політичні обмеження щодо використання в певних районах ведення бойових дій.

У січні 2025 року компанія Space X розпочала тестування революційної технології Starlink Direct to cell на території України, яка дозволяє підключати мобільні телефони безпосередньо до супутникової мережі, без необхідності використання додаткових терміналів.

Starlink Direct to cell – це прямий зв'язок між супутниками, що знаходяться на низькій навколоземній орбіті, та звичайними стільниковими телефонами – смартфонами. Для роботи в мережі Direct to cell не потрібно, щоб у смартфоні був встановлений модуль супутникового зв'язку, достатньо того, щоб смартфон

підтримував певні частоти зв'язку 5G та отримав певне оновлення програмного забезпечення.

Для забезпечення роботи Starlink Direct to cell компанія Space X поетапно здійснює розгортання спеціальної серії супутників. Starlink Direct to cell підтримує лише надсилання повідомлень, але впродовж 2025 року має бути забезпечена передача даних і голосовий зв'язок.

Поки що інформації про роботу Starlink Direct to cell досить мало. Основну роль відіграватимуть два фактори – це завадостійкість супутникового зв'язку Starlink Direct to cell та швидкість передачі даних.

З переваг Starlink Direct to cell можна відзначити, що смартфони, швидше за все, матимуть значно менше енергоспоживання та масогабаритні характеристики, порівняно з існуючими терміналами Starlink.

Одним із напрямків може стати оснащення БПЛА-камікадзе зв'язком Starlink Direct to cell для надання їм функцій перенацілювання в польоті, розвідки на маршруті, а також можливостей візуальної оцінки результатів удару при груповому використанні.

Відносна дешевизна терміналів Direct to cell (звичайних сучасних смартфонів) потенційно дозволить встановлювати їх на величезну кількість контрнаступальних та оборонних зразків озброєння сил оборони України.

Швидше за все, протидіяти існуючими способами роботі Starlink Direct to cell, наприклад, засобами радіоелектронної боротьби, буде складною задачею для противника.

Підводячи підсумки, можна зробити висновок, що система Starlink Direct to cell може бути дуже корисна для тих, у кого вона є, і дуже небезпечна для тих, хто її не має.

УДК 004.946.5.056 (06)

Поручник А.В.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА

Як в давні часи так і в сучасному світі інформація є одним із найцінніших ресурсів, адже вона відіграє важливу роль у функціонуванні фінансових установ, бізнесу, органів державної влади, державних чи комунальний підприємств (установ та організацій), а також в особистому житті людей. В ході розвитку інформаційних технологій стало можливим збереження даних у віддалених серверах та на хмарних сховищах. На ряду з цим зросли загрози кібербезпеки, наприклад: з'явились часті випадки хакерських атак, поширились випадки розповсюдження шкідливих програмних забезпечень, злом систем з метою витоку інформації, а також зовнішні несанкціоновані втручання в роботу з метою зміни даних. З початку російської збройної агресії проти України росіяни нерідко вчиняли кібератаки на урядові сайти та роботу основних систем. Наприклад, 19.12.2024 відбулась наймасштабніша зовнішня кібератака на державні реєстри України за останній час, що на одинадцять днів призвело до призупинення роботи цілої низки державних реєстрів. Також, з початком війни була відключена Публічна кадастрова карта України, що здійснено для забезпечення безпеки даних та запобігання їх можливому протиправному використанню. Це один із випадків, коли реєстри не можуть запрацювати під час війни в повній мірі, адже це може становити загрозу національній безпеці. А тому, поряд із захистом територіальної цілісності державних кордонів від збройної агресії російської федерації, не можна забувати і про захист інформації та кібербезпеку, адже від цього залежить не тільки конфіденційність даних, а й фінансова стабільність, репутація компаній та безпека користувачів.

На сьогоднішній день для протидії загрозам застосовуються різні методи захисту інформації, одним із них є криптографія. Шифрування перетворює дані у закодований вигляд, що унеможливлює їх перехоплення. Популярні алгоритми шифрування включають AES та RSA. Цифровий підпис в свою чергу гарантує справжність документів, а хешування (SHA-256, MD5) використовується для перевірки цілісності даних. Аутентифікація та контроль доступу також відіграють важливу роль у захисті інформації. Системи безпеки включають однофакторну аутентифікацію (логін + пароль), двофакторну аутентифікацію (пароль + код із телефону), а також біометричну аутентифікацію (відбитки пальців, розпізнавання обличчя). Брандмауери та антивірусні системи є невід'ємною частиною кібербезпеки. Брандмауери блокують несанкціонований доступ до мережі, а антивірусні програми (Bitdefender, Kaspersky, McAfee) захищають від вірусів. Важливим аспектом кібербезпеки є захист мереж: VPN (шифрує інтернет-з'єднання), IDS/IPS (системи виявлення та запобігання атак). Проте і цих методів не достатньо для захисту інформації від зовнішніх посягань.

Слід звернути увагу на сучасні тенденції розвитку кібербезпеки, що включають використання штучного інтелекту, квантової криптографії та блокчейну. Технологія блокчейну є дуже перспективною, адже може використовуватись наприклад у забезпеченні роботи державних реєстрів в Україні, де зберігаються важливі дані про нерухомість, права власності та інші офіційні записи. Всі українські системи працюють на централізованих серверах, а вони як я вже зазначав часто стають мішенню для хакерів, через що можуть виникати витоки даних, підробка документів або повна втрата інформації. Саме тому, для захисту таких систем, потрібно звертати увагу на технологію блокчейн.

Що ж таке блокчейн – це своєрідний цифровий ланцюг, що складається з послідовно з'єднаних блоків. У кожному блоці зберігається певна інформація, яка захищена криптографічними методами. Головна особливість у тому, що кожен блок пов'язаний з попереднім за допомогою спеціального коду – хешу. Якщо хтось спробує змінити інформацію в одному з блоків, це одразу змінить хеші всіх наступних, і система відразу зафіксує спробу підробки. Саме ця особливість робить блокчейн таким надійним.

Однією з головних переваг блокчейну є децентралізація. Це означає, що інформація не зберігається на одному сервері, а копіюється на тисячі комп'ютерів по всьому світу. Якщо навіть один із них зламають, інші вузли мережі залишаться цілими, і дані не загубляться. Крім того, всі записи у блокчейні незмінні. Як тільки інформацію внесли, її вже неможливо видалити чи підробити без згоди більшості учасників мережі. Це дуже важливо для державних реєстрів, адже дозволяє уникнути шахрайства та корупції.

Наприклад, при реєстрації прав власності на нерухомість кожен запис можна зберігати у блокчейні. Це означає, що будь-яка зміна власника буде прозорою, а сам факт угоди неможливо підробити. Якщо людина купує квартиру, то після оплати відповідний запис автоматично з'являється у реєстрі, і новий власник одразу отримує свої права. У цьому допомагають так звані смарт-контракти – спеціальні програми, які виконують умови договору автоматично. Наприклад, якщо покупець відправив гроші, смарт-контракт сам передає йому право власності, це спрощує процес і зменшує ризики обману, наприклад не дозволить «чорним нотаріусам» вчиняти свої шахрайські дії.

А тому, одна з найважливіших переваг блокчейну – це захист від кібератак. У звичайних системах хакери можуть атакувати сервер і змінити дані, а з блокчейном це зробити майже неможливо. Оскільки, щоб зламати систему, потрібно контролювати більшість вузлів мережі, а це вимагає величезних ресурсів і є практично нереальним. До того ж кожен блок захищений криптографією, що робить дані ще більш безпечними. Тобто, щоб змінити дані в блокчейні потрібно підробити усі комп'ютери, які взаємодіяли з ним.

Звичайно, впровадження блокчейну потребує певних зусиль. Це не тільки технічні питання, а й юридичні. Верховна Рада повинна розробити відповідний закон, щоб

нормативному полі блокчейн визнавався як офіційний. У подальшому, ця технологія повинна інтегрована в державні установи, також потрібне навчання персоналу, щоб усі знали, як працювати з цією технологією, як це було з мобільним застосунком «Дія».

Переваг у блокчейну дійсно багато. Це перш за все безпека, прозорість, зниження витрат на адміністрування та захист прав громадян. Наприклад, автоматизація процесів за допомогою смарт-контрактів дозволяє зменшити кількість помилок, кількість працівників які обслуговуватимуть дані процеси, а також прискорить роботу реєстрів.

Отже, блокчейн – це перспективне рішення для захисту державних реєстрів. Завдяки децентралізації, прозорості та криптографічному захисту ця технологія дозволяє надійно зберігати інформацію та захищати її від підробок. Хоча впровадження вимагає часу та інвестицій, переваги, які отримають громадяни та держава, значно перевищують можливі труднощі. У майбутньому блокчейн може стати основою для безпечного та прозорого цифрового простору, де права кожного будуть надійно захищені. А дивлячись на те якими темпами здійснюється цифровізація України я впевнений, що уповноважені службові особи звернуть увагу на можливість впровадження технологію блокчейн в життя кожного українця.

УДК 621.391

Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Гетьман А.В.

АНАЛІЗ ВПЛИВУ РОСІЙСЬКИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ НА УКРАЇНУ

У 2025 році мона сміло констатувати, що сучасні військові конфлікти покидають стандартні межі і починають наповнюватися гібридними методами впливу, де перше місце займають інформаційні операції. Для підриву стійкості опонентів, маніпуляції громадською думкою, а також для формування потрібної для росії інформаційної реальності, росія використовує інформаційні операції. Для захисту інформаційного простору потрібно детально проводити дослідження інформаційних операцій росії тому, що у сучасних війнах значну роль відіграють інформаційні технології. Інформаційний вплив росії розрахований на різні аудиторії, де враховано їх соціум та стійкість до маніпуляцій. Сьогодні в Україні росія використовує інформаційні операції для підриву єдності українського народу, дискредитації влади та міжнародних партнерів, створення фейків, Telegram-каналів, мережу агентів впливу. Слід зазначити, що росія веде інформаційні операції і проти Заходу, які мають на меті послаблення підтримки України через висловлювання про «втому від війни», «корупцію» і економічну недоцільність допомоги. Для проведення інформаційних операцій кремль використовує підконтрольні медіа, ботоферми, лобістів для проведення політичних розколів. Потрібно провести дослідження щодо оцінки ефективності російських інформаційних операцій та виявити вразливості на аудиторії, а також відпрацювати заходи для покращення стійкості до інформаційних операцій в Україні.

Метою тези є аналіз впливу російських інформаційних операцій на Україну під час повномасштабного вторгнення росією до України. Дослідимо, як росія діє в Україні.

Основні аспекти інформаційних операцій включають у себе: пропаганду, дезінформацію та маніпуляцію громадською думкою. Можна виділити основні методи, які використовуються під час інформаційних операцій:

1) пропаганда та інформаційні компанії, які використовуються через телебачення та радіо, де через підконтрольні медіа-канали формують позитивний образ росії, а натомість дискредитують український уряд; використання соціальних мереж за рахунок ботів, фейкових акаунтів, створення сторінок для просування проросійських поглядів;

2) розповсюдження дезінформації та фейкових новин для отримання паніки, розколу суспільства, недовіри до українських інституцій;

3) проведення психологічних операцій, для яких підбирають агентів впливу, котрі маніпулюють думкою населення;

4) використання культурних подій, щодо спільного минулого для підсилення ностальгії, а також маніпуляцій історичними фактами, щоб створити розбіжності на історичні погляди;

5) створення економічного тиску через енергетичні важелі, щоб вплинути на політику та економіку України. Навмисне знищення енерго об'єктів на території України, для утворення енергетичного голоду в Україні, погрози через економічні санкції;

6) проведення культурних заходів, у вигляді концертів, виставок для пропаганди російської культури;

7) здійснення кібератак на українські інформаційні системи для заволодіння конфіденційною інформацією.

Проти України, як ми бачимо, росія використовує комплексний підхід, який включає в себе різні методи та інструменти для впливу на українське суспільство, політику.

Даний підхід включає в себе дезінформацію, економічний тиск, інформаційні операції, культурні заходи, кібероперації. Російські інформаційні операції впливу на Україну є складними і призначені для послаблення України, створення хаосу, підтримання впливу росії в регіоні та світі. Таким чином використання різних методів і інструментів дає можливість росії досягати успіхів у деяких цілях, але успіх залежить від контексту і конкретної ситуації.

Провівши загальну порівняльну оцінку методів інформаційних операцій стало відомо, що всі складові операцій впливу росії на Україну здійснюються комплексно і мають величезний вплив на різні аудиторії. Самими ефективнішими є телебачення та радіо, кібератаки, створення розколу всередині суспільства та ворожнечі тому, що у них найбільша аудиторія і вони можуть впливати на громадську думку.

Дискредитувати український уряд, росії допомагає телебачення та радіо маючи велику аудиторію, особливо серед старшого покоління. На такому ж рівні важливу роль відіграють соціальні мережі, забезпечуючи поширення дезінформації серед активних користувачів інтернету.

Росія також використовує різні інструменти та підходи для інформаційних операцій впливу на нейтральні до війни в Україні країни світу.

Такі методи, як соціальні мережі та кібератаки, є одним із найефективніших, інші, наприклад, ностальгія за спільним минулим, мають менший вплив. Важливо і в подальшому проводити дослідження для визначення ефективності кожного методу та розробки стратегії протидії російській пропаганді і дезінформації.

При проведенні досліджень у цьому напрямку мають треба включити аналіз ефективності визначених пропагандистських компаній та впливу різних типів інформаційних впливів на громадську думку.

Також потрібно дослідити вплив російської пропаганди на політичні погляди в нейтральних країнах та розвиток технологій для виявлення і протидії дезінформації.

Виявляти шляхи підвищення стійкості суспільства до маніпуляцій та впливу ззовні.

Список використаних джерел

1. Коваль В., Семененко О. Ірраціональні війни в контексті сучасної світової геополітичної обстановки: український аспект. Міжнародний науковий журнал «Military Science», 2023, Том 1, No 1, с. 14–32.
2. Гібридна війна проти України: історія, інструменти, технології. Вінницька обласна універсальна наукова бібліотека, 2023. URL: https://library.vn.ua/news-and-events/novini/gibridna-vijnaproti-ukraiini.

3. Левантович О. Гібридні війни XXI століття: нові виклики для медіапростору. Вісник Львівського університету. Серія: Журналістика, 2019, вип. 45, с. 52–59. URL: https://library.vn.ua/newsand-events/novini/gibridna-vijna-proti-ukraiini.
4. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни. Український центр медіаініціатив, 2023. URL: https://www.jta.com.ua/wpcontent/uploads/2023/08/UMCI_-Effectiveness-of-Russian-Disinformation Counteration_UA.pdf.
5. Лизанчук В. Журналістська правда і постправда в контексті гібридної війни Російської Федерації проти України. Вісник Львівського університету. Серія: Журналістика, 2019, вип. 45, с.323–334.
6. Семененко О., Коваль В., Водчиць О., Добровольський Ю. Мультидоменна операція – сучасний погляд на адаптацію форм і способів воєнних дій до трансформації середовища викликів та загроз. Міжнародний науковий журнал «Military Science», 2024, Том 2, № 1, с. 17–34.

Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Гетьман А.В.

АНАЛІЗ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ПРОГНОЗУВАННЯ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сьогодення є достатньо програмних інструментів, які призначені для функції збору текстових повідомлень, котрі розміщуються на тематичних інтернет-сервісах.

Практичне використання програмних інструментів дає змогу реалізації функції нечіткої інформаційно-аналітичної системи формування інтернет-потоку повідомлень тематичних інтернет-ресурсів.

Метою тези є відображення варіантів вирішення задач щодо прогнозування вразливостей та загроз інформаційної безпеки даних.

У зв’язку з тим, що форуми тематичних інтернет-ресурсів мають сховища з неформалізованими даними , щодо інформаційної безпеки, які містять розпливчаті поняття та знання (не має форматів викладу текстових повідомлень, користувачі застосовують специфічний сленг), потрібно застосовувати в цій ситуації для роботи з такими форумами механізми нечіткої логіки. При значній частці невизначеності потоку повідомлень, яка обумовлена неповнотою інформації, можливо обґрунтувати задіяння нечітких логічних моделей. Для ефективності отримання жаданого результату пропонується задіяти нечітку інформаційно-аналітичну систему прогнозування вразливостей та загроз інформаційної безпеки для покращення функціональних можливостей, які наведені на рисунку1.

В залежності від того якої якості будуть бази знань використані у інформаційно-аналітичній системі прогнозування вразливостей та загроз інформаційної безпеки, буде визначена ефективність роботи системи. База знань сполучає між собою ключові модулі системи та сховище даних.

Структура нечіткої інформаційно-аналітичної системи відображає процес аналізу потоку текстових повідомлень тематичних форумів інтернет-ресурсів та прогнозування вразливостей та загроз інформаційної безпеки конфіденційних даних, яка відображена на рисунку 2.

На початку роботи інформаційно-аналітичної системи список формується експертним шляхом, із загальної кількості форумів тематичних інтернет–ресурсів виділяються ті, тематика яких дозволяє інтернет-інформацію віднести до хакерських (інформація містить результати спеціалізованих досліджень з виявлення вразливостей та загроз інформаційної безпеки конфіденційних даних, повідомлення про комп'ютерні атаки, вразливості, шкідливе програмне забезпечення). Автоматизоване виявлення

нових форумів тематичних інтернет-ресурсів, в даній ситуації, можливо, шляхом проведення аналізу різноманітних форумів інтернет-ресурсів, з використанням запропонованих критеріїв відбору текстових повідомлень, що належать до заданої предметної області, для якої проводиться аналіз з використання онтології.

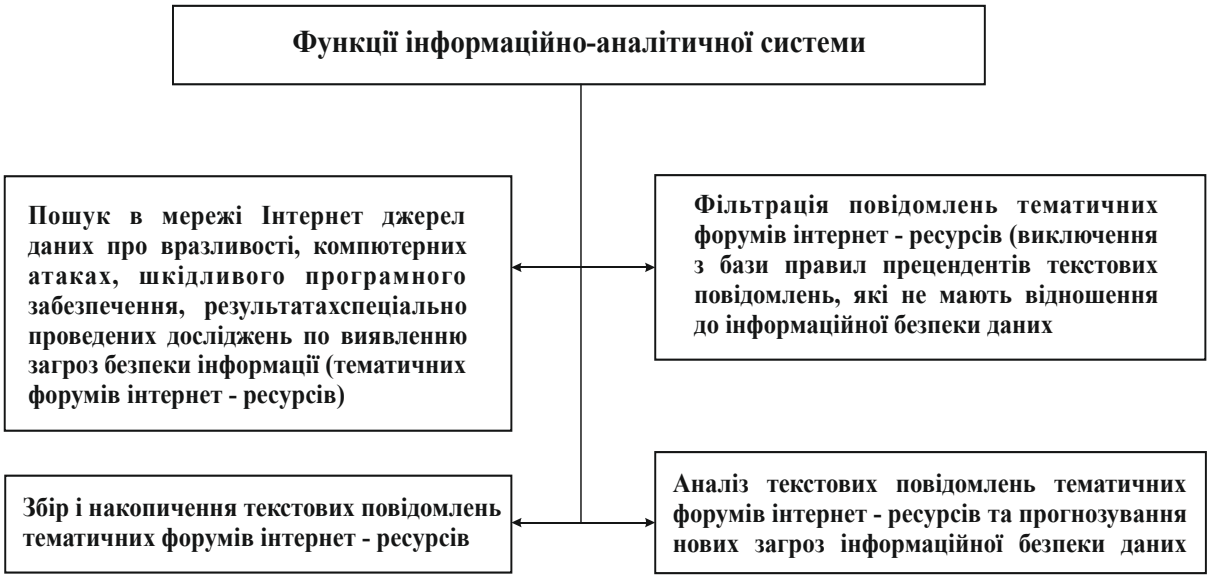


Рисунок 1 – Функції інформаційно-аналітичної системи аналізу потоку повідомлень тематичних інтернет-форумів

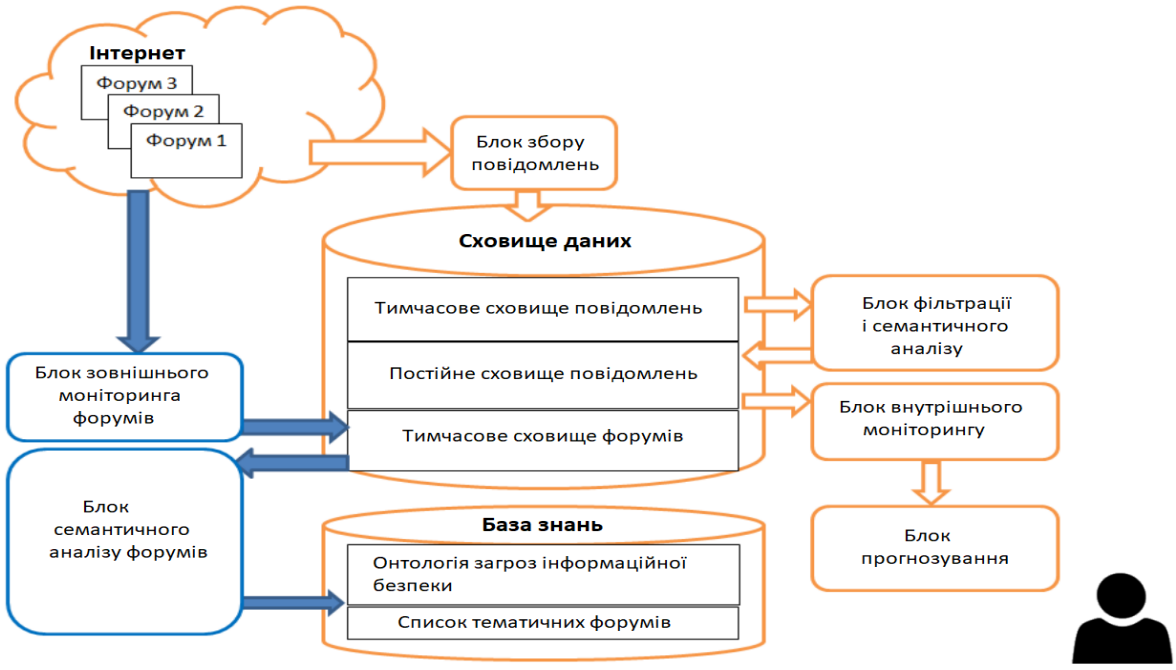


Рисунок 2 - Структура нечіткої інформаційно-аналітичної системи

Сьогодні для вирішення задачі проектування та розробки інформаційно-обчислювальних систем використовується універсальна мова моделювання UML, яка дозволяє реалізувати об'єктно-орієнтований підхід до проектування систем, будувати моделі систем із зазначеннями їх основних якостей.

Щоб побудувати та розробити концептуальну модель інформаційно-обчислювальної системи потрібно задіяти моделі бізнес-об’єктів, а саме: варіанти використання,

діаграми діяльності, послідовність дій. Вимоги до моделі інформаційно-обчислювальної системи у процесі її проектування будуються беручи за основу застосування діаграм варіантів використання. Під час попереднього проектування інформаційної системи застосовують діаграми станів, класів, послідовностей. Далі на етапі проектування фізичної моделі інформаційної системи використовують діаграми класів, компонентів та розгортання. Щоб описати функціональне призначення інформаційної системи потрібні діаграми UML варіантів використання. У процесі розробки та проектування діаграми є концептуальним представленням інформаційної системи (вхідними моделями). При вирішенні задач різного типу, працювати з інформаційною системою можуть користувачі двох типів:

1. Експерти, які використовують у роботі чотири модулі інформаційної системи:

– Protege – редактор онтології, який використовується для формалізації накопичених експертних знань у форматі онтології, які належать до предметної області;

– Fuzzy Logic Designer – редактор функцій вхідних та вихідних параметрів, правил логічних нечітких продукцій, який використовується для логічного нечіткого виводу про вразливості та загрози інформаційної безпеки конфіденційних даних;

– підсистема розширення ядра онтології – для вилучення з текстів термінології предметної області, де експерт оцінює вилучення та термінологічність і вносить їх до онтології предметної області, тим самим наповнюючи базу знань правил продукцій;

– редактор списку тематичних форумів інтернет-ресурсів, якій використовується для формування потоку текстових повідомлень, які аналізуються.

2. Спеціалісти з інформаційної безпеки, для прийняття рішень про достатність заходів, для захисту конфіденційних даних. При виникненні вразливостей та загроз безпеки інформації, користувачу надається доступ до підсистеми логічного нечіткого виводу, де в основі лежить проведення аналізу текстових повідомлень тематичних форумів інтернет-ресурсів.

При виникненні вразливості чи загрози безпеки інформації під час отримання виводу, користувач оцінює актуальність безпеки для інформаційно-обчислювальної системи та приймає відповідні запобіжні заходи для усунення негативних чинників. Нечітка інформаційно-аналітична система розробляється для обробки потоку інтернет повідомлень тематичних форумів інтернет-ресурсів, фільтрації текстових повідомлень на основі онтології заданої предметної області, проведення статистичного аналізу, соматичного аналізу потоку даних, логічного нечіткого виводу, базується на результатах потоку текстових повідомлень.

Покращення якості прогнозування виникнення вразливостей та загроз безпеки інформації з використанням систем логічного нечіткого виводу може сприяти збільшення кількості вхідних змінних, використанню більш точних нечітких правил продукцій, також велике значення має визначення функцій приналежності вихідних та вхідних параметрів системи логічного нечіткого виводу.

Список використаних джерел

1. Lienkov, S., Podlipaiev, V., Tolok, I., Lisitsky I., .Lytvynenko, N., Kuznichenko, S. The Information and Analytical Using of Non-Structured Information Resources CEUR Workshop Proceedingsthis link is disabled, 2021, 3126, pp. 81–87.
2. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.
3. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король – Харків: Вид-во ХНЕУ, 2016. – 476 с.
4. Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп’ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

5. Сигнатура атаки. Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атаки.
6. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Електронний ресурс] – Режим доступу до ресурсу: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt.
7. Ленков, С.В. Методы и средства защиты информации. В 2-х томах /С.В. Ленков, Д.А. Перегудов, В.А. Хорошко –К: Арий, 2008. – 464 с.
8. Yemchuk L. Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team. Zhylinska O.; Chornyi A.; Dzhuliy V. – Institute of Electrical and Electronics Engineers (30 September 2020); INSPEC Accession Number: 20008165; DOI: 10.1109/ACIT49673.2020.

УДК 621.391

Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Гетьман А.В.

ОЦІНКА ЯКОСТІ СИСТЕМИ ПРОГНОЗУВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

При оцінці ефективності системи прогнозування вразливостей та загроз інформаційної безпеки і для коректної роботи інформаційної системи проводилися експерименти. Під час даних експериментів був проведений аналіз потоку повідомлень форумів тематичних інтернет-ресурсів. Проведені наступні дії [1,2,3,4,5]:

– побудована онтологія вразливостей і загроз інформаційної безпеки конфіденційних даних, із задіянням словника інформаційної безпеки, класифікації вразливостей і загроз безпеки інформації, яка була отримана експериментальним шляхом;

– зібрана база правил логічних нечітких продукцій, яка призначена для відображення залежності кількості з’явившихся на форумі тематичних інтернет-ресурсів текстових повідомлень, а також для складання середнього рейтингу авторів від залежності виникнення вразливостей та загроз інформаційної безпеки;

– зібрані текстові повідомлення, відбір яких проходив експертним шляхом тематичних форумів інтернет-ресурсів;

– проведено розрахунки ефективності алгоритму безпеки інформації. Отримані ймовірності виникнення вразливостей та загроз інформаційної безпеки із вказанням записів, які включені до бази знань;

– пораховані показники кількості текстових повідомлень форумів тематичних інтернет-ресурсів та складання середнього рейтингу авторів повідомлень. Результати, які отримані, будуть використані в якості вхідних параметрів інформаційної системи логічного нечіткого виводу та розрахунку ймовірності виникнення загроз та вразливостей інформаційної безпеки;

– проаналізовано статистично та семантично текстові повідомлення шляхом фільтрації даних, які не містять термінів заданої онтології інформаційної безпеки конфіденційних даних.

Для вирішення задачі оцінки якості прогнозування інформаційної системи, задіяні показники, що наведені в таблиці 1.

MAPE – це середня абсолютна процентна помилка, яка використовується для оцінки якості прогнозування загроз та вимірюється у відсотках від значення прогнозованого показника. Цей показник потрібен для порівняння якості прогнозування конкретних моделей, у яких рівень помилки прогнозування критичний.

Таблиця 1 – Показники якості прогнозування аналітичної системи

№ п/п	Назва, формула, опис
1.	*MAPE* – середня абсолютна процентна помилка системи прогнозування $$MAPE = \frac{1}{h}\sum_{i=1}^{h}\left|\frac{f_{T,i} - y_{T+i}}{y_{T+i}}\right| \cdot 100\%, \quad (1)$$ де h - довжина інтервалу, на якому проводиться прогнозування загроз; $f_{T,i}$ - прогнозне значення часового ряду, отримане в момент часу T на i кроків наперед; y_{T+i} - значення часового ряду в момент часу $T+i$
2.	*MAE* - середня абсолютна помилка системи прогнозування: $$MAE = \frac{1}{h}\sum_{i=1}^{h}\left| f_{T,i} - y_{T+i}\right|, \quad (2)$$
3.	*RMSE* - квадратний корінь із середньої квадратичної помилки системи прогнозування: $$RMSE = \sqrt{\frac{1}{h}\sum_{i=1}^{h}\left(f_{T,i} - y_{T+i}\right)^2}, \quad (3)$$

Щоб оцінити метод прогнозування вразливостей та загроз безпеки інформації на основі проведеного аналізу текстових повідомлень учасників тематичних форумів інтернет-ресурсів провели експерименти з автоматизованого збору повідомлень інтернет-ресурсів. Результати проведеного аналізу текстових повідомлень були задіяні під час обчислення функцій приналежності вхідних параметрів. Завдяки отриманим результатам при застосуванні даного методу, проводилися обчислювальні експерименти для формування логічного нечіткого виводу про виникнення вразливостей та загроз інформаційної безпеки конфіденційних даних.

Для отримання оцінки результатів проведено розрахунки показників MAPE, MAE, RMSE (за формулами 1,2,3, які наведені вище) для значень прогнозування інформаційно-аналітичної нечіткої системи виникнення вразливостей та загроз безпеки інформації, а також кількість виявлених вразливостей та загроз під час проведення аналізу.

Було також проведено розрахунки згладжених часових рядів з інтервалом згладжування три та п’ять діб. Результати даних розрахунків наведені у таблиці 2.

Таблиця 2 – Показники якості прогнозування загроз

Показник	Експериментальні дані	Згладжування з періодом 3 доби	Згладжування з періодом 5 діб
MAPE (%)	94,21	147,04	119,73
MAE (%)	26,87	17,82	13,14
RMSE (%)	17,14	12,27	10,01

Проведено розрахунок показника точності прогнозування загроз η, для довірчих інтервалів 10, 15, 20%. Результати обчислень наведено у таблиці 3.

$$\eta = \frac{p}{p+q}, \quad (4)$$

де p – число випадків прогнозування, які підтверджені фактичними даними; q – число випадків, які не знайшли фактичного підтвердження.

Таблиця 3 – Показники точності прогнозування загроз

Довірчий інтервал	Експериментальні дані	Згладжування з періодом 3 доби	Згладжування з періодом 5 діб
10%	0,517	0,189	0,114
15%	0,554	0,559	0,482
20%	0,683	0,695	0,696

Результати прогнозування інформаційно-аналітичної нечіткої системи в більшості випадків будуть підтверджені даними бази знань вразливостей та загроз, згідно висновку по наведеним показникам.

На основі отриманих результатів прогнозування вразливості або загрози, фахівець із інформаційної безпеки, має змогу оцінити ступінь небезпеки інформаційних ресурсів установи та вжити відповідних заходів для усунення загроз та вразливостей.

Якщо якість прогнозування виникнення вразливостей та загроз безпеки інформації з використанням систем логічного нечіткого виводу буде покращена, то відповідно буде збільшена кількість вхідних змінних, використання точніших нечітких правил продукцій, а також визначення функцій приналежності вихідних та вхідних параметрів системи логічного нечіткого виводу, необхідно враховувати статистичні показники потоку текстових повідомлень форумів тематичних інтернет-ресурсів.

Проаналізовано системи нечіткого логічного виводу, сучасних засобів обробки великих об’ємів даних, засобів морфологічного аналізу тексту, редакторів онтологій.

В інформаційно-аналітичній системі реалізовано метод прогнозування вразливостей та загроз безпеки інформації на основі дослідження потоку даних тематичних ресурсів дозволяє автоматизувати інформаційний процес виявлення нових вразливостей, загроз, надає фахівцям інформаційної безпеки можливість оцінити своєчасно ступінь захищеності ресурсів та при необхідності вжити відповідних заходів щодо нейтралізації можливих загроз та вразливостей. Що тим самим дає змогу фахівцям інформаційної безпеки підвищити інформаційну безпеку обчислювальних комп'ютерних систем від реалізації нових мережевих комп'ютерних атак.

Під час проведення оцінки отриманих результатів були обчисленні показники *MAPE, MAE, RMSE* для значень прогнозування виникнення вразливостей та загроз інформаційної безпеки, а також розраховані на їх основі згладжені часові рядки з періодом три і п’ять діб.

Список використаних джерел

1. Джулій, В.М. Модель потоку текстових повідомлень тематичних інтернет-ресурсів системи прогнозування інформаційної безпеки / В. Джулій, Н. Петляк, Ю. Хмельницький, О. Пахар // Вісник Хмельницького національного університету. Технічні науки. – 2022. – № 5. – С. 294-300.
2. Джулій, В.М. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах/ І.В. Муляр, В.М. Джулій, В. М. Пічура, О.О Зацепіна – Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022), - 73–78 с.
3. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. / С.Ф. Гончар. – Київ, 2019. – 175 с.
4. Сигнатура атаки. Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атаки.
5. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Електронний ресурс] – Режим доступу до ресурсу: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt.

УДК 355.23

Радзіковський С.А., Павельчук В.Л.

ПРАКТИКА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРОЦЕСІ НАВЧАННЯ МАЙБУТНІХ ОФІЦЕРІВ СУХОПУТНИХ ВІЙСЬК

Четвертий рік запеклого протистояння повномасштабній збройній агресії рф висуває вимоги до процесу підготовки офіцерських кадрів, а саме зростання обсягу та складності інформації за незмінних термінів навчання потребує інтенсифікації навчального процесу, викладання матеріалу в більш доступному для розуміння та засвоєння вигляді, мотивації курсантів на навчання. Уміння офіцера використовувати надбання науково-технічного прогресу, вільно почувати себе в інформаційному просторі, у якому він виконує свої обов'язки, навики швидко та якісно працювати з інформацією, що постійно надходить, – ось головні риси сьогоднішнього професійного лідера. Шляхом вирішення цієї проблеми може бути більш широке використання в процесі навчання інформаційних технологій (ІТ), які наразі відіграють важливу роль у питанні впровадження інновацій в освітній простір вищого військового навчального закладу (ВВНЗ). Але при цьому для задоволення зазначених вимог ІТ мають відповідати специфіці вивчення навчальних дисциплін: використання топографічних карт (схем місцевості), інфографіки; моделювання обстановки; проведення розрахунків; аналіз великих обсягів інформації; виконання завдань у нормативні терміни тощо.

Необхідно зазначити, що не існує універсальної моделі, яка б забезпечувала формування єдиного інформаційного середовища вишу; наявність різноманітних поглядів на проблеми управління навчальним закладом та інформатизації навчального процесу обумовлює необхідність визначення теоретичних засад застосування ІТ; виникає потреба в інтеграції ІТ і традиційних технологій управління та навчання для їх найбільш ефективного використання для досягнення кінцевої мети – формування професійно підготовлених кадрів для Сухопутних військ (СВ) Збройних Сил (ЗС) України.

Серед ІТ, що ефективно використовуються в ході навчального процесу у Національній академії сухопутних військ (НАСВ), слід відмітити такі: мультимедійні системи (CD-sys), електронна пошта (e-mail), голосова електронна пошта (v-mail), електронний підручник, навчальний посібник (e-tbook), електронний бібліотечний каталог (e-libr), банк даних (db), локальні та розподільчі (глобальні) обчислювальні системи (LAN/WAN), автоматизована система адміністративних і навчально-методичних процесів «Деканат».

Вдосконалення засобів отримання, переробки та зберігання інформації, її передавання у часі та просторі, що стало можливим завдяки використанню нових знань, стало одним із чинників росту потоків інформації. Разом з тим, розвиток засобів передавання інформації вплинув і на процес управління. Якщо раніше у керівника було декілька потоків надходження інформації, то тепер їх у нього декілька десятків. У системі управління військами (силами) з'явились автоматизовані системи управління (АСУ) та нові покоління машин, що дозволило практично перейти на безпаперовий обіг інформації. Як приклад, використання АСУ повсякденною діяльністю ЗС України «Дніпро» з активним залученням одного з її серверів «Седо-М» для здійснення обігу інформації.

З розвитком технічних засобів передавання, перетворення інформації зазнав змін і технологічний процес її обробки. Мова іде ще про один чинник, що впливає на вимоги до посадової особи – рівень узгодженості технологічного процесу управління з можливостями людини. Під технологічним процесом мається на увазі система послідовно змінюючих один одного методів обробки, зміни стану та властивостей

інформації під час спілкування посадовця з підлеглими, взаємодіючими органами за допомогою технічних засобів у процесі вироблення та впровадження управлінського рішення. Зрозуміло, що можливості керівника повинні відповідати вимогам, які висуваються технологічним процесом до нього. Серед всіх інформаційних потоків потрібно визначитись і одержати таку інформацію, яка необхідна для конкретної справи. Нагромадження великої кількості будь-якої інформації значною мірою впливає на психіку користувача, не дає можливості зосередитись на головному, призводить до помилкових дій. Одним із шляхів вирішення даної проблеми стало «стискання» даних, використання термінів, абревіатур, формалізація передавання інформації. А ця робота вимагає підвищення рівня можливостей офіцера з опрацювання інформації.

Наступним чинником впливу на ефективність управлінської діяльності посадовця є стан його інформаційного режиму – сукупності форм і методів опрацювання отриманої інформації з метою вироблення нової для забезпечення прийняття управлінського рішення за мінімальних затрат як внутрішніх, так і зовнішніх ресурсів. У процесі діяльності людина створює свій особистий базис форм і методів роботи, які застосовує для обробки інформації, встановлює правила їх використання з найбільшою для себе ефективністю. Розширення інструментарію керівником для роботи з інформацією допоможе йому більш точно визначитись у видах та інформаційному наповненні даних, необхідних для виконання обов'язків і здійснювати пошук, збільшення об'єму та повноти обробки інформації, що надходитиме. Тобто мова іде щодо організації його інформаційної системи, яка є комплексом дій, що знаходяться у логічному нерозривному поєднанні один з одним, спрямованих на пошук, передавання, перетворення та зберігання інформації управління, та створюють єдність заходів щодо досягнення поставленої мети – прийняття управлінського рішення. І чим вище рівень інформаційних процесів, що відбуваються в інформаційному просторі, в якому здійснює свою діяльність офіцер, тим вище повинен бути рівень його інформаційної системи, що забезпечуватиме весь аспект його дій, пов'язаних із роботою з інформацією.

Сучасний ВВНЗ характеризується наявністю великої кількості інформаційних зв'язків як в адміністративній діяльності, так і в організації навчального процесу. Автоматизація повсякденної діяльності носить інтеграційний характер, тобто всі інформаційні ресурси логічно пов'язані в єдиний процес. Основними етапами реалізації процесно-орієнтованого підходу при формуванні інформаційного простору з використанням новітніх ІТ, є визначення стратегії навчального закладу та алгоритму її досягнення. Цей алгоритм містить опис взаємовідносин і взаємозв'язків між структурними підрозділами вишу, передбачає термін отримання результатів реалізації конкретних функцій.

Загальноакадемічна локальна обчислювальна мережа є основною мережею в НАСВ і забезпечує: роботу користувачів у мережі, використання навчальних класів для тестування, інтерактивного навчання тощо; користування внутрішньою web-сторінкою академії, ftp-сервером, який містить необхідне програмне забезпечення, що не потребує ліцензування; вхід до внутрішнього чату (за допомогою програмного забезпечення Jabber) з питань повсякденної діяльності; доступ до електронного каталогу загальної бібліотеки на базі програмного забезпечення універсальний фондовий дім (УФД) «Бібліотека».

Основою сучасної освітньої системи є високоякісні навчальні продукти, створені засобами ІТ. Серед них – електронні підручники, навчальні посібники, тестові комп'ютерні системи, електронні карти, електронні розрахункові задачі, які передбачають інтерактивні процеси навчання і забезпечують формування електронного навчального середовища вишу. В НАСВ науково-педагогічними працівниками факультетів і кафедр запроваджені електронні навчальні ресурси за всіма напрямами

підготовки військових фахівців, зокрема повнотекстові конспекти лекцій, доповнені ілюстративним матеріалом із використанням медіа-технологій.

Електронні навчальні посібники розміщуються на web-сторінках кафедр у локальній мережі академії, характеризуються доступністю та зручними умовами для використання, сприяють розвитку навичок самостійної роботи курсантів. Проте, розповсюдження електронних навчальних курсів і формування експертно-навчальних систем не вирішують наукову проблему щодо інформаційного забезпечення навчального процесу та передбачають запровадження новітніх педагогічних підходів в усіх сферах навчальної роботи. Майбутній офіцер, отримавши навики роботи зі спеціальним програмним забезпеченням, опанувавши знаннями з дисциплін професійної спрямованості, зобов'язаний вміти: оцінювати оперативну обстановку, яка склалась в ході виконання навчально-бойових завдань, проводити необхідні тактичні розрахунки; приймати доцільні рішення на організацію бойових дій у різних умовах обстановки; ставити завдання підпорядкованим силам і засобам; твердо здійснювати управління підрозділом в ході виконання поставлених завдань тощо.

Поява таких технологій, як гіпертекст, використання у комп'ютерних програмах звуків і графіки, застосування графіки, відео в режимі реального часу, надання можливості здійснювати моделювання бою, використання електронних підручників забезпечило активне впровадження ІТ в освітній процес підготовки майбутніх офіцерів. Сьогодні мультимедійна техніка дозволяє інтегрувати різні засоби надання інформації – текст, статичну та динамічну графіку, аудіо та відео в єдиний комплекс. Такий підхід суттєво підвищує результативність навчального процесу. Аналіз наукових доробок вітчизняних і закордонних вчених щодо використання програмних засобів на основі мультимедійних комплексів у навчанні дає підстави стверджувати, що їх застосування суттєво сприяє інтенсифікації навчального процесу, оптимальному поєднанню провідної ролі викладача і групових та індивідуальних способів організації навчання курсантів.

Найкращим видом підготовки для підрозділів є, поза сумнівом, безпосереднє навчання в «полі». Однак висока вартість цього виду підготовки, його ресурсна затратність зумовлюють пошук інших підходів до організації підготовки підрозділів. Одним з інструментів такої підготовки є використання засобів імітаційного моделювання (ЗІМ). Упровадження їх в освітній процес ВВНЗ дозволяє досягнути оперативної сумісності зі збройними силами держав-членів НАТО та іншими організаціями шляхом створення можливості для участі в навчаннях з міжнародними партнерами. Під час навчань з використанням ЗІМ, як правило, задіяні конструктивні тренажери, тобто комп'ютерні програми. Одним з таких тренажерів є система імітаційного моделювання JCATS (Joint Conflict & Tactical Simulation), яка дозволяє імітувати дії за участю багатьох сторін на рівні до окремих одиниць і використовується як засіб для проведення об'єднаних навчань, аналізу, досліджень планування та розіграшу поставлених завдань. Використання ЗІМ під час підготовки курсантів допомагає набути досвід в організації виконання завдань за призначенням без суттєвих витрат, великої кількості людей і техніки.

Таким чином, систематичне та організоване використання новітніх ІТ у навчальному процесі ВВНЗ значно сприяє підвищенню рівня оволодіння навчальним матеріалом, проте його ефективність залежить від наявності сучасних інформаційних систем, методичного забезпечення навчальних дисциплін та електронної інформаційної бази для відбору навчального матеріалу.

Радченко М.М., Скляров О.В., Сайко В.Г.

ВОЛОКОННО-ОПТИЧНІ СИСТЕМИ ПЕРЕДАЧІ ДЛЯ БЕЗПІЛОТНИХ СИСТЕМ

На теперішніх бойових діях набули стрімкого розвитку та застосування технології та різноманітні рішення безпілотних систем (БпС). Ефективна робота БпС вимагає високонадійних, швидкісних систем передачі даних, що забезпечуватимуть безперервний зв'язок, оперативну обробку та обмін як службовою так і цільовою інформацією.

Передача даних є важливою складовою для забезпечення стабільного функціонування БпС. Безперервний потік даних дозволяє таким системам взаємодіяти з іншими об'єктами, допомагати операторам приймати рішення в режимі реального часу та адаптуватися до умов навколишнього середовища що часто відбувається в умовах радіоелектронної боротьби (РЕБ) з боку противника. Створення переваги над противником в електромагнітному просторі однією із протиборчих сторін у збройному конфлікті веде до пошуків альтернативних середовищ передачі даних для БпС іншою стороною. Тому пошук шляхів перспективних систем передачі даних для БпС, які не піддаються впливу засобів РЕБ є критично важливим.

Застосування волоконно-оптичних систем передачі даних, Fiber Optic Communication Systems (FOCS) як раз і є одним із можливих шляхів для ефективного протистояння впливу з боку сучасних засобів РЕБ оскільки такий підхід передбачає перехід інформаційних потоків (сигналів керування, телеметрії та відео), що циркулюють в БпС, на ділянці впливу РЕБ, в інше фізичне середовище. В середовищі, яке створюється FOCS дані передаються електромагнітними випромінюваннями інфрачервоного спектру діелектричним середовищем сигналів відео з телеметрією та керування між наземною станцією керування (НСК) та безпілотним літальним апаратом (БпЛА), що унеможливлює вплив на канали передачі з боку радіоелектронного придушення (РЕП).

Нижче наведені напрями застосувань волоконно-оптичних систем передачі даних у БпС.

БпЛА з волоконно-оптичним каналом зв'язку використовується для забезпечення управління та безперервної передачі відеоданих в реальному часі для розвідки або при використанні БпЛА-камікадзе для ураження рухомих цілей на відносно відкритій місцевості у районі застосування.

У морських беспілотних апаратах (надводні, підводні) використання оптоволокна дозволяє забезпечити стабільний канал зв'язку із НСК з морської поверхні або суходолу для передачі великих обсягів даних, таких як гідроакустична інформація або відео, у середовищі, де інші форми зв'язку (наприклад, радіохвилі) є малоефективними через фізичні обмеження властивостей води.

В системах керування БпС для забезпечення швидкої та безпечної передачі даних між різними модулями системи керування, особливо якщо йдеться про системи із застосуванням штучного інтелекту, які потребують обробки великих обсягів даних у режимі реального часу а також для зниження електромагнітного впливу у між модульних з'єднаннях складових БпС.

Для, прикладу, на теперішній час виробники пропонують широку лінійку виробів волоконно-оптичних ліній зв'язку (ВОЛЗ), в тому числі і для ударних БпЛА із системою FPV. Так, на платформі Brave1 [1] долучений список українських компаній, у яких можна придбати БпЛА із волоконно-оптичними лініями, що забезпечують зв'язок між НСК та БпЛА див. таблицю 1. Аналіз продукції дає змогу робити висновки що вітчизняні виробники спроможні витовляти волоконно-оптичні системи передачі у випадку отримання ними відповідних технічних завдань.

Таблиця 1 – Продукція виробників волоконно-оптичних котушок, що придатні для ударних безпілотних літальних апаратів із системою FPV

Назва компанії	Варіанти намотки котушок, км	Країна намотки котушок	Орієнтовна вартість FPV дрона з котушкою 10км, грн	Орієнтовна вартість котушки 10км, грн	Вага котушки 10км, кг	Орієнтовна маса додатков. корисного навантаження на дрон з 10 км котушкою, кг
Камік-А	10, 15	Україна	29 000	-	0,9	1,5
ТЕХ ЕКС	5, 10, 15, 20	Україна	41 000	16 676	1,2	2,5
FG-drone	2, 5, 10, 15, 20	Україна	Виробник котушок	До 27 000 з наземним модулем	1.2	3
РАПТОР ІНЖИНІРІНГ	5, 10, 15, 20	Польща	39 000	23 572	1.8	3
Бойові Птахи України	5, 10, 15	Україна	41 500	-	1	3
3DTech	10, 15, 20	Китай, Україна	40 000	Від 17 000	1.1/2.5	2.5
На дроті	5, 10, 15, 20	Україна	Виробник котушок	12 507	1.2	-
Ортаверон	2, 5, 10	Україна	-	27 000	1.09	1.5
Secret1	10	Україна	40 000	30 000	1	3
BattleBorn	2, 5 10	Китай	55 000	33 000	2.4	1
Secret2	2, 5, 10, 15, 20	Україна	52 500	10 422.5	1.4	1.6
OWAD	5, 10, 15 (з інтегрованим холодним боєприпасом)	Україна	33 000	18 199	1.2	2
Dronarium & WARMAKS	5, 10, 15	Китай, (організовуються потужності в Україні)	58 999	29 999	2,2	3
Ratel	10, 15, 20	Україна	Наземний РК 1,2млн - 5 шт з оптикою на 10км і загальним навантаженням 35 кг. – НРК-камікадзе	-	1-2	35
Севлюш Авіа	2, 5, 10, 15	Китай та Україна	50 000	27 625	2,2; 1,5	1,5

Таким чином використання волоконно-оптичних систем передачі даних для БпС створює наступні ключові переваги:

– волоконно-оптичні системи можуть передавати значні обсяги даних на високих швидкостях, що є вагомим для БпС, які можуть потребувати одночасної передачі відео, телеметрії, навігаційних даних, сигналів керування;

– волоконно-оптична лінія забезпечує мінімальні затримки сигналів при передачі даних, що важливо для керування БпС в бойових умовах режимі реального часу;

– волоконно-оптичний канал передачі даних нечутливий до електромагнітних завад, що особливо важливо для застосувань БпС в середовищах із потужним впливом засобів РЕБ або впливу електромагнітних імпульсів надвисокої частоти (у випадку застосування мікрохвильових систем знищення БпС);

– волоконно-оптичну лінію складніше прослухати або підключитися до неї без фізичного втручання, що робить її привабливою для забезпечення безпеки передачі даних у БпС, де конфіденційність має критичне значення;

– відсутність металевих компонентів робить легшою БпС за рахунок меншої ваги оптоволокна.

Недоліком використання волоконно-оптичних систем передачі даних для БпС є вразливість до фізичних пошкоджень та обмеження дії, обумовлена довжиною оптичного кабелю, що, зазвичай, складає не більше декілька десятків км.

Використання ВОЛЗ у системах керування ударними БпЛА із технологією First Person View (FPV) дозволяє суттєво підвищити надійність і стійкість зв’язку в умовах РЕП. Для забезпечення ефективного функціонування ВОЛЗ необхідно визначити оптимальні технічні характеристики волоконно-оптичного кабелю.

З урахуванням специфіки експлуатації ВОЛЗ для керування ударними БпЛА із системою FPV, до волоконно-оптичного кабелю доцільно висувати такі основні вимоги:

Мала маса та гнучкість. Кабель не повинен значно впливати на аеродинаміку та маневреність БпЛА, особливо це стосується повітряної компоненти, що використовується одноразово і доцільно виготовляти з параметрами не нижчими за визначені технічною специфікацією ITU-T G.657.A2.

Механічна міцність та зносостійкість. Стійкість до розривів, вигинів та вібрацій під час польоту. Використання зміцнених структур у складі наземної компоненти, що використовуватиметься багаторазово (оплетення з кевлару, полімерні зміцнені оболонки).

Низьке загасання сигналу. У ВОЛЗ доцільно використовувати високоякісне одномодове оптичне волокно для забезпечення мінімального затухання із взаємосумісними у роботі оптоконверторами із робочими довжинами хвиль 1310 нм або 1550 нм. Оскільки при дослідженні спектральних характеристик загасання у кварцовому волокні визначені так звані «вікна» прозорості у цих діапазонах довжин хвиль, де оптичні втрати є мінімальними.

Стійкість до впливу зовнішнього середовища. В конструкції ВОЛЗ необхідно застосовувати термо- та вологостійкі матеріали для роботи у складних погодних умовах, з високою стійкістю до ультрафіолетового випромінювання.

Швидкість та пропускна здатність. З урахуванням специфіки використання ударних БпЛА із системою FPV, необхідне забезпечення високошвидкісного передавання відеосигналу FPV без затримок з оптимальною смугою пропускання не менше1 Гбіт/с.

Оптимальна довжина кабелю визначається замовником і може складати 5, 10, 20, 40 км для забезпечення радіусу дії. Даний параметр обумовлюється вагою котушки та міцністю волоконно-оптичного кабелю під конкретний тип БпЛА.

Рєзніков Ю.В., Аркушенко П.Л., Андрушко М.В., Матющенко О.Г.

РОЗРОБКА МЕТОДИЧНОГО АПАРАТУ ВИПРОБУВАНЬ АКУСТИЧНОЇ ПОМІТНОСТІ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ

Сучасні наземні роботизовані комплекси (далі – НРК) відіграють важливу роль у військовій справі, охороні об'єктів, розвідці та рятувальних операціях. Одним із ключових факторів їх ефективності є рівень акустичної помітності, який визначає здатність противника чи системи спостереження виявити роботизований комплекс за звуком. Дослідження акустичних характеристик дозволяє підвищити скритність НРК і покращити їхню ефективність у бойових умовах та спеціальних операціях. Зниження акустичної помітності є важливим аспектом, який впливає не лише на військову ефективність, а й на можливості застосування НРК у цивільних сферах, таких як автоматизовані логістичні системи, розумні міста та екологічний моніторинг.

Наукові дослідження у сфері акустичної помітності техніки зосереджені переважно на військових транспортних засобах, літаках і підводних човнах. У той же час аналіз літератури вказує на обмежену кількість публікацій, присвячених саме наземним роботизованим комплексам. Відсутність єдиної методики оцінки акустичної помітності ускладнює розробку заходів зі зниження шумового фону НРК. Ряд наукових праць висвітлюють методи математичного моделювання акустичних характеристик, проте практичні методи випробувань не стандартизовані. Це створює необхідність у розробці нових підходів, які враховують особливості різних типів НРК, їхні розміри, джерела шуму та сценарії застосування. Крім того, акустичне моделювання та випробування можуть сприяти створенню більш ефективних та екологічно безпечних мобільних платформ.

У рамках дослідження пропонується методичний апарат, що включає:

1) критерії оцінки акустичної помітності НРК з урахуванням різних експлуатаційних умов, включаючи міські, природні та військові ландшафти;

2) методики проведення лабораторних і польових випробувань із використанням сучасних акустичних сенсорів і аналізаторів шуму;

3) математичну модель розповсюдження шуму для прогнозування акустичного профілю НРК, зокрема з використанням методів машинного навчання для точного передбачення можливостей детектування;

4) рекомендації щодо зниження рівня шуму шляхом оптимізації конструкції, використання звукопоглинальних матеріалів та покращення алгоритмів керування двигунами та рухомими механізмами;

5) оцінку ефективності акустичних заходів на основі порівняння експериментальних та розрахункових даних, що дозволить сформувати єдині стандарти для проектування малопомітних роботизованих платформ.

Зазначений методичний апарат випробувань дозволить:

1) стандартизувати процес оцінки акустичної помітності НРК, що важливо для розробників і операторів таких комплексів;

2) вдосконалити конструкцію роботизованих платформ для зниження рівня шуму та підвищення їхньої енергоефективності;

3) підвищити бойову ефективність і прихованість НРК, що сприятиме кращій реалізації завдань у військових умовах;

4) розширити можливості інтеграції таких комплексів у різні сфери застосування, включаючи промислову автоматизацію, екологічний моніторинг та розумні інфраструктури;

5) покращити методи навчання операторів НРК, особливо у сфері тактичного використання роботизованих систем у складних акустичних середовищах.

УДК 621.396.67

Сахарчишина А.І., Бабарика А.О.

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ПАТЧ-АНТЕН В РАДІОСИСТЕМАХ УКХ ДІАПАЗОНУ

Широке застосування УКХ радіосистем породжує актуальну задачу розробки ефективних антенних систем. Для радіосистем військового призначення особливо актуальним є те щоб такі антенні системи були оптимальними для визначених діапазонів використання радіохвиль, мати характеристики завадостійкості та в окремих випадках мати спрямовані діаграми направленості. Аналіз штирьових, телескопічних та ФАР антен показав, що кожен із цих типів має свої унікальні переваги та недоліки, проте жоден з них не може повністю задовольнити всі вимоги, які висуваються до сучасних антенних систем. Патч-антена виділяється як перспективний варіант завдяки своїм компактним розмірам, низькому профілю та відмінним характеристикам випромінювання. Вона забезпечує високу ефективність при мінімальних габаритах, що робить її ідеальною для використання в мобільних додатках та малопомітних системах. Завдяки здатності працювати в різних частотних діапазонах та легкості інтеграції з іншими компонентами антенної системи, патч-антена є привабливим рішенням для сценаріїв, де критично важливі непомітність і стабільний зв’язок. Також однією з переваг патч-антен є можливість забезпечувати лінійну або кругову поляризацію [1].

Серед різних типів антен, використовуваних у військовій сфері, патч-антена вважається одним із найперспективніших варіантів Це зумовлено її конструктивними особливостями, які забезпечують високу ефективність випромінювання, компактність і можливість інтеграції в різні види техніки та особистого оснащення військовослужбовців. Основою патч-антени є проста, проте ефективна конструкція, що складається з двох металевих пластин: випромінюючого елемента (патча) та заземлюючої поверхні, між якими розташовується діелектрична підкладка. Така будова дозволяє досягти стійких характеристик випромінювання за мінімальних розмірів. Завдяки своїй компактності ці антени добре підходять для встановлення на бронетехніці, безпілотниках, портативних засобах зв’язку, а також у системах прихованого розміщення антенного обладнання [2, 3].

Патч-антени добре досліджені для використання у гігігерцовому діапазоні. В УКХ діапазоні такі типи антен не набули широкого застосування через те що геометричні розміри таких антен будуть складати 40-200 см. Проте застосування різних типів матеріалів для створення таких систем дозволяють значно зменшити геометричні розміри.

Список використаних джерел

1. Rachok R., Katerynchuk I., Prokopenko Y., Strelbitskyi M., Babaryka A., Basarab O. Separate Issues of the Rational Construction of a Wireless Sensor Radio Network. *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv. Ukraine, 2024. P. 121-124. doi: 10.1109/TCSET64720.2024.10755682.
2. Breed G. The fundamentals of patch antenna design and performance / G. Breed // High Frequency Electronics. – 2009. – № 3.12. – P. 49–51.
3. Muralidharan J**.** Wideband Patch Antenna for Military Applications / J. Muralidharan // National Journal of Antennas and Propagation. – 2020. – Т. 2, № 1. – С. 25–30.

УДК 621.396.67

Січевська К.В., Шевчук І.В., Поліщук Є.Ю., Площик А.С.

АКТУАЛЬНІСТЬ РОЗРОБКИ ПРИСТРОЮ ДЛЯ АНАЛІЗУ УЗГОДЖЕННЯ АНТЕНИ ТА РАДІОСТАНЦІЇ НА ОСНОВІ КОЕФІЦІЄНТА СТОЯЧОЇ ХВИЛІ

У сучасних радіотехнічних системах ефективність передачі радіочастотної енергії між передавачем та антеною є важливим фактором для забезпечення надійного зв'язку. Показником ефективності такого узгодження є коефіцієнт стоячої хвилі (КСВ), що кількісно показує на скільки лінія передачі не відповідає навантаженню. Розробка компактних та точних пристроїв для вимірювання КСВ залишається актуальним завданням, оскільки неоптимальне узгодження призводить до зниження дальності зв'язку та можливого пошкодження передавального обладнання.

КСВ є ключовим параметром для оцінки якості узгодження в системах передачі радіочастотної енергії [5]. Цей параметр має базове значення для ефективної роботи всієї радіотехнічної системи, оскільки безпосередньо впливає на ефективність передачі енергії від передавача до антени. В умовах сучасних телекомунікаційних систем, де оптимізація енергоспоживання та дальності зв'язку є критичними вимогами, точне вимірювання та контроль КСВ стають необхідними елементами налаштування обладнання.

При створенні радіосистем важливо досягти мінімального значення КСВ, а саме 1:1. Такий показник вказує нам на те, що відбита енергія відсутня,а опір передавача та антени узгоджений. У реальних умовах значення КСВ становить 1,5:1, така величина є прийнятною, але для військової комунікації та супутникового зв`язку це може бути суттєвою проблемою.

Необхідно зазначити, що КСВ є інтегральним показником, який пов'язаний з іншими параметрами радіочастотних систем, такими як коефіцієнт відбиття, повернені втрати та відсоток відбитої потужності. Ці взаємозв'язки дозволяють проаналізувати причини неоптимального узгодження і застосувати відповідні коригувальні заходи..

Особливого значення вимірювання КСВ набуває в системах з високою потужністю передачі, де невідповідність може призвести не лише до зниження ефективності, але й до значних пошкоджень обладнання через перегрів або електричний пробій компонентів. Саме тому розробка сучасних приладів для точного вимірювання КСВ залишається актуальним напрямком досліджень і розробок у галузі радіотехніки.

За визначенням, КСВ – це відношення максимальної напруги до мінімальної напруги вздовж лінії передачі, що представлено у формулі [1]:

$$\text{КСВ} = \frac{|V(\text{макс.})|}{|V(\text{мін.})|} \quad (1)$$

Невідповідність електричних характеристик призводить до того, що частина енергії відбивається назад до джерела, створюючи стоячі хвилі – явище, коли падаюча та відбита хвилі взаємодіють, утворюючи характерний розподіл напруги та струму вздовж лінії. При ідеальному узгодженні, коли комплексний опір навантаження дорівнює опору джерела (зазвичай 50 Ом для більшості радіочастотних систем), КСВ дорівнює 1:1 [8].

КСВ можна також виразити через коефіцієнт відбиття (Г):

$$\text{КСВ} = \frac{1 + |\Gamma|}{1 - |\Gamma|} \quad (2)$$

де коефіцієнт відбиття розраховується як:

$$\Gamma = \frac{ZL - Z0}{ZL + Z0} \quad (3)$$

де ZL - імпеданс навантаження, а Z0 - характеристичний імпеданс лінії передачі.

Високий КСВ має ряд негативних наслідків:

1. Зниження ефективності передачі енергії, оскільки частина потужності відбивається назад до передавача замість випромінювання антеною.

2. Ризик пошкодження підсилювачів потужності через високу напругу та струм, що виникають через накладання падаючих та відбитих хвиль.

3. Активація схем захисту, що призводить до автоматичного зниження вихідної потужності.

4. Спотворення сигналу через затримку, яка виникає через багаторазове відбиття [4].

Пристрій для аналізу узгодження антени аа радіостанції формується на вимірюванні прямої та відбитої потужності за допомогою спрямованого відгалужувача. Основними компонентами пристрою є [2]:

1. Двонаправлений відгалужувач для одночасного вимірювання прямої та відбитої потужності.

2. Точні вимірювачі для перетворення РЧ-потужності в постійну напругу.

3. Мікроконтролер для обчислення КСВ за формулою:

$$КСВ = \frac{1 + \sqrt{\frac{Pr}{Pf}}}{1 - \sqrt{\frac{Pr}{Pf}}} \quad (4)$$

де Pr - відбита потужність, а Pf - пряма потужність

4. Дисплей для відображення результатів вимірювань.

5. Інтерфейс для передачі даних на комп'ютер або смартфон для можливого аналізу.

На відміну від звичайних вимірювачів КСВ, запропонований пристрій буде містити такі функції:

– автоматичне вимірювання КСВ та параметрів, що характеризують якість узгодження, включаючи коефіцієнт відбиття;

– аналіз смуги пропускання антени, за допомогою графіку залежності КСВ та частоти;

– алгоритм для покращення антени на основі отриманих параметрів;

– можливість зберігати профілі антен, для порівняння та аналізу.

При створенні пристрою слід звернути увагу на такі фактори, як забезпечення точності вимірювань у діапазоні частот від 1 МГц до 1 ГГц, зменшення власних втрат пристрою для збереження характеристик передачі, компактність та енергоефективність, надійність конструкції для використання в польових умовах.

Розробка пристрою для аналізу узгодження антени та радіостанції на основі КСВ має на меті підвищення ефективності радіозв'язку. Цей пристрій дасть можливість покращити характеристики антен та забезпечити більш надійний зв'язок.Таким чином запропонований пристрій буде корисним для широкого кола користувачів. Якщо далі продовжити дослідження, то вони будуть спрямовані на вдосконалення алгоритмів обробки сигналу та зменшення компонентів пристрою, що підвищить його функцоіональність.

Солодовник В.І., Пантась С.О., Пантась І.О.

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ПІДРОЗДІЛІВ БРИГАДИ ТА ЗАСТОСУВАННЯ ЗАСОБІВ ЗВ’ЯЗКУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

В умовах відсічі широкомасштабної збройної агресії рф проти України принципи роботи воїна-зв’язківця зазнали певних змін. Гібридна війна внесла корективи з погляду розміщення (розосередження) підрозділів, їх бойового застосування, способів протистояння діям загарбника тощо. Слід враховувати той факт, що основою ситуаційної обізнаності на теперішній час є не донесення від розвідувальних груп, що висуваються в глибину бойових порядків противника, а стріми з відеокамер

безпілотних літальних апаратів (БпЛА), дронів різного типу та дані, що забезпечуються рядом інформаційно-комунікаційних систем типу Дельта, Вежа, Кропива, «Віраж-планшет ЗРВ», Graphite Ui, Дамба тощо. Також активно застосовуються конференції Google Meet для постійного зв'язку (передачі голосу) між операторами БпЛА та іншими посадовими особами (черговий, начальник розвідки та артилерії). Особлива увага приділяється безпеці електронних комунікаційних мереж (ЕКМ) та антивірусному програмному забезпеченню.

Для функціонування згаданих систем па пунктах управління (ПУ) необхідно реалізувати кілька прив'язок до ЕКМ Збройних сил України (ЗСУ) та доступ до мережі Інтернет. Основою надійного зв'язку та управління підрозділами є резервування, тому прив'язок до електронного комунікаційного ресурсу (ЕКР) має бути кілька:

1. Волоконна оптика (ВО). За домовленістю провайдер ISP (Internet Service Provider) забезпечує швидкість передачі даних від 500 Мбіт/с до 1 Гбіт/с через оптоволоконний кабель (ОК), чого достатньо на командно-спостереженому пункті (КСП) батальйону (Б).

При викопуванні траншей для переміщення особового складу або при прокладанні ВО до підрозділів (наприклад, від точки забору ЕКР до КСП Б) слід залучати представника оператора зв'язку (ISP) – власника оптоволоконних ліній – для унеможливлення пошкодження прокладених ОК.

2. Станції супутникового зв'язку (ССЗ) Starlink. Різні версії та релізи ССЗ Starlink забезпечують реальну досягнуту швидкість (Data Rate) 100 – 300 Мбіт/с.

Приховане та відносно безпечне розміщення ССЗ повинно передбачати використання антитепловізорних, антидронових чохлів або клітки Фарадея, або ж, як мінімум, заглиблення терміналу нижче рівня землі із забезпеченням організації водовідвідних шляхів із ями/заглиблення та прикриття комплекту оргсклом (на відстані 20 см від терміналу) та/або маскувальною сіткою, чи, хоча б, пакетом для сміття – для маскування.

Для стабільної роботи ССЗ Starlink необхідно врахувати споживану терміналом потужність та забезпечити йому безперебійне стабільне живлення, оскільки стрибки напруги (три підряд) кожного разу скидатимуть налаштування до дефолтної конфігурації та призведуть до тимчасово-постійної відсутності сигналу.

При плановому сервісному оновленні ССЗ Starlink відзначається нормальний доступ до мережі Інтернет та з перебоями, до завершення цього процесу, – до ресурсів Warcloud.

За відсутності ЕКР від Starlink при прориві на ворожі території успішно застосовуються ССЗ інших виробників – Satcube Ku та Intellian OW10Hx.

3. Радіомости. Для забезпечення основних або резервних прив'язок до ресурів ЕКМ із практичними актуальними відстанями між точками від 2 до 12 км та швидкостями до 300 Мбіт/с широко застосовуються такі засоби: Ubiquiti AirGrid, AirFiber 5X HD; Rocket 5AC; Rocket M5; LHG MikroTik lte kit.

4. Станції широкосмугового доступу (СШД) Silvus StreamCaster SC 4200, 4400. Достойною альтернативою ССЗ та радіомостам є СШД Silvus, які будують неієрархічну mesh-мережу та дозволяють передавати дані, стріми та голос, забезпечуючи ситуаційну обізнаність та зв'язок із віддаленим підрозділами (наприклад, у наступі) зі швидкістю до 100 Мбіт/с. Наявність антенних пристроїв із різними коефіцієнтами підсилення дозволяє проєктувати складні розгалужені мережі та управляти підрозділами навіть в умовах навмисних завад внаслідок роботи засобів радіоелектронної боротьби (РЕБ) противника.

Для забезпечення радіозв'язку у наступі використовуються мобільні групи ретрансляторів Motorola (SLR 5500, 8000) на транспортній базі, оскільки стаціонарні ретранслятори встановити складно або неможливо внаслідок об'єктивних причин.

Нашими групами, які потрапили в оточення або засідку (перебувають під обстрілом) та тимчасово приховано розміщені у підвальних приміщеннях закинутих/ пошкоджених будівель, де портативна радіостанція Motorola DP4400e (або DP4800, DP48001E R7), хоч і знаходиться в секторі обслуговування ретранслятора, проте зв'язатись можливості не дає – замість звичайних штатних коротких Omni-антен використовуються «антени-павуки». Завдяки кабелям-подовжувачам до таких антен (довжина 5 м, 15 м, або два по 15 м), їх можливо відносно безпечно викинути із підвалу на поверхню землі та зв'язатись зі своїми підрозділами через ретранслятор.

Перепрошивання радіостанцій, заміна ключів шифрування відбувається щотижня або частіше (у разі компроментації ключів, або втрати/ захоплення радіостанцій ворогом) – підрозділи привозять засоби Motorola до начальника зв'язку Б (Бр) або визначеної посадової особи самостійно. Відома успішна практика передачі перепрошитих налаштованих радіостанцій групам, що тимчасово переховуються у підвалах, FPV-дроном (який, до речі, потім навіть можуть повернути). Найбільші втрати нашої живої сили відбуваються, на жаль, під час переміщення або ротації.

Радіостанції Motorola DP48001E R7 не мають запасних акумуляторних батарей (АКБ), тому можуть використовуватись тиловими підрозділами (медики, підрозділи забезпечення), а всі бойові організми забезпечуються DP4400e із взаємозамінними АКБ.

Для заряджання АКБ часто використовують перехідники для заряду від пауербанка із роз'ємом Type-C. Також підрозділи відновлюють та перепаюють АКБ радіостанцій Motorola DP4400e / 4800 під зарядку Type-C з індикацією рівня заряду на самій АКБ.

Для підвищення ситуаційної обізнаності, розвідки, вогневого враження противника, доставки засобів зв'язку тощо на вогневі позиції наших підрозділів та для виконання інших завдань підрозділами активно застосовуються гексакоптери Vampire, квадрокоптери Mavic Pro 3, Autel, FPV-дрони та дрони з оптоволоконним зв'язком (котушки звичайні на 8 км та подовжені – на 15-20 км).

Комплексні (переобладнані) апаратні зв'язку (типу Р-142Н, Р-145БМ) на теперішній час використовуються обмежено, або не використовуються. Наприклад, відома апаратна Roshel Senator, що запланована до застосування в якості передового пункту управління (ППУ), комплектується терміналом Starlink, генератором, телевізійними панелями, засобами радіозв'язку Motorola, ноутбуками, планшетами, засобами телефонії, а також телекомунікаційним комплектом Буревій (BUREVII TO-A2). Комплекти телекомунікаційні типу КТ 5.1, 5.2 та 5.3 застосовуються обмежено.

Для повноцінного якісного застосування власних засобів РЕБ та радіоелектронного подавлення (РЕП) слід знати тактико-технічні характеристики (ТТХ) та можливості таких засобів, а також можливості своїх та ворожих (безпілотних літальних апаратів) БпЛА. Не слід недооцінювати противника, оскільки рф переважає Україну кількісно як за особовим складом, так і за різноманіттям засобів, що вони використовують. Слід згадати хоча б трофейні радіостанції Baofeng зі специфічним діапазоном роботи 200 – 260 МГц, який до певного часу ЗСУ навіть активно не моніторили на предмет потенційного для прослуховування ворожих переговорів.

Для встановлення засобів РЕБ на позиціях спочатку проводиться оцінка доцільності роботи таких засобів у певному секторі та робота з мапами. Оскільки мапи є часто застарілими, підрозділи друкують на плотері свіжі аерофотознімки (до 14 днів із системи Вежа, або з Інтернета – Google Maps).

Для групи, що має висуватись для встановлення засобів РЕБ, проводиться:

– вибір позиції для встановлення відповідного засобу із подальшим обслуговуванням;

– рекогносцировка – для оцінки можливості та рівня безпеки доставки засобів на транспортному засобі та у пішому порядку;

– аналіз відео зі своїх дронів конкретної місцевості;

– усвідомлення задуму командира та вивчення карт (мінімум – півдоби);

– первинна розвідка двома особами підрозділу (а не чотирма), без засобів (нічого важкого) – із постійним супроводом дроном та зі зв'язком через радіостанції Motorola;

– безпосередньо – операція доставки засобу групою із чотирьох осіб.

Слід брати до уваги неможливість безпосереднього підвезення засобів РЕБ автотранспортом (АТ) до позиції, обраної для встановлення. Часто відбувається спішування та переміщення їх вручну або на власноруч змайстрованих візках (загальна вага засобу РЕБ, генератора, палива, води тощо, – іноді сягає 100 кг).

Вік, фізична витривалість та стресостійкість особового складу – також важливий фактор, коли існує безпосередня загроза ураження ворожим ударним дроном. У разі, коли ворожий розвідувальний або ударний дрон помітив переміщення нашого особового складу, можливо задіяти засоби РЕП взаємодіючих підрозділів для роботи – з метою позбавлення ворожого дрона сигналу управління. Наприклад, якщо власні засоби РЕП спрямованої дії працювали з метою захисту нашого особового складу на висоту 100 – 200 метрів, діаграму спрямованості засобу можна скоригувати на висоту 50 – 70 метрів, зменшивши кут місця (точність скиду у такому випадку істотно знижується).

Слід зауважити, що при вмиканні окопного РЕБ купольного типу, встановленого на АТ для власного захисту – зв'язок через радостанції Motorola втрачається, хоча діапазони і не перекриваються (засоби РЕБ, що працюють в діапазоні 600 – 1200 МГц заважають роботі радіостанцій Motorola (136 – 174 МГц)).

Сканер Uniden – цивільний засіб сканування радіоефіру з метою виявлення та прослуховування незашифрованих розмов ворога, який спілкується через такі радіостанції: Kenwood, Baofeng, DMR, Терех. У подальшому здійснюється перетворення аудіо у текст за допомогою спеціалізованого програмного забезпечення (штучного інтелекту – типу Community), мінімальне коригування та розсилка в підрозділи (месенджерами – у групи). Для максимальної ефективності необхідно 3 сканери Uniden:

– один виявляє факт передачі першою ворожою станцією та аналізує протягом 1 хв;

– інший виявляє факт відповіді другою ворожою станцією та аналізує протягом 1 хв;

– третій продовжує сканування радіоефіру.

На практиці сканування можливе на відстані до 28 км. Відстань залежить від багатьох факторів: ТТХ засобів, рельєфу місцевості, перешкод, метеорологічних явищ тощо. За фактом частоти переговорів та аналізу сутності розмов командирами приймається рішення про вогневе ураження місць скупчення ворога.

На бронетехніці часто встановлюється засіб РЕБ Яструб, застосування якого призводило до втрати сигналів управління ворожих БпЛА із їх подальшим приземленням. Обов'язковим є узгодження дій розвідки із взаємодіючими підрозділами на напрямках при роботі засобів РЕБ. Відомі непоодинокі випадки глушіння власними засобами своїх або сусідніх (взаємодіючих) підрозділів.

На теперішній час у підрозділах бригад активно застосовуються такі засоби РЕБ: Sky Wiper Omni, КВЕРТУС AD KRAKEN-U, КВЕРТУС AD KRAKEN Counter FPV, щит купол 3М, STR 50 – 1V, STR ШАТРО 50 – 1LP. Іноді, за наявності, використовують антидронові гвинтівки типу Drone Gun Tactical, Drone Defender, Sky Wiper EMD4S, що достатньо непогано зарекомендували себе. Разом із тим, ворог активно розвивається і використовує нові діапазони частоти управління своїх дронів, де наші засоби РЕБ поки неспроможні ставити ефективні завади.

УДК 004.932

Соломоненко Ю.С., Худов Г.В., Хижняк І.А., Грідасов І.Ю.

МЕТОД СЕГМЕНТУВАННЯ ЗОБРАЖЕННЯ В СИСТЕМІ НАВЕДЕННЯ FPV-ДРОНІВ НА ОСНОВІ ПЕРЕТВОРЕННЯ ХАФА

Аналіз досвіду ведення російсько-української війни показує, що повномасштабне вторгнення дало поштовх до розвитку і застосування нових форм і способів ведення збройної боротьби, а саме впровадження в тактику дій підрозділів застосування ударних безпілотних літальних апаратів з метою знищення вогневих засобів сил противника, бойової техніки, елементів системи протиповітряної оборони, радіолокаційних станцій та особового складу.

Застосування ударних безпілотних літальних апаратів сприяло підвищенню ефективності бойового застосування підрозділів, збереження життя та скорочення втрат серед особового складу.

Бойові завдання, що виконуються за допомогою безпілотних літальних апаратів, стають все більш різноманітними та складними.

Для вирішення таких задач зараз широко використовуються FPV-дрони, вони здатні забезпечити велику швидкість, гарну маневреність і високу точність наведення на ціль.

Перевага застосування FPV-дронів також полягає в їхній відносно невеликій вартості порівнянні з традиційними безпілотними літальними апаратами.

Завдяки своїй модульній конструкції, FPV-дрони можуть бути адаптовані під різні завдання, включаючи виконання функцій камікадзе, бомбардувальників, розвідувальних апаратів тощо.

Оператор FPV-дрона керує літальним апаратом у реальному часі в режимі «від першої особи», завдяки встановленим на борту дрона відеокамері та передавачу відеосигналу. Оператор керує дроном за допомогою спеціальних окулярів, спостерігаючи за польотом так, ніби знаходиться всередині повітряного судна. Сама абревіатура FPV походить від англійського терміну «First Person View», що означає «вид від першої особи». Це дозволяє оператору здійснювати точне управління дроном, навіть у складних умовах міського бою або на пересіченої місцевості.

Тому для швидкого та якісного виконання завдання оператор повинен мати якісне оптико-електронне зображення з виділеними об’єктами пошуку, щоб визначати ціль для ураження.

При аналізі відеозображення можливо його розбиття на складові частини за деякими ознаками, які містять корисну інформацію, таку наприклад як характерні геометричні особливості об’єктів інтересу. Такий процес розбиття на групи по ознакам називається сегментацією.

Сегментація розділяє оптико-електронне зображення на області чи об'єкти, з яких воно складається. Та ступінь деталізації, до котрого доводиться таке розбиття, залежить від завдання, що вирішується. Сегментацію слід завершити тоді, коли об'єкти, які нас цікавлять, ізольовані.

Сегментація візуальної інформації є попереднім етапом будь-якої системи обробки зображень, так як дозволяє спростити подальший аналіз однорідних областей зображення, їх яскравості і геометричних характеристик.

Сегментацію можливо проводити як статичних зображень у вигляді окремого зображення так і динамічних зображень у вигляді відео потока даних.

На етапі сегментування можливо виділення визначених ознак об’єктів розвідки.

Візуальна оцінка сегментованого зображення на системах моніторингу дає змогу визначити йомовірні об’єкти інтересу значно простіше і швидше.

Сегментацію використовують для виділення об’єктів та меж на отриманому

зображенні. Для проведення автоматизованої сегментації зображень на цей час розроблено багато різних методів. Кожен метод має свої переваги та недоліки.

Тому необхідно обрати прийнятний метод сегментації, з конкретним рівнем деталізації, достатнім для того, щоб давати якомога більше інформації для вирішення поставлених завдань при мінімальних затратах часу.

Від якості виконання операції сегментування оптико-електронного зображення залежить кінцевий результат обробки зображення.

Елементи озброєння та техніки є досить контрастними і містять дуже багато геометрічних примітивів, прямих ліній та кіл.

Відомо, що одним з найбільш ефективних методів пошуку аналітично заданих примитівів є група методів, заснована на використанні перетворення Хафа.

Ця ідея може бути модифікована для випадку знаходження на зображенні різнорідних геометрічних примітивів, форма яких може бути описана певним аналітичним виразом.

Застосування при обробці зображення методу сегментування на основі перетворення Хафа в системі наведення FPV-дронів для виділення заданих об'єктів пошуку дасть змогу скоротити час на пошук, визначення та наведення на ціль ураження, що дозволить підвищити оперативність та якість роботи оператора FPV-дрона.

Матеріали даних досліджень можуть бути використані в подальшому під час створення та модернізації моніторингових систем.

УДК 681.396, 681.375

Старцев В.В., Леках А.А., Мусієнко О.П., Михальова Л.В

ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОЦЕСАХ АВТОМАТИЗАЦІЇ РУХУ ТА ОБЛІКУ МАТЕРІАЛЬНО-ТЕХНІЧНИХ ЗАСОБІВ ПІД ЧАС ВОЄННОГО СТАНУ

З початком здійснення повномасштабної збройної агресії з боку РФ одним із пріоритетних завдань Кабінету Міністрів України та Міністерства оборони України є вирішення питань постачання матеріально-технічних засобів (МтЗ) військового призначення для потреб ЗС України, які базуються на підписаних договорах та зобов’язаннях державних органів та інституцій західних партнерів і НАТО. Тому, в органах військового управління з питань логістичного забезпечення (ЛЗ) для здійснення систематичного контролю (стеження, супроводу) та визначення місця розташування військових вантажів необхідно удосконалювати системи моніторингу та трекінгу логістики ЗС України під час воєнного стану.

Використання сучасних технологічних рішень щодо удосконалення автоматизації обліку та руху матеріально-технічних засобів (МтЗ) може допомогти забезпечити автоматизований спосіб моніторингу найважливіших аспектів постачання товарів військового призначення. Для забезпечення безпеки держави вкрай важливо, щоб засоби та ресурси, що надаються ЗС України та військово-промисловому комплексу, були доступними, коли це необхідно. Щоб досягти максимально можливого рівня безпеки та підтримувати високу якість матеріальних ресурсів для військових потреб, важливо в умовах воєнного стану мати ефективну систему їх моніторингу та відстеження.

Система моніторингу та трекінгу переміщення МтЗ – це система постійного спостереження за явищами і процесами, які відбуваються під час переміщення МтЗ, результати якого служать для обґрунтування управлінських рішень по забезпеченню безпеки людей та об'єктів В рамках системи моніторингу та трекінгу переміщення МтЗ відбувається оцінка, контроль об'єкта, управління станом об'єкта залежно від впливу

певних факторів.

Під поняттям трекінг (англ. tracking – «відстеження, супровід») розуміється процес відстеження, супровід, визначення місця розташування рухомих об'єктів (озброєння та військової техніки, МтЗ) під час їх пересування за допомогою технічних систем та приладів.

Структура системи моніторингу та трекінгу переміщення МтЗ в загальній системі логістичного забезпечення ЗС України може складатися з наступних складових елементів (підсистем): підсистеми обліку, зберігання та пошуку необхідних МтЗ, відповідно до етапів постачання; підсистеми визначення місця знаходження транспортних засобів та контролю їх технічного стану; підсистеми забезпечення надійного двостороннього зв'язку та оперативного управління впродовж всього маршруту руху МтЗ; підсистеми оптимізації маршрутів доставки МтЗ, формування єдиної картини переміщення транспортних засобів логістики.

Принцип роботи системи контролю GPS моніторингу scheme-truck складається з того, що система супутникового моніторингу транспортних засобів об'єднує в собі дві основні складові, а саме бортове обладнання та програмне забезпечення.

Бортове обладнання – це, в першу чергу, GPS-трекер – пристрій для прийому-передачі даних в рамках супутникового контролю об'єкту. Основними функціональними елементами трекера є GPS-приймач, який за допомогою глобальної навігаційної системи (GPS, Galileo, Glonass, Beidou) визначає географічні координати транспортного засобу, та GSM-передавач який передає отриману інформація на сервер (або смартфон) через GPRS та SMS канали. Крім того, такий гаджет обладнується батареєю резервного живлення, картою пам'яті, антенами та іншим функціоналом (залежно від запиту). Також сюди відноситься периферійне обладнання, таке як датчики витрат пального, датчики температури, протиугінні системи та багато іншого, які під'єднуються безпосередньо до GPS-модуля.

Програмне забезпечення покликане опрацьовувати дані, які отримані з бортових приладів та трансформувати їх у визначений формат. Завдяки цьому користувач системи GPS-моніторингу має можливість он-лайн відстежувати місцезнаходження та маршрут об'єкту на електронній карті, отримувати показники витрат палива, швидкості, точки зупинок, місце й час заправок, зчитувати данні з бортового комп'ютера та багато іншого. Весь комплекс інформації є доступним не лише в режимі реального часу а й постфактум, тобто зберігається на сервері. Слід наголосити, що сервіс «FREETRACK» працює на програмному забезпеченні власної розробки, яке створювалось спеціально під запити українського ринку з урахуванням всієї його специфіки.

До технологій щодо обліку матеріальних ресурсів можливо застосовувати штрих-кодування, QR-кодування та RFID-технології. Найпоширенішою технологією контролю складських процесів е штрих-кодування. Свій розвиток рішення такого типу отримали внаслідок дешевизни та простоти використання. На відміну від штрих-коду, який сканують тонким променю, QR-код сприймається сенсором як двовимірне зображення. Основна перевага QR-коду – це легке розпізнавання сканувальним обладнанням.

Перевага використання RFID (Radio Frequency IDentification) – технологій полягає у безконтактній взаємодії радіомітки та радіозчитувача, завдяки якому відсутнє тертя, що прискорює зношування обладнання. З кожним роком, це рішення стає дешевшим і надійнішим. RFID-технологія може бути адаптована для різних сфер військової логістики, як вирішення загальних та специфічних завдань. Дана технологія найбільш сучасна та ефективна для відстеження ланцюжків постачання та контролю будь-яких товарів. При цьому не заперечує використання штрих-кодування для додаткового контролю, оскільки RFID зчитувачі можуть мати додатковий модуль bar-кодів. Спеціальні зчитувачі генерують електромагнітне поле. За допомогою антени в позначці цим полем заряджається конденсатор і передає інформацію, записану на мікрочипі, назад на зчитувач.

На підставі аналізу застосування різних способів автоматичної ідентифікації об'єктів

(МтЗ) при здійсненні процесу моніторингу та трекінгу переміщення військових вантажів у арміях держав членів НАТО, в доповіді розглядається структура системи моніторингу та трекінгу переміщення військових вантажів в загальній системі ЛЗ ЗС України, визначені основні принципи та режими роботи системи трекінгу та визначено найбільш просунуті технології автоматизації обліку та руху МтЗ, склад обладнання, основні принципи та режими роботи, переваги та недоліки їх застосування.

Аналіз проведених досліджень дозволяє стверджувати, що застосування сучасних технологій та систем автоматизації є дуже перспективним напрямком впровадження нових способів та методів ідентифікації, обліку та руху МтЗ військового призначення, скорочення термінів проведення інвентаризацій на складах військових частин.

Таким чином, автоматизація процесів ідентифікації об'єктів (МтЗ) при здійсненні процесу моніторингу та трекінгу переміщення військових вантажів має бути одним з пріоритетних напрямків роботи з підвищення ефективності діяльності логістики ЗС України. Створення нових і модернізація існуючих автоматизованих систем управління логістикою на основі передових інформаційних технологій, дозволить підвищити її ефективність, скоротити час на одержання і всебічну оцінку відомостей про МтЗ на всіх етапах їх руху, а також покращити взаємодію з аналогічними системами країн-партнерів НАТО.

Список використаних джерел

1. Про затвердження Порядку логістичного забезпечення сил оборони під час виконання завдань з оборони держави, захисту її суверенітету, територіальної цілісності та недоторканності : Постанова Кабінету Міністрів України від 27 грудня 2018 № 1208. https://zakon.rada.gov.ua/laws/show/1208-2018-%D0%BF. (дата звернення : 31.01.2025).
2. Положення з військових перевезень залізничним, морським, річковим та повітряним транспортом : Наказ Міністерства оборони України від 05 вересня 2013 № 595 https://zakon.rada.gov.ua/laws/show/z1662-13. (дата звернення : 31.01.20225).
3. Про впровадження у дослідну експлуатацію інформаційно-комунікаційної системи планування та управління логістичного забезпечення з використанням спеціалізованого програмного забезпечення LOGFAS : Наказ Міністерства оборони України від 18.08.2022 №242. https://www.mil.gov.ua/news/2022/10/21/ukraina-uspishno-integruetsya-v-nato-na-rivni-logistiki. (дата звернення : 31.01.2025).
4. Порядок кодифікації предметів постачання: Наказ Міністерства оборони України від 18.12.2017 № 673 https://zakon.rada.gov.ua/laws/show/z0050-18. (дата звернення : 31.01.2025).
5. Доктрина з організації переміщень та перевезень (транспортувань) у Збройних Силах України : Наказ Генерального штабу Збройних Сил України від 19.08.2020. https://sprotyvg7.com.ua/wp-content/uploads/2022/04.pdf. (дата звернення : 31.01.2025).
6. Гаврилюк І., Мацько О., Дашковський В. Концептуальні основи управління потоками в системі логістичного забезпечення Збройних Сил України. Сучасні інформаційні технології у сфері безпеки та оборони. – 2019. – № 34. – С. 37-44. DOI: https://doi.org/10.33099/2311-7249/2019-34-1-37-44.
7. Городнов В.П., Власюк В.В., Овчаренко В.В. Комплексна модель оцінювання ефективності та управління елементами матеріального забезпечення під час підготовки та в ході виконання службово-бойових завдань частинами (підрозділами) Національної гвардії України в особливий період // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. – № 1(26). – С. 123-132. http://nbuv.gov.ua/UJRN/Nitps_2017_1_27.
8. Кивлюк В.С., Ганненко Ю.О. Удосконалення системи забезпечення матеріальними ресурсами Збройних Сил України. Social development Security. – 2018. – № 2(4). – С. 49-58. URL: https://paperssds.eu/index.php/ JSPSDS/article/view/36/33.

9. Романченко І.С., Хазанович О.І., Трегубенко С.С.. Моделювання систем матеріально-технічного забезпечення: Монографія. – Львів: НАСВ ЗС України, 2015. – 156 с. http://www.irbis-nbuv.gov.ua.
10. Шуєнкін В.О., Ішутін І.С., Максименко М.Я. Понятійно-методичні аспекти обґрунтування вимог до системи забезпечення військ (сил) матеріально-технічними засобами: Збірник наукових праць ЦНДІ ЗС України. – 2013. – № 1(63). – С. 101-110. https://crsi.mil.gov.ua/collection-sct-papers.html.
11. RFID у транспортній логістиці. Електронний ресурс. Режим доступа: http://www.isbc-rfid.ru/applications/logistics/ (дата звернення: 30.01.2025).
12. Allied Joint Doctrine for Logistics, Edition B Version 1 (ADP 4-0 Sustainment). 2019. 84 с. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18450_ADP%204-0%20FINAL%20WEB.pdf. (дата звернення: 30.01.2025).
13. Joint Logistics, February 2019, Incorporating Change May 2019 («Доктрина об'єднана логістика», МО США). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp4_0ch1.pdf. (дата звернення: 30.01.2025).

УДК 2:004.056.53

Стратійчук І.О.

МЕТОД ФОРМУВАННЯ ВИМОГ ДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ВІД РАДІОКЕРОВАНИХ БОЄПРИПАСІВ НА АВТОМОБІЛЯХ ТА БРОНЕТЕХНІЦІ

Метод формування вимог до побудови системи захисту від радіокерованих боєприпасів на автомобілях та бронетехніці

У сучасних умовах ведення бойових дій, зокрема у збройних конфліктах асиметричного типу, широкого поширення набули радіокеровані боєприпаси (РКБ), які використовуються противником для дистанційного ураження особового складу та техніки. З огляду на це, побудова ефективної системи захисту автомобільної та бронетанкової техніки від РКБ є критично важливим завданням, що потребує науково обґрунтованого підходу до формування її технічних вимог.

Метод формування вимог до побудови такої системи ґрунтується на комплексному аналізі структури, принципу дії та характеристик каналів управління РКБ, а також враховує тактичні умови бойового застосування техніки. Основною метою методу є забезпечення високої ймовірності функціонального ураження РКБ за рахунок електромагнітного впливу на елементи їхньої радіоелектронної апаратури.

Ключовим елементом запропонованого підходу є використання циліндричної фазованої антенної решітки (ФАР), яка дозволяє формувати сфокусоване електромагнітне поле у заданій точці простору. Це дозволяє:

– автоматично адаптувати параметри випромінювання до умов розміщення техніки та змін у маршруті руху;
– збільшити дальність та ширину зони функціонального ураження;
– знизити рівень радіо- і візуальної помітності антенного пристрою.

Метод включає такі етапи:

1. Аналіз частотних характеристик каналів радіоуправління РКБ;
2. Визначення вимог до ЕМ-імпульсів за амплітудно-часовими параметрами для виводу з ладу приймальних пристроїв РКБ;
3. Моделювання зони ураження з урахуванням електромагнітної сумісності (ЕМС) з іншими РЕЗ на борту;
4. Розробка алгоритму адаптивного керування ФАР для забезпечення динамічного захисту в русі;

5. Обґрунтування інтеграції системи в конструкцію техніки з урахуванням бойового навантаження та просторових обмежень.

Використання даного методу дозволяє:

– зменшити залежність ефективності захисту від наявності розвідданих про РКБ;
– підвищити ймовірність нейтралізації загрози без безпосереднього контакту;
– забезпечити безперервне прикриття колони під час руху.

Метод формування вимог є основою для проектування мобільних систем радіоелектронного впливу, що можуть застосовуватися на платформах легких бронетранспортерів, броньованих автомобілів, спеціалізованих засобів супроводу.

Таким чином, запропонований метод створює передумови для розробки новітніх засобів захисту особового складу та техніки в умовах радіоелектронної протидії противника, сприяє підвищенню боєздатності підрозділів та загальному зміцненню системи державної безпеки.

УДК 621.396.67

Струкевич Д.І., Зелінська А.В., Алексєєва О.О., Площик А.С.

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ АНТЕН ДЛЯ СУПУТНИКОВОГО ЗВ’ЯЗКУ В ПОЛЬОВИХ УМОВАХ

Супутниковий зв'язок став невід'ємною частиною сучасних систем зв'язку, особливо там, де традиційна інфраструктура зв'язку може бути недоступною або пошкодженою. У цій статті розглядаються методи підвищення ефективності антенних систем для супутникового зв'язку, з особливим акцентом на їх застосування в польових умовах системою Satcom.

Ефективність супутникового зв'язку значною мірою залежить від характеристик антенної системи. Ключовими параметрами є коефіцієнт підсилення, який коливається від 15 до 45 дБ в залежності від застосування, частотного діапазону роботи та поляризаційних характеристик. [1]

Найчастіше використовуються діапазони: L (1-2 ГГц); S (2-4 ГГц); C (4-8 ГГц); X (8-12 ГГц); Ku (12-18 ГГц); Ka (26,5-40 ГГц).

Для роботи в польових умовах антени повинні відповідати специфічним вимогам. Конструкція має бути достатньо міцною, щоб витримувати механічні навантаження при транспортуванні та встановленні, але водночас легкою для мобільного застосування. Оптимальним рішенням часто є складані параболічні антени з діаметром рефлектора від 0,6 до 2,4 метрів, залежно від потреб зв'язку. [2]

Оптимізація геометрії рефлектора є одним з основних методів підвищення ефективності. Використання сучасних композитних матеріалів дозволяє створювати легкі та жорсткі конструкції з високою точністю поверхні. Важливим аспектом є забезпечення точності позиціонування антени. Для цього використовуються прецизійні механізми наведення з кроковими двигунами та системами автоматичного супроводу супутника. [3]

Сучасні антенні системи можуть містити адаптивні елементи, які автоматично компенсують зміни умов поширення сигналу. Це особливо важливо при роботі в Ka-діапазоні, де атмосферні явища можуть суттєво впливати на якість зв'язку. Використання адаптивних поляризаторів дозволяє оптимізувати прийом сигналів з різною поляризацією.

Сучасні технології виробництва дозволяють виготовляти високоточні компоненти для антенних систем різними методами. Одним з найперспективніших напрямків є адитивні технології, зокрема 3D-друк. Ця технологія має низку переваг: швидке

створення прототипів, відносно низька собівартість виробництва і висока точність для деталей зі складною геометрією. При правильному виборі матеріалів та налаштуванні параметрів друку можна досягти необхідної точності виготовлення компонентів антенних систем.

При виготовленні антен для польового застосування особливу увагу слід приділяти технологіям, що забезпечують необхідну точність при прийнятній вартості. Використання сучасних методів 3D-друку дозволяє створювати складні елементи конструкції з високою точністю. Важливим є вибір матеріалів з відповідними механічними та електричними характеристиками.

Ефективність антени значною мірою залежить від конструкції системи живлення та опромінювача. Використання гофрованих рупорних опромінювачів забезпечує оптимальне опромінення поверхні рефлектора та мінімізує рівень бічних пелюсток. Важливим є забезпечення узгодження імпедансів у широкій смузі частот. [4]

Для роботи в польових умовах необхідно забезпечити надійний захист антени від атмосферних впливів. Використання спеціальних покриттів та герметичних корпусів для електронних компонентів є обов'язковим. Система повинна зберігати працездатність при температурах від -40 до +60°C та відносній вологості до 100%.

Точне налаштування антени є критичним для забезпечення максимальної ефективності. Розроблені спеціальні методики польового калібрування, які дозволяють оптимізувати параметри антени безпосередньо на місці експлуатації. Використання вбудованих датчиків та програмного забезпечення спрощує процес налаштування. [5]

В польових умовах важливим аспектом є енергоефективність антенної системи. Використання сучасних малошумлячих підсилювачів та енергоефективних систем наведення дозволяє мінімізувати енергоспоживання. При цьому важливо забезпечити стабільність характеристик при різних режимах роботи.

Сучасні антенні системи повинні легко інтегруватися з різними системами управління та моніторингу. Використання стандартних інтерфейсів та протоколів забезпечує сумісність з різним обладнанням. Важливим є забезпечення можливості віддаленого управління та діагностики. [6]

При розробці антенних систем для польового застосування важливо знайти оптимальний баланс між характеристиками та вартістю. Використання модульної конструкції дозволяє спростити обслуговування та ремонт. Важливим є врахування повної вартості володіння, включаючи витрати на встановлення та обслуговування.

Розвиток технологій відкриває нові можливості для підвищення ефективності антенних систем. Використання метаматеріалів дозволяє створювати антени з покращеними характеристиками. Перспективним є застосування активних фазованих решіток для створення багатопроменевих систем. [7]

Для роботи через супутники Satcom використовується діапазон частот X-band (7.25-7.75 ГГц (приймання) з довжиною хвилі робочого діапазону та 7.9-8.4 ГГц (передавання) з довжиною хвилі. При самостійному виготовленні антен для роботи супутники Satcom необхідно враховувати ряд важливих факторів. Перш за все, потрібно точно визначити необхідні параметри: робочий діапазон частот, необхідний коефіцієнт підсилення та тип поляризації. Важливо забезпечити високу точність виготовлення рефлектора - відхилення від теоретичної поверхні не повинно перевищувати $\lambda/16$ [8].

Підвищення ефективності антен для супутникового зв'язку в польових умовах вимагає комплексного підходу, що враховує множину факторів. Використання сучасних технологій та матеріалів дозволяє створювати системи з високими технічними характеристиками при збереженні прийнятної вартості. При самостійному виготовленні антени критичним є забезпечення необхідної точності та якості конструкції.

Особлива увага повинна приділятися питанням надійності та зручності експлуатації в польових умовах. Розвиток технологій відкриває нові можливості для вдосконалення антенних систем, що дозволяє забезпечити все більш ефективний супутниковий зв'язок у різноманітних умовах застосування.

Список використаних джерел

1. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/ laws/show/1089-IX#Text (дата звернення: 14.12.2023).
2. Про космічну діяльність: Закон України від 15.11 1996 №502/96-ВР. URL: https://zakon.rada.gov.ua/rada/ show/502/96-%D0%B2%D1%80#top (дата звернення: 14.12.2023).
3. Військова публікація: ВКДП 6-135(03).01. Настанова Супутниковий зв’язок. Затверджена наказом КВЗ та КБ ЗСУ від 24.12.2020. Київ: КВЗ та КБ ЗСУ, 2020, 36 с.
4. Військова публікація: ВКП 6-00(01).01. Доктрина Зв’язок та інформаційні системи. Затверджена ГК ЗС України від 01.07.2020. Київ: ЦУЗ та ІС ГШ ЗСУ, 2020, 78 с.
5. Гуржій П.М., Зарубенко А.О., Палівода В.С., Колодійчук Л.В. Методичні рекомендації з налаштування станції супутникового зв’язку Starlink. Київ : ВІТІ ім. Героїв Крут, 2023. 30 с.
6. Ніколаєнко Б.А., Пелешок Є.В. Сучасні супутникові системи зв’язку: навч. посіб. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2022. 146 с.
7. Шевченко Д.Г., Зінченко А.О., Розум І.Ю. Комплекси, системи та засоби військових телекомунікаційних мереж: навч. посіб. Київ.: НУОУ ім. Івана Черняховського, 2019. 319 с.
8. Білий О.А., Шолудько В.Г., Малих В.В., Гай Ю.І. Перспективи розвитку системи супутникового зв’язку ЗС України. Збірник наукових праць ВІТІ. 2018. Вип. 2. С. 6–15.
9. Про схвалення Концепції Загальнодержавної цільової науково-технічної космічної програми України на 2021–2025: Розпорядження Кабінету Міністрів України № 15-р від 13.01.2021. URL: https://zakon.rada.gov.ua/laws/show/15-2021-(дата звернення: 14.12.2023).

Тарасенко А.В., Кобзєв В.Г.

ВИКОРИСТАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗБОРУ ІНФОРМАЦІЇ З ІНТЕРНЕТ-РЕСУРСІВ

З появою потужних інструментів для автоматизації обробки тексту та аналізу даних, штучний інтелект (ШІ) впевнено закріпився в численних галузях, зокрема у процесах дослідження та моніторингу веб-ресурсів з метою збору необхідної інформації. Величезний обсяг веб-контенту у різних предметних областях щодня зростає і потребує швидкої та якісної обробки. Звичайні методи дослідження на кшталт ручного пошуку та збереження даних не дають змоги впоратися з потоками інформації належним чином. Гнучкі рішення для виконання таких завдань сьогодні пропонують засоби ШІ, даючи змогу фільтрувати, структурувати й аналізувати дані у масштабах, недоступних для засобів, які існували раніше. Завдяки сучасним технологіям суттєво змінюються самі уявлення про те, як можна отримувати та аналізувати дані.

Безумовно, однією з головних переваг автоматизованого збору інформації є суттєве прискорення процесу. ШІ-рішення спроможні обробити колосальні обсяги даних за короткий час і виявити закономірності, важливі для конкретної сфери. Водночас при впровадженні таких технологій виникають і певні виклики. Юридичні обмеження та

правила про конфіденційність вимагають ретельно перевіряти джерела даних і способи їх обробки. Не менш важливо слідкувати за етичними аспектами: алгоритми можуть успадковувати або підсилювати упередження, закладені в даних. Тому вибір, якісне навчання моделей і контроль за їхнім використанням є одним із пріоритетів для всіх, хто має справу з ШІ [1].

Наведені виклики потребують усунення для більш ефективного використання засобів ШІ, оскільки це допоможе оптимізувати процес і покращити результати збору даних з використанням ШІ. Наведемо можливі дослідження та методи для усунення вказаних викликів:

1) дослідження ефективності різних ШІ-моделей (наприклад, ChatGPT, Claude, Llama і DeepSeek) при вирішенні задачі збору інформації в Інтернеті. Це дозволить створити дослідницьку базу для створення програмного забезпечення (ПО), яке буде виконувати задачі збору інформації з інтернет-ресурсів;

2) використання динамічної системи комбінування різних ШІ-моделей. Це дозволить оперативно використовувати різні ШІ-моделі для окремих задач та проводити заміни ШІ-моделей коли одна з них не зможе повноцінно виконати поставлену задачу;

3) створення нової ШІ-моделі, яка буде навчатися на результатах та процесах існуючих ШІ-моделей на базі розробленого ПО. Це дозволить з часом відмовитися від існуючих ШІ-моделей та їх обмежень, що надасть розробленому ПО можливість більшої автономії [2].

Засоби штучного інтелекту відкривають нові можливості для ефективного збору та аналізу інформації з веб-ресурсів. Утім, щоб така технологія працювала коректно для поставлених цілей, необхідно проводити додаткові дослідження та дотримуватися принципів етичного використання даних і зважати на юридичні аспекти. За умови грамотної інтеграції ці інструменти стануть незамінними помічниками в науці, бізнесі, медіа та багатьох інших сферах.

Список використаних джерел

1. Weerasinghe M. Enhancing Web Scraping with Artificial Intelligence: A Review // 4th Research Symposium of Faculty of Computing KDU, Sri Lanka, 2024. P. 22.
2. Padraig Cunningham, Matthieu Cord, Sarah Jane Delany. Supervised Learning // Machine Learning Techniques for Multimedia, 2008. P. 21-49.

УДК 004.056:378.147:355

Терещенко І.О., Лученко Я.В., Каук В.І.

АДАПТИВНІ ОСВІТНІ СИСТЕМИ ЯК ІНСТРУМЕНТ ПІДГОТОВКИ КАДРІВ З КІБЕРБЕЗПЕКИ В СИЛОВИХ СТРУКТУРАХ

У контексті зростаючої цифрової загрози та інтенсивної мілітаризації кіберпростору особливого значення набуває ефективна підготовка фахівців з кібербезпеки, зокрема у силових структурах. Сучасна аналітика вказує на суттєвий дисбаланс між вимогами ринку кібербезпеки та реальними навичками випускників відповідних освітніх програм. За даними [1], глобальний дефіцит кадрів у сфері кібербезпеки перевищує 3 мільйони, при цьому кваліфікація більшості претендентів не відповідає вимогам роботодавців. Основні розриви знань простежуються у напрямах управління безпекою, безпеки програмного забезпечення, комплаєнсу та сертифікації, а також інтелекту про кіберзагрози.

Особливістю освітнього процесу для силових структур є наявність специфічних вимог[2]: обмежений час на навчання, потреба в захищеності даних, підвищене

значення практичних навичок (цифрова криміналістика, інцидент-менеджмент, етичний хакинг), а також потреба в адаптації навчального контенту до типу служби (наприклад, військові, поліція, спецслужби). Як свідчить дослідження [3], більшість чинних навчальних програм недостатньо гнучкі, а підходи до підготовки персоналу є переважно однотипними й не враховують розмаїття початкових компетентностей.

У цьому контексті адаптивні освітні системи (АОС) виступають як ефективний інструмент індивідуалізації підготовки. АОС аналізують поточний рівень знань, навчальні цілі, темп навчання і навіть особистісні характеристики здобувача, коригуючи траєкторію та складність навчання в реальному часі. За даними [4], [5], такі системи суттєво покращують успішність та підвищують залученість. Адаптивне оцінювання компетентностей дозволяє виявити не лише знання, а й хід мислення, поведінкові шаблони й рівень критичного мислення — що особливо актуально для кадрів кібербезпеки.

У сфері безпеки доцільним є поєднання АОС із симуляційними платформами, CTF-змаганнями та системами сценарного навчання. Наприклад, робота [6] підкреслює потенціал штучного інтелекту у цифровій криміналістиці та важливість навчання персоналу роботі з AI-системами для попередження кіберзагроз у режимі реального часу. Це також потребує розбудови освітніх програм, орієнтованих на Explainable AI, цифрову етику та розуміння обмежень алгоритмів.

Значущість адаптації освітнього контенту до ролі слухача підтверджена дослідженням [3], де встановлено, що найбільш важливим фактором ефективного навчання у сфері кібербезпеки є саме посадова роль. Отже, створення персоналізованих програм для, наприклад, аналітиків загроз, цифрових слідчих або спеціалістів SOC – необхідна умова підвищення якості кадрів.

Серед українських досліджень варто відзначити роботу [7], яка пропонує модель побудови адаптивної освітньої траєкторії з урахуванням індивідуальних особливостей, навчальних цілей та обмежень у часі. Застосування таких алгоритмів у середовищах дистанційного або гібридного навчання є перспективним інструментом підвищення ефективності підготовки фахівців.

Підготовка кадрів з кібербезпеки у силових структурах потребує переосмислення класичних підходів, зокрема з урахуванням досвіду США щодо перепрофілювання ветеранів через програми швидкої підготовки, як-от CREATES [8]. Адаптивні освітні системи дозволяють зменшити дефіцит навичок, підвищити швидкість та якість підготовки, враховуючи як технічні, так і поведінкові аспекти навчання.

Список використаних джерел

1. Goupil F., Laskov P., Pekaric I., Felderer M., Dürr A., Thiesse F. Towards Understanding the Skill Gap in Cybersecurity // ITiCSE ’22. – 2022. – ACM. – DOI: 10.48550/arXiv.2204.13793.
2. Hag A., Bhadauria V., Gibson C., Neupane R., Creider D. A conceptual learning framework of cybersecurity education for military and law enforcement: workforce development // International Journal of Smart Education and Urban Society. – 2022. – Vol. 13. – P. 1–14. – DOI: 10.4018/IJSEUS.309953.
3. Ben Salamah F., Palomino M. A., Papadaki M., Furnell S. The Importance of the Job Role in Social Media Cybersecurity Training // Proceedings of the Euro S&P Workshops. – 2022. – IEEE. – DOI: 10.1109/EuroSPW55150.2022.00054.
4. Khan M. Impact of Personalized Learning Paths on Student Motivation and Achievement in Online High School Programs in Pakistan // International Journal of Online and Distance Learning. – 2024. – Vol. 5, No. 2. – P. 52–61. – DOI: 10.47604/ijodl.2748.
5. Hakim N., Jastacia B., Mansoori A.A. Personalizing Learning Paths: A Study of Adaptive Learning Algorithms and Their Effects on Student Outcomes // Journal Emerging Technologies in Education. – 2024. – Vol. 2, No. 4. – DOI: 10.70177/jete.v2i4.1365.

6. Zaman K.T., Zaman S., Bai Y., Li J. Empowering Digital Forensics with AI: Enhancing Cyber Threat Readiness in Law Enforcement Training // SSRN. – 2024. – [Електронний ресурс]. – Режим доступу: https://ssrn.com/abstract=5039717
7. Barchenko N., Tolbatov A., Lavryk T., Tolbatov V., Obodiak V., Yakovliev V., Motorin Y., Artamonov Y. An Approach to the Formation of Adaptive Learning Paths for Students of Cybersecurity in E-learning System // CMiGIN 2022: 2nd International Conference on Conflict Management in Global Information Networks. – CEUR Workshop Proceedings. – 2022.
8. Zantua M., Dupuis M. Re-engineering the Cybersecurity Human Capital Crisis // University of Washington. – 2015. – [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/305778185

УДК 004.4

Ткаченко К.М., Лазарев В.Д.

ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ XMIND У НАВЧАЛЬНОМУ ПРОЦЕСІ

Сучасні тенденції цифровізації освіти вимагають використання інноваційних програмних засобів для підвищення ефективності навчального процесу. Одним із таких інструментів є програмне забезпечення Xmind, він дозволяє створювати ментальні карти для структуризації та візуалізації знань. Незважаючи на популярність цього підходу, необхідно більш детально дослідити ефективність Xmind у навчальній діяльності, зокрема його вплив на засвоєння матеріалу, розвиток когнітивних навичок здобувачів вищої освіти та його інтеграцію з іншими освітніми платформами.

Значна кількість освітніх установ активно впроваджує цифрові інструменти у навчальний процес, проте не всі з них дозволяють забезпечити комплексний підхід до організації знань та розвитку аналітичного мислення. Саме тому Xmind становить особливий інтерес як програмний продукт, що поєднує гнучкість, простоту у використанні та багатофункціональність.

Ментальні карти давно використовуються у сфері освіти для структуризації навчального матеріалу, візуалізації знань та розробки стратегій навчання. Дослідження підтверджують, що використання таких інструментів сприяє глибшому розумінню матеріалу та підвищенню академічної успішності. У порівнянні з традиційними методами ведення конспектів, використання Xmind дозволяє значно прискорити процес запам’ятовування та аналізу інформації.

Програмні аналоги Xmind, такі як MindMeister, FreeMind, SimpleMind, також забезпечують можливості для створення ментальних карт, проте Xmind має значні переваги. Зокрема, він відзначається інтуїтивним інтерфейсом, гнучкими налаштуваннями дизайну, підтримкою командної роботи та інтеграцією з популярними сервісами, такими як Evernote, Microsoft Office та Google Docs. Окрім цього, Xmind підтримує роботу з великими обсягами інформації, що особливо корисно для наукових досліджень та систематизації знань у вищій освіті.

Xmind надає широкі можливості для візуалізації знань та організації навчального матеріалу. Основні переваги програми включають:

– гнучкість у створенні, редагуванні та персоналізації ментальних карт;

– можливість колективної роботи в режимі реального часу, що підвищує інтерактивність навчання;

– інтеграцію з іншими програмами та платформами, що сприяє ефективному управлінню освітнім контентом;

– підтримку різних форматів експорту, що дозволяє адаптувати матеріали під конкретні освітні завдання;

– використання засобів аналітики для візуалізації взаємозв'язків між концепціями, що покращує процес ухвалення рішень та стратегічного планування в навчанні;

– можливість ведення нотаток, додавання зображень, посилань та інших мультимедійних елементів для збагачення навчального матеріалу.

Застосування Xmind у навчальному процесі дає змогу здобувачам вищої освіти краще структурувати знання, аналізувати складні концепції та розвивати критичне мислення. Викладачі, у свою чергу, можуть ефективніше організовувати навчальні модулі, візуалізувати зв'язки між темами та покращувати контроль засвоєння матеріалу.

Досвід застосування Xmind у вищих навчальних закладах підтверджує, що програма може використовуватися не лише для конспектування, але й для планування проектів, організації групової роботи та моделювання процесів прийняття рішень. Вона також є корисним інструментом для дистанційного навчання, дозволяючи здобувачам вищої освіти ефективно взаємодіяти у віртуальному середовищі. Зокрема, у рамках онлайн-курсів Xmind може слугувати візуальним навігатором для проходження навчальних модулів, полегшуючи орієнтацію в матеріалах курсу.

Додатково варто відзначити можливість використання Xmind у дослідницькій діяльності, коли необхідно систематизувати велику кількість літературних джерел, визначити ключові концепції та побудувати логічні зв'язки між ними. Цей підхід дозволяє покращити якість наукових досліджень і сприяє швидкому доступу до важливої інформації.

Використання Xmind у навчальному процесі значно підвищує ефективність освітнього процесу, сприяє кращому сприйняттю інформації та стимулює розвиток когнітивних навичок здобувачів вищої освіти. Інструмент надає можливість створювати інтерактивні навчальні матеріали, покращувати комунікацію між учасниками навчального процесу, а також забезпечує ефективний контроль за прогресом у навчанні.

Подальші дослідження можуть бути спрямовані на розробку методик впровадження Xmind у різні навчальні дисципліни, оцінці його впливу на рівень засвоєння знань і навчальну мотивацію здобувачів вищої освіти, а також розширенні функціоналу для покращення інтеграції з іншими освітніми платформами. Досвід використання Xmind може стати корисним для освітян, які прагнуть оптимізувати викладання та створити ефективне навчальне середовище з використанням сучасних цифрових технологій.

УДК 332.3:510.6

Толстов О.С.

КОРЕЛЯЦІЙНО-ЕКСТРЕМАЛЬНИЙ МЕТОД ВИМІРУ КУТА ФАЗОВОГО ЗСУВУ

Метрологічне забезпечення багатьох зразків ОВТ передбачає операції вимірювання КФЗ. Наприклад, радіолокаційні курсо-глисадні системи забезпечення зльоту та посадки літаків, декілька типів контрольно-перевірочних машин тактичних, оперативно-тактичних ракетних комплексів, керованого протитанкового озброєння, гідролокаційні станції кораблів ВМС, радіолокаційні станції, зенітно-ракетні комплексі, при полігонних іспитах зразків ОВТ та інші.

Система передачі одиниці кута фазового зсуву у Збройних Силах України вимагає забезпечення єдності і вірогідності вимірювань кута фазового зсуву між двома електричними коливаннями на рівні (0,1–0,01)°.

Існують багато методів вимірювання КЗФ між двома напругами в залежності від їх математичних моделей, реалізації, різноманітних алгоритмів. Найрозповсюдженими методами прямого перетворення для вимірювання КЗФ є осцилографічні методи, методи з перетворенням КЗФ на струм чи напругу та методи з перетворенням КЗФ на число імпульсів. При використанні методом зрівноважуючого перетворення вимірюваний КЗФ порівнюється з КЗФ, що створюється за допомогою каліброваного фазообертача. Застосовують параметричні, кругові фазообертачі та фазообертачі у вигляді лінії затримки. Похибка фазообертача залежить від точності виготовлення та стабільності його елементів, робочої частоти і опору навантаження. У кореляційному та ортогональному методах вимірювання КЗФ визначають лише по двох точках, не використовуючи іншу інформацію. Наявність вищих гармонік в сигналах та шумів у вхідному колі приладів призводить до зміни моменту переходу через нуль перших гармонік сигналів, тобто змінюється значення КЗФ і з’являються значні похибки [1].

Фахівцями Метрологічного центру військових еталонів в рамках НДР «Удосконалення макетного зразка вихідного еталону військового призначення для вимірювання кута фазового зсуву двох гармонійних сигналів в діапазоні частот від 5 Гц до 10,0 МГц», шифр «Такт» [2] запропонований кореляційно-екстремальний метод виміру кута фазового зсуву. Принципова відмінність цього методу від методів визначення кута фазового зсуву застосовуваних у доступній вимірювальній апаратурі складається у використанні інформації, що міститься у формі сигналу, а не тільки в окремих характерних точках. Сучасна комп'ютерна техніка дозволяє накопичувати достатні масиви даних і обробляти по запропонованому алгоритму. При цьому похибка не перевищує декількох тисячних градуса, що з запасом покриває потреби.

Список використаних джерел

1. Олег Величко, д.т.н., проф., Юлія Куліш. Автоматизація вимірювань на державному еталоні одиниці кута зсуву фаз між двома напругами Державне підприємство «Укрметртестстандарт», Україна; ISTCMTM.2023; Випуск 84(1). С. 18-24. https://doi.org/10.23939/istcmtm2023.01.018.
2. Удосконалення макетного зразка вихідного еталону військового призначення для вимірювання кута фазового зсуву двох гармонійних сигналів в діапазоні частот від 5 Гц до 10,0 МГц. НДР, шифр «Такт». Звіт. –Харків.: НМЦ (ВЕ), 2004. – 63 с.

УДК 621.317.3

Уднiков О.М., Шеховцова І.О., Климченко С.В.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНОГО ВИМІРЮВАЛЬНОГО ОБЛАДНАННЯ ПРИ КАЛІБРУВАННІ ВИМІРЮВАЧІВ ПОТУЖНОСТІ ЕЛЕКТРОМАГНІТНИХ КОЛИВАНЬ НАДВИСОКОЇ ЧАСТОТИ

Комплектування вихідних еталонів Збройних Сил України новітніми зразками вимірювальної техніки є одним із основних напрямків розвитку еталонної бази. Використання сучасних засобів вимірювань надає можливість змінити процес отримання вимірювальної інформації, скоротити час виконання вимірювань, автоматизувати процес виконання калібрувальних робіт, усунути надлишкове вимірювальне обладнання.

На виконання Програми розвитку еталонної бази Збройних Сил України Вихідний еталон одиниці потужності електромагнітних коливань в коаксіальних трактах було укомплектовано генератором сигналів високочастотним Keysight N5173B та вимірювачем потужності Keysight U8481A–100.

На ряду з безперечними перевагами використання сучасного вимірювального обладнання є і ряд недоліків, які пов'язані з тим, що в якості робочих еталонів, які калібруються, є застарілі перетворювачі падаючої потужності типів Я2М-21…Я2М-22 та ватметри прохідні зразкові типів ВПО-1…ВПО-4, тип вхідних та вихідних роз'ємів яких 7/3, що не відповідає роз'ємам сучасного обладнання (тип N). Крім того, нестабільність вихідного сигналу генератора Keysight N5173B за рівнем потужності складає близько $3 \cdot 10^{-4}$ дБ, що не дає змоги отримати сигнал вимірювальної інформації з необхідною точністю. У вимірювача потужності Keysight U8481A–100 відсутній канал загального користування GPIB (IEEE 488.2), до якого підключені інші прилади зі складу еталона. Комунікація з вимірювачем потужності Keysight U8481A–100 може виконуватися тільки в автоматичному режимі через інформаційний канал USB. Перетворювачі падаючої потужності Я2М-23 та Я2М-24 на початкових частотах мають значне перехідне ослаблення між входом та виходом (до 25 дБ), що значно зменшує рівень вихідного сигналу (при максимальному значенні вихідної потужності генератора Keysight N5173B відбувається ослаблення сигналу на вході вимірювача потужності Keysight U8481A–100 на рівні 1-2 мВт).

Усунення вище наведених проблем здійснюється наступним чином. Для з'єднання з типу 7/3 на тип N використовується безшайбовий перехід. З метою виключення похибки, пов'язаної з використанням безшайбового переходу, калібрування вимірювача потужності Keysight U8481A–100 в органах національної метрологічної служби здійснюється разом з переходом. Вплив нестабільності вихідної потужності генератора Keysight N5173B зменшуємо за рахунок проведення багатократних вимірювань з наступною обробкою отриманих результатів, які виконуються в автоматичному режимі за допомогою розробленого програмного забезпечення. Інформаційний канал вихідного еталона сформований з двох інформаційних каналів USB та GPIB (IEEE 488.2), через які під час вимірювального процесу здійснюється комунікація з приладами зі складу еталона. Для зменшення впливу перехідного ослаблення між входом та виходом перетворювачів падаючої потужності Я2М-23 та Я2М-24 на початкових частотах вимірювання коефіцієнта перетворення здійснюється на рівні сигналу, близького до 1 мВт. У подальшому планується закупівля підсилювача потужності, що дозволить підвищити рівень потужності на вході вимірювача потужності Keysight U8481A–100.

УДК 004.89:355

Ушаков В.А.

ОГЛЯД МОЖЛИВОГО ВИКОРИСТАННЯ СПЕЦІАЛІЗОВАНИХ МОДЕЛЕЙ CHAT GPT У НАВЧАЛЬНОМУ ПРОЦЕСІ

Стрімкий розвиток штучного інтелекту та його інтеграція у сферу освіти створює нові можливості для організації навчального військових здобувачів вищої освіти. Використання користувацьких моделей чату GPT дає змогу покращити якість підготовки викладачів до занять та засвоєння навчального матеріалу навчаємими, автоматизувати оцінювання знань із застосуванням різних модельованих користувачем сценаріїв. У цій роботі розглядаються основні підходи до застосування мовних моделей у навчальному процесі, їх переваги, виклики та перспективи розвитку.

Актуальність теми полягає в необхідності застосування передових інформаційних технологій для реалізації сучасних методів підготовки військових фахівців. GPT-моделі дозволяють створювати інтелектуальні навчальні середовища, адаптовані до індивідуальних потреб всіх учасників навчального процесу. В умовах зростаючої складності інформаційного простору такі технології забезпечують швидке оновлення знань, інтерактивне навчання та симуляцію реальних ситуацій, дозволяють значно розширити можливості як викладачів так і здобувачів вищої освіти в тому числі завдяки оптимізації часу за рахунок автоматизації рутинних процесів.

Сучасні користувацькі моделі GPT поділяються на три основні категорії:

– стандартні GPT-моделі – можуть використовуватись для генерації текстів, пояснення складних понять, адаптації матеріалу під рівень знань навчаємих.

– спеціалізовані (fine-tuned) GPT-моделі – мають змогу налаштовуватись на вибіркову тематику в тому числі військову, дозволяють моделювати та аналізувати різні сценарії, автоматизувати процеси оцінювання знань.

– інтерактивні чат-боти на основі GPT – можливо використовувати для навчання у форматі рольових ігор, тренування комунікацій у різних модельованих середовищах та ситуацях.

Для розуміння вищезгаданого слід розглянути найбільш доступні практичні інструменти ChatGPT, які можуть бути застосованими у навчальному процесі:

1. «Мої GPT» – самостійне створення користувачем спеціалізованих навчальних моделей:

– розробка налаштованих мовних моделей для підготовки до занять, пояснення складних тем та формування навчальних і наукових матеріалів різних напрямків;

– використання інструкцій для створення адаптованих асистентів потрібної спеціалізації в тому числі, наприклад, для військової тематики, тактичних задач, технічних пояснень тощо;

– налаштування GPT для автоматизації проведення опитувань, тестування знань та створення варіативних тестових завдань;

2. «Проекти» – робота з тематичними проектами, в тому числі колективна:

– робота з багатоконтекстними науковими та навчальними матеріалами, такими як посібники, підручники, наукові статті тощо;

– організація групової роботи над навчальними і науковими проектами, обговорення складних питань, колективне створення навчальних та наукових матеріалів;

– використання для аналізу реальних кейсів, розробки спільних рішень у навчальному середовищі;

– автоматизована перевірка та аналіз текстів, виявлення помилок та вдосконалення формулювань;

3. «Глибоке дослідження» – розширення доступу до інформації (знань):

– автоматизований аналіз матеріалів, підготовка коротких довідкових витягів, структуризація інформації;

– пошук актуальних джерел інформації, огляд новітніх технологій за вказаною тематикою;

– створення адаптованих підручників, конспектів і навчальних програм для курсантів за результатами поглибленого пошуку та аналізу інформації з відкритих джерел в інтернеті або доданої користувачем.

Звичайні та тимчасові чати – інтерактивне навчання:

– використання GPT як персонального навчального асистента для консультацій, пояснень та обговорень навчальних тем;

– створення сценаріїв навчальних діалогів, імітація різних ситуацій для тренування комунікаційних навичок;

– проведення експрес-опитувань та оперативний зворотний зв’язок після проведених занять.

Виклики та ризики:

– контроль якості та точності отриманої інформації, потенційні неточності у відповідях потребують корекції викладачем;

– використання GPT у рамках безпечного навчального середовища, наявні ризики інформаційної безпеки;

– необхідність розробки методичних рекомендацій для викладачів щодо оптимального використання мовних моделей та їх адаптації до специфіки занять.

Висновки. Впровадження спеціалізованих моделей ChatGPT у навчальний процес військових фахівців значно покращує персоналізацію навчання, дозволяє автоматизувати частину викладацьких завдань та сприяє розвитку інтерактивних підходів у навчанні. Використання інструментів ChatGPT дозволяє також розширити можливості курсантів у самостійному опрацюванні матеріалу та підготовці до занять. Водночас, ефективна інтеграція цих технологій потребує розробки методичних рекомендацій, контролю якості генерованого контенту та дотримання принципів інформаційної безпеки. Подальший розвиток цієї технології потребує удосконалення методик навчання та їх адаптації до специфіки військової освіти.

Федоров О.Ю., Томчук О.А., Циганков П.М., Варванець Ю.В.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ СИЛАМИ ОБОРОНИ УКРАЇНИ У ХОДІ ВІДСІЧІ ШИРОКОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Аналіз застосування сил оборони України у ході ведення Антитерористичної операції, Операції об’єднаних сил та відсічі широкомасштабної збройної агресії російської федерації проти України дозволяє дійти висновків, що кількість та якість озброєння і військової техніки, що знаходяться на озброєнні протидіючих сторін і надалі залишається вирішальним фактором для досягнення успіху у війні. У той же час, враховуючи сучасні тенденції розвитку форм та способів ведення збройної боротьби, що пов’язані із зростанням динамічності і маневреності дій військ (сил), розширенням бойового простору та масштабів збройної боротьби, застосування новітніх зразків озброєння і воєнної техніки домінуючої ролі набуває така функція як - управління військами (силами). Саме покращення скорочення і оптимізація циклу бойового управління, підвищення ситуативної обізнаності командирів (начальників), обґрунтованість та оперативність прийняття ними рішень дозволяють суттєво підвищити ефективність дій військ (сил), та як наслідок – забезпечити стримування просування переважаючого противника, а у майбутньому - здобути перевагу над ним. Для вирішення цих завдань силами безпеки та оборони України серед широко кола заходів і застосовуються сучасні інформаційні технології. Їх впровадження у бойову діяльність сил оборони забезпечує: створення єдиного інформаційного середовища як на оперативному так і на тактичному рівнях; оперативне і гнучке управління в режимі реального часу військовими формуваннями включно до бойової машини та окремого військовослужбовця; глибоку ситуаційну обізнаність командирів (начальників); оперативний обмін текстовою, графічною та іншою інформацією; постійний контроль за ходом виконання завдань в реальному режимі часу; накопичення та оброблення інформації тощо.

Значний прогрес в області інформаційних технологій на сьогоднішній день дозволяє технічно реалізувати можливості по створенню систем управління, автоматизованого

прийняття рішення, управління просторовими даними які відповідатимуть вимогам по забезпеченню взаємної узгодженості як між собою так і з системами збору і обробки розвідувальних даних, датчиками (сенсорами) систем озброєння і визначення місцезнаходження будь яких об'єктів на місцевості, створення єдиного інформаційно-комунікаційного простору в якому усі елементи бойового прядку, включаючи окремого військовослужбовця, матимуть можливість здійснювати обмін інформаційний потоком в реальному масштабі часу. І з кожним роком ці можливості тільки зростають. Так наприклад, якщо у ході ведення Антитерористичної операції силами оборони використовувалися лише окремі програмно - апаратні продукти такі як «КОМБАТ» та «ГІС АРТА» то вже сьогодні мова йде про комплекси спеціального програмного забезпечення «Дельта», «Кропива-Д», «Дзвід-АС», «АС ЦОК», «ВІРАЖ-планшет» тощо. Їх використання у бойовій діяльності суттєво підвищує спроможності сил оборони та забезпечує: інтеграцію інформаційних ресурсів різнотипних інформаційних та автоматизованих систем; створення єдиного геоінформаційного та інформаційно-аналітичного середовища органів військового управління, військових частин та підрозділів Збройних Сил України та інших складових сил оборони; збір, обробку та видачу інформації про повітряну і надводну обстановку тощо.

Водночас, підвищення ефективності управління силами оборони України за рахунок використання лише комплексу засобів автоматизації управління неможливе без запровадження сучасних методик прийняття рішення, оптимізації організаційно-штатних структур органів управління та штабів, удосконалення системи пунктів управління. Саме тому в Збройних Силах України запроваджуються передові методики прийняття рішення, що застосовується в збройних силах країн – членів НАТО такі як TLP (troop leading procedures) та MDMP (military decision making process). Зазначені алгоритми роботи вже закладено у проекти новітніх Бойових статутів механізованих і танкових військ. Триває плановий перехід органів військового управління Збройних Сил України на структури типу «G» з розподілом між ними функцій із формування, підготовки, розвитку і забезпечення військ (сил) та функцій з управління застосуванням військами (силами) під час ведення операцій (бойових, спеціальних дій). На тактичному рівні відбувається перехід штабів військових частин на структури типу «S». Що стосується системи пунктів управління слід зауважити, що тривалий час відбувається дискусія щодо напрямків вдосконалення їх існуючої структури та її уніфікації, доцільності створення нових елементів таких як Тактичний операційний центр (Tactical Operation Center) – структурний підрозділ основного командного пункту, що являє собою сукупність робочих місць, які розташовані у захищених спорудах, будівлях або на рухомій базі.

Підсумовуючи вище викладене слід зауважити, що в умовах ведення сучасного збройного конфлікту досягти перемоги над переважаючим за складом сил та засобів противником неможливо без застосування новітніх інформаційних технологій. Тому їх розвиток і впровадження у бойову діяльність сил оборони повинно бути одним з пріоритетних завдань наукових установа та організацій.

Флорін О.П., Богачов С.О., Кот О.Б., Кузміч О.Є.

РОЗВИТОК БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ У КОМПЛЕКСАХ ТЕХНІЧНОГО КОНТРОЛЮ

Сучасні виклики вимагають від Збройних Сил України впровадження новітніх технологій для забезпечення ефективного моніторингу та діагностики стану військової техніки та об’єктів інфраструктури.

Одним із перспективних напрямів є інтеграція бездротових сенсорних мереж (БСМ) у системи технічного контролю, що дозволятиме здійснювати оперативний збір та аналіз даних у реальному часі.

БСМ застосовуються для вирішення задач, що пов’язані зі збором та обробкою інформації у важкодоступних місцях та не потребують значного втручання у разі виникнення збоїв чи виходу з ладу окремих вузлів мережі.

Загальними особливостями функціонування БСМ є:

– значна розмірність мережі (сотні і тисячі вузлів);

– обмеженість ресурсів: ємність батареї, обсяг пам'яті, обчислювальна продуктивність, потужність передачі даних, пропускна здатність;

– неоднорідний і незбалансований трафік;

– динамічна топологія мережі та її здатність до самоорганізації в разі відмови (знищення) окремих вузлів;

– швидке розгортання, легка масштабованість тощо.

Кожна БСМ характеризується певним набором показників, що визначаються призначенням, типом, технічними параметрами вузлів та їх розміщенням (топологією мережі).

Серед основних показників БСМ слід виділити наступні:

– загальна кількість вузлів в мережі, їх тип та цільове призначення;

– швидкість передачі даних по каналах радіозв'язку (визначається протоколами, які використовуються для 3-х нижніх рівнів еталонної моделі взаємодії відкритих систем: фізичного, канального і мережевого);

– вибір та побудова маршрутів для забезпечення надійної передачі даних, в залежності від топології конкретної БСМ;

– щільність розміщення вузлів - кількість та дальність розміщення вузлів-сусідів (параметр визначається поточною топологією та може використовуватися, як керований параметр для її оптимізації);

– діаметр мережі - мінімальна кількість ретрансляцій даних між вузлами при передачі пакетів між двома найбільш віддаленими вузлами мережі (визначається топологією мережі і може використовуватися для її комплексної оцінки);

– латентність - параметр, що визначає час затримки від моменту виникнення події до передачі інформації до базової станції (центру збору інформації);

– час життя БСМ визначається часом роботи без заміни або підзарядки акумуляторів її окремих вузлів;

– пропускна здатність визначає обсяг інформації, що проходить через мережу в одиницю часу із заданою якістю.

Особлива увага приділяється забезпеченню завадостійкості та кіберзахисту БСМ, розробці енергоефективних сенсорних вузлів для тривалої автономної роботи в польових умовах.

Маємо констатувати, що агресія росії проти України актуалізувала важливість використання сенсорних систем з метою отримання розвідувальної інформації та її комплексного аналізу для забезпечення ефективного прийняття управлінських рішень. Здатність до швидкого розгортання, самоорганізація і відмовостійкість є ключовими особливостями бездротових сенсорних мереж, що роблять їх надійним інструментом для ефективного виконання оперативних завдань.

Впровадження БСМ сприяє автоматизації процесів моніторингу, зменшенню залежності від людського фактору та підвищенню точності та достовірності даних.

Таким чином, розвиток бездротових сенсорних мереж у комплексах технічного контролю є стратегічно важливим напрямом, що забезпечує підвищення надійності та ефективності функціонування Збройних Сил України в сучасних умовах. Це сприятиме скороченню часу на діагностику та ремонт техніки, підвищенню рівня її боєготовності та загальної ефективності виконання бойових завдань.

УДК 340.13 + 007.51 + 165.12 + 004.8

Фтемов Ю.О.

ЗАСТОСУВАННЯ STEM-ПІДХОДУ У ПРОЦЕСІ ВИКОНАННЯ КУРСОВОЇ РОБОТИ КУРСАНТАМИ ВІЙСЬКОВИХ ЗАКЛАДІВ ОСВІТИ

Сучасні тенденції у військовій освіті вимагають від фахівців не лише високого рівня технічної компетентності, а й творчого підходу до вирішення проблем та вміння працювати з новітніми технологіями. У зв'язку з цим все більше уваги приділяється впровадженню інноваційних методів навчання, які сприяють розвитку цих навичок. Одним із таких методів є STEM-підхід (Science, Technology, Engineering, Mathematics), що інтегрує науку, технології, інженерію та математику в освітній процес, забезпечуючи міждисциплінарний підхід до вирішення практичних задач.

Особливо актуальним впровадження STEM-методології є у військових закладах освіти, які готують фахівців, здатних не лише виконувати стандартні операції, а й розробляти та впроваджувати інноваційні інженерні рішення в умовах збройних конфліктів і кризових ситуацій.

Важливу роль у цьому відіграють курсові роботи (КР), що дозволяють курсантам застосовувати теоретичні знання на практиці. Використання STEM-підходу під час виконання КР сприяє підвищенню рівня підготовки майбутніх офіцерів, формуванню критичного мислення та розвитку навичок вирішення комплексних інженерних задач, які є ключовими для їхньої професійної діяльності. Таким чином, інтеграція STEM-методології в освітній процес є необхідною умовою ефективної підготовки військових спеціалістів.

Одним із ключових напрямів розвитку сучасної військової освіти є створення інформаційно-освітнього «Е-середовища», що забезпечує відкритість і доступність навчання через використання електронних та мобільних технологій. У межах цього підходу для виконання КР розроблено «Е-ГІД» – інтерактивний ресурс із ієрархічною структурою, основою якого є інформаційна база даних.

Отримавши посилання або QR-код, курсанти можуть приєднатися до електронного ресурсу, використовуючи будь-який зручний пристрій. Це надає їм доступ до інформації про викладача, завдання, цілі, методичні рекомендації та інші навчальні матеріали. Після реєстрації та вибору індивідуального завдання курсант переходить до наступного етапу роботи, де представлено навчально-наукові джерела у форматі PDF, а також посилання на додаткові матеріали.

Важливим елементом підготовки є робота з тестами, схемами, а також використання інтерактивного контенту – podcasts, videocasts тощо. Цей етап можна умовно назвати «вироблення рішення», оскільки саме тут курсант аналізує проблему, формулює ключові запитання та знаходить науково обґрунтовані відповіді. Він застосовує наукові принципи для аналізу даних, проведення експериментів чи розробки теоретичних моделей, що є основою STEM-підходу.

Подальший етап включає виконання розрахунків, де STEM-методологія забезпечує комплексний підхід, поєднуючи теоретичні знання з практичним застосуванням математичних методів і сучасних технологій. Це дозволяє курсантам розробляти ефективні та науково обґрунтовані рішення.

Не менш важливим є візуалізація результатів у графічній частині КР, яка допомагає наочно представити технічні аспекти проєкту, пояснити розрахунки, забезпечити точність і дотримання стандартів. Використання спеціалізованого програмного забезпечення сприяє автоматизації складних інженерних розрахунків, що значно

скорочує час виконання завдання.

Завдяки впровадженню новітніх технологій курсанти отримують можливість розробляти інноваційні рішення, підвищувати ефективність своїх проєктів, орієнтуючи їх на економічну доцільність, оптимізацію часу та ресурсів.

Узагальнюючи та порівнюючи отримані результати виконання проєктів із традиційним підходом і з використанням STEM-методик, включаючи якість виконаних завдань, рівень залученості курсантів та їхню здатність вирішувати військово-технічні завдання, можна дійти до висновків:

– покращено рівень технічної компетентності курсантів завдяки інтеграції STEM-підходу;

– підвищено якість КР за рахунок використання сучасних інженерних інструментів;

– відбувся поступовий розвиток креативного і критичного мислення у курсантів, здатності самостійно вирішувати складні технічні та тактичні задачі;

– здійснено підготовку курсантів до реальних завдань військової інженерної справи, що потребують знань на межі наук та технологій;

– збільшено міждисциплінарну інтеграцію знань, оскільки виконання проєктів потребує застосування знань з різних галузей, що сприяє більш комплексному розумінню курсантами специфіки їхньої майбутньої діяльності;

– підвищено рівень адаптивності до нових технологій і розвиток навичок командної роботи.

Отже, застосування STEM-підходу у процесі виконання КР дозволяє курсантам військових вишів не лише отримати фундаментальні знання, але й розвинути навички, необхідні для вирішення складних технічних завдань у реальних умовах. Це сприяє підвищенню якості підготовки майбутніх офіцерів, розвитку їх лідерських та командних якостей, а також їх здатності застосовувати сучасні технології, що є важливим фактором забезпечення обороноздатності держави та готовності до виконання реальних бойових завдань.

УДК 621.396.6

Фурман К.С., Бондар К.А., Демидас М.О.

ДОСЛІДЖЕННЯ ДЖЕРЕЛ РАДІОЧАСТОТНИХ ЗАВАД І МЕТОДИ ЇХ ЗМЕНШЕННЯ

Вступ. Радіочастотні завади стають дедалі актуальною проблемою в сучасному світі, де мобільні телефони, Wi-Fi мережі та Bluetooth пристрої міцно увійшли в наше повсякденне життя. Ці джерела електромагнітного випромінювання можуть значно впливати на роботу радіоелектронного обладнання й інших пристроїв, що здійснюють передачу даних за допомогою електромагнітних хвиль.

Усі джерела радіочастотних завад можна розділити на природні та штучні. Основними штучними джерелами є побутова техніка та засоби зв’язку. У міських умовах найпоширенішими генераторами таких завад виступають мобільні телефони, Wi-Fi точки доступу та пристрої з Bluetooth. Для зменшення радіочастотних завад застосовуються різноманітні методи.

Серед них – використання екранованих приміщень для збереження функціонування чутливого обладнання, встановлення фільтрів для обмеження частот випромінювання, а також оптимізація розташування антен приймальних і передавальних пристроїв для мінімізації взаємних перешкод. Дане дослідження спрямоване на вивчення основних джерел радіочастотних завад, пов’язаних із сучасними комунікаційними технологіями, та розробку ефективних способів їх зниження, щоб гарантувати стабільну роботу

електронної апаратури в умовах зростаючої насиченості електромагнітного поля в навколишньому середовищі [2].

Мета. Метою даного дослідження є аналіз джерел радіочастотних завад, що виникають від мобільних телефонів, Wi-Fi мереж та технологій Bluetooth, а також розробка дієвих методів їх мінімізації. Це спрямовано на забезпечення стабільної роботи радіоелектронної апаратури та інших пристроїв, які використовують електромагнітні хвилі для передачі даних.

Виклад основного матеріалу. Серед основних джерел радіочастотних перешкод можна виділити мобільні телефони різних поколінь (2G, 3G, 4G і 5G), які працюють на різних частотах. Наприклад, стандарт GSM використовує частоти близько 900 МГц і 1800 МГц, що потенційно може взаємодіяти з іншими системами зв'язку або приймачами в сусідніх діапазонах. Вагомий внесок у створення радіозавад також роблять мережі Wi-Fi всіх поколінь (802.11b/g/n/ac/ax), які працюють у діапазоні від 2 до 5 ГГц. Така частотна активність може створювати перешкоди для інших систем зв'язку та приймачів у тому ж спектрі. Пристрої з функціями Bluetooth, що працюють на частотах близько 2,4 ГГц, також можуть створювати перешкоди, оскільки їхні частотні діапазони часто накладаються на інші системи в межах одного приміщення.

Радіочастотні завади помітно впливають на роботу приймачів сигналів в інших діапазонах. Інтерференція між каналами зв'язку здатна спричиняти помилки під час передавання даних, порушуючи нормальну роботу мікросхем і антен. Крім того, таке випромінювання може дестабілізувати роботу електронних пристроїв, особливо тих, що належать до критичної інфраструктури або є високоточним обладнанням.

Розглянемо основні методи зменшення радіочастотних завад. Одним із найефективніших підходів є використання екранованих приміщень для захисту чутливої техніки. Такі приміщення мінімізують вплив перешкод завдяки застосуванню спеціальних екранувальних матеріалів, які блокують зовнішнє випромінювання. Додатково можна застосовувати фільтри, які обмежують певний спектр випромінювання. Це дає змогу зменшити взаємну інтерференцію між системами зв'язку або приймачами сигналів у близьких частотних діапазонах [1].

Правильне розміщення антен приймачів і передавачів також відіграє важливу роль у мінімізації перешкод, адже оптимальне розташування дозволяє знизити вплив інтерференції. Не менш значущим напрямом є оцінка ефективності існуючих методів захисту від радіозавад та розробка сучасних підходів із використанням новітніх матеріалів і технологій. Це дає змогу створювати більш ефективні рішення в умовах швидкого збільшення щільності електромагнітного поля.

Зазначені тези спрямовані на глибоке дослідження проблеми радіочастотних завад. Існують різні типи радіоперешкод, спричинених випромінюванням мобільних телефонів, Wi-Fi роутерів та Bluetooth пристроїв. Одним з них є міжканальна інтерференція, коли пристрої, що працюють на близьких частотах, заважають іншим пристроям, спричиняючи погіршення якості сигналу [3].

Перехресні перешкоди виникають, коли пристрої, що працюють на різних частотах, взаємодіють один з одним. Наприклад, Bluetooth-пристрої використовують той самий діапазон частот, що й Wi-Fi роутери, і тому можуть створювати перешкоди. Іншим важливим фактором є пульсації, спричинені нерегулярним випромінюванням сигналу від мобільних телефонів і Wi-Fi роутерів. Такі коливання можуть створювати додаткові перешкоди для чутливого електронного обладнання.

Для зниження рівня радіочастотних перешкод розроблено кілька ефективних методів. Одним з них є розміщення джерел радіоперешкод на достатній відстані один від одного, щоб мінімізувати їхній вплив. Наприклад, відокремивши мобільні телефони від Wi-Fi роутерів і Bluetooth пристроїв, можна значно знизити рівень перешкод. Інший спосіб зменшити рівень сигналу – дозволити кожному пристрою регулювати рівень

вихідної потужності відповідно до умов навколишнього середовища. Це може зменшити рівень перешкод, спричинених цими пристроями.

Також важливо використовувати спеціальні екрануючі матеріали, щоб зменшити випромінювання, яке випускають пристрої. Наприклад, використання екранування важливо в медичних установах та інших чутливих середовищах, де необхідно забезпечити мінімальний рівень електромагнітних перешкод. Для фільтрації сигналів, що заважають, можна використовувати фільтри, які обмежують смугу частот, що використовується пристроєм. Це зменшує діапазон можливих перешкод і покращує продуктивність [4].

Інший метод – використання технології співіснування, яка дозволяє пристроям працювати в одній смузі частот, не впливаючи суттєво на інші системи. Для цього використовуються алгоритми, що оптимізують взаємодію між пристроями, які працюють в одному діапазоні частот. З розвитком нових бездротових технологій, таких як 5G, проблема радіочастотних перешкод зростає, оскільки ці технології працюють у ще ширшому діапазоні частот.

Це призводить до збільшення електромагнітного забруднення і вимагає розробки нових методів зменшення завад. Одним з них є адаптивне управління частотою, яке оптимізує використання частот і зменшує завади.

Висновки. Джерела радіочастотних завад, зокрема мобільні телефони, Wi-Fi роутери та пристрої з підтримкою Bluetooth, суттєво впливають на якість функціонування бездротових технологій. Водночас існує низка ефективних методів для мінімізації таких завад. До них належать оптимальне розташування пристроїв, регулювання потужності сигналу, застосування екранування, використання фільтрів і впровадження технологій спільного використання частот. Для забезпечення стабільної та ефективної роботи бездротових мереж, особливо в умовах зростаючого попиту на високошвидкісний зв'язок і сучасні технології, як-от 5G, необхідно продовжувати дослідження в цій галузі.

Список використаних джерел

1. Бурячок В.Л., Соколов В.Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів : Монографія. Київ : КУБГ, 2019. 164 с.
2. Богуш В.В., Соколов В.Ю. Дослідження захищеності Wi-Fi мереж. *Зв'язок*. 2009. №4 (88). С. 29–31.
3. Iyare, R.N., Volskiy, V. & Vandenbosch, G.A.E. (2021). Comparison of peak electromagnetic exposures frommobile phones operational in either data mode or voicemode. *Environmental Research,* 197, article number110902. doi: 10.1016/j.envres.2021.110902.
4. IEEE standard for safety levels with respect to humanexposure to electric, magnetic, and electromagneticfields, 0 Hz to 300 GHz. (2019). doi: 10.1109/IEEESTD.2019.8859679.

УДК 004.8

Хмелевський С.І., Скріпченко Є.Л.

ПРОЕКТУВАННЯ СИСТЕМИ ОПЕРАТИВНОЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ОСОБАМИ БОЙОВОЇ ОБСЛУГИ

Сучасні бойові дії характеризуються високою інтенсивністю використання засобів повітряного нападу, широким застосуванням засобів радіоелектронної боротьби та комплексним використанням різноманітних типів авіаційних і ракетних систем. В

умовах великого обсягу інформації, яку необхідно аналізувати у стислі терміни, ухвалення своєчасних та обґрунтованих рішень стає ключовим фактором успішної оборони. Для забезпечення її надійності важливо впровадити систему оперативної підтримки дій, яка забезпечує автоматизацію ключових етапів збору, обробки, аналізу та відображення даних, що значно підвищує швидкість і точність ухвалення рішень. Її важливість полягає у здатності забезпечити осіб бойової обслуги актуальною та структурованою інформацією навіть у складних умовах сучасного бою.

Сучасні інформаційні системи управління вимагають постійного вдосконалення через такі виклики: збільшення кількості повітряних об’єктів, що беруть участь у бойових діях, та їхня складна динаміка; інформаційне перевантаження осіб бойової обслуги через обмежені можливості обробки великих обсягів даних; недостатня ефективність існуючих методів прогнозування загрозливих напрямків та координації дій.

Для вирішення цих проблем розроблено алгоритми управління інформаційною моделлю повітряної обстановки. Основний акцент зроблено на формалізації процесів ідентифікації повітряних об’єктів та їх групування у тактичні групи. Це дозволяє суттєво зменшити обсяг даних, які аналізуються, і підвищити точність оцінки повітряної обстановки.

Запропонована удосконалена методика оцінки проривонебезпечних напрямків, яка ґрунтується на аналізі щільності ударів засобів повітряного нападу супротивника у порівнянні з можливостями наших засобів протиповітряної оборони. Такий підхід забезпечує виявлення напрямків, які потребують посиленого захисту, та дозволяє оперативно розподіляти ресурси.

Система оперативної підтримки дій дозволяє суттєво скоротити час ухвалення рішень, знижуючи середній час обробки даних на 10-15%. Застосування прогнозних моделей, таких як графіки щільності ударів ЗПН, забезпечує операторів точними та наочними інструментами для аналізу обстановки.

Інтерфейс системи інтегрує таблиці та візуалізацію, які допомагають у швидкому прийнятті рішень. Тобто, інтерактивне табло оперативних напрямків надає деталізовану інформацію про кількість об'єктів та їхні параметри на кожному напрямку. Це суттєво мінімізує ймовірність помилок осіб бойової обслуги.

Дослідження показали, що впровадження запропонованої системи дозволяє скоротити час аналізу обстановки приблизно на 30% у порівнянні з традиційними методами. Використання сучасних інформаційних технологій також підвищує стійкість системи до зовнішніх впливів, таких як радіоелектронні перешкоди та людський фактор. Система оперативної підтримки дій є важливим елементом сучасного управління Повітряними Силами. Її впровадження дозволяє не лише підвищити ефективність оборонних операцій, але й оптимізувати процеси управління, забезпечуючи швидкість і точність ухвалення рішень. Завдяки впровадженню алгоритмів групування об’єктів, прогнозування напрямків ударів та інтерактивних інструментів для аналізу даних, ця система сприяє адаптації до викликів сучасної війни та посиленню обороноздатності України.

УДК 004.8

Хмелевський С.І., Хмелевська О.О.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ

Постійність певної фізичної чи іншої величини, що характеризує стан об’єкта, або зміна цієї величини відповідно до певного закону на основі конкретної інформації про стан об’єкта та навколишнього середовища забезпечує технологію

управління будь-яким об’єктом.

Інформаційну модель будь-якої системи управління можна уявити як сукупність двох основних компонентів: об’єкта управління та керуючої частини.

Під об’єктом управління розуміємо, чітко виділена обмежена сутність із точно зафіксованим складом і специфікацією елементів, що входять до цієї сутності, а також із чітко встановленими відносинами між елементами цієї сутності.

Об’єктом управління може бути будь-який об’єкт, предмет, процес, явище, на які спрямовано управлінську дію.

Найважливіша властивість об’єкта управління – цілісність. Припускається, що об’єкт управління може функціонувати автономно доти, доки не змінюються певні умови. Іншим принципово важливим компонентом системи управління є керуюча частина. Під управлінням розуміємо, свідомий цілеспрямований інформаційний вплив за допомогою керуючої частини з метою переведення об’єкта управління з одного стану в інший. Взаємодіюча керуюча частина й об’єкт управління утворюють систему управління. Система управління підтримує цілісність, як об’єкт управління вищого рівня. Управління має бути результативним. Взаємодія між об’єктом управління та керуючою частиною може відбуватися за кількома каналами.

Керуюча частина повинна мати дані про зовнішнє середовище та внутрішній стан об’єкта управління й відповідно до параметрів зовнішнього середовища і параметрів стану об’єкта управління – виробляти керуючий вплив на об’єкт управління.

Можна виділити три основні групи параметрів управління:

– критерії ефективності управління – складне, часто математичне поняття, яке визначає керуючу частину та закладає основну (функціональну) стратегію управління.

– норматив управління – дозволяє порівнювати поточний стан об’єкта управління із заздалегідь визначеним ідеалізованим станом (зразком) і визначає коректність (законність) керуючих впливів.

– зовнішні впливи, що задаються – дозволяють цілеспрямовано переводити об’єкт управління з одного стабільного (стійкого) стану в інший.

Переведення об’єкта управління у нестабільний стан призводить до дестабілізації об’єкта управління. Дестабілізація характеризується втратою керованості об’єкта управління, що може призвести до саморуйнування та втрати об’єкта управління.

Взаємодія керуючої частини та керованого об’єкта подвійна: здійснюється за допомогою прямого та зворотного зв’язку. За прямим зв’язком відбувається безпосередня передача керуючих впливів від керуючої частини до об’єкта управління. За зворотним зв’язком здійснюється передача інформації про фактичні (поточні) параметри стану об’єкта управління від об’єкта до керуючої частини. Такий спосіб передачі інформації є основної функцією зворотного зв’язку.

Де зворотний зв’язок відображає фундаментальне поняття кібернетики, теорії управління та теорії інформації. Зворотні зв’язки можуть бути лінійними і нелінійними. Розрізняють також негативний і позитивний зворотний зв’язок.

Негативний зворотний зв’язок широко використовується в замкнених автоматичних системах з метою підвищення стійкості (стабілізації), покращення перехідних процесів, зниження чутливості (під чутливістю розуміється відношення нескінченно малого зміни вихідного впливу до викликаного ним нескінченно малому вхідному впливу).

Позитивний зворотний зв’язок підсилює вихідний вплив ланки (або системи), призводить до підвищення чутливості і, як правило, до зниження стійкості (часто до незатухаючих і розбіжних коливань), погіршення перехідних процесів і динамічних властивостей.

Усі види взаємодії в будь-якій системі управління повинні бути узгоджені за точністю і періодичністю. Де точність взаємодії це характеристика взаємодії, що відображає ступінь близькості його параметрів до потрібного значення. Чим менше параметри взаємодії відхиляються від потрібних, тобто чим менша його похибка, тим вища точність взаємодії, незалежно від того, чи є похибка систематичною чи випадковою або містить і ту, і іншу складову. Та періодичність взаємодії це характеристика взаємодії, що визначається зміною параметрів взаємодії.

Необхідно виділити основні види інформаційних технологій (ІТ) в управлінні:

– ІТ інтерфейсу системи управління із зовнішнім середовищем;
– ІТ підтримки вибору управлінських впливів;
– ІТ підтримки процесу виконання управлінських впливів;
– ІТ зворотного зв'язку;
– ІТ створення, управління конфігураціями та реінжинірингу ІТ в управлінні (CASE-технології, CALS-технології);
– ІТ баз, банків і сховищ знань;
– ІТ документообігу;
– ІТ адміністрування інформаційних систем;
– ІТ надійного функціонування та захисту управління;
– ІТ візуалізації даних;
– ІТ моделювання проблем ситуаційного управління;
– ІТ призначення (ІТ логістики, ІТ фінансових потоків, ІТ корпоративного управління тощо);
– ІТ інтелектуальних систем управління.

Таким чином, під ефективністю інформаційної технології розуміємо властивість інформаційної технології, що характеризується сукупністю ефективностей технічного, економічного та соціального характеру при використанні інформаційної технології.

Інформаційні технології управління постійно вдосконалюються, адаптуючись до потреб організації, державного управління та суспільства загалом. Їхній подальший розвиток визначається глобальними трендами, такими як цифрова трансформація, штучний інтелект, великі дані та автоматизація та роботизація процесів.

Подальший розвиток інформаційних технологій управління спрямований на підвищення ефективності управління, зниження витрат і ризиків, а також забезпечення гнучкості та стійкості процесів. Впровадження інноваційних технологій дозволяє оптимізувати операційні процеси та сприяє цифровій трансформації організацій і державних структур.

Ховрат А.В., Стрельченко А.В., Кобзєв В.Г.

ДВОРІВНЕВА СИСТЕМА КЛАСИФІКАЦІЇ ДЕЗІНФОРМАЦІЇ В СОЦІАЛЬНО-ОРІЄНТОВАНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Проблема виявлення спотворень контенту в системах із високим рівнем користувацької взаємодії, таких як соціальні мережі, набуває все більшого значення в академічних та правових контекстах. У критичних ситуаціях соціальної нестабільності дезінформація становить значну загрозу як для окремих осіб, так і для суспільства загалом [1, 2]. Однак проблема мультикласифікації для різних груп потенційної загрози досі залишається відкритим дослідницьким питанням.

Представлене дослідження зосереджується виключно на текстовому новинному контенті через відсутність надійних інструментів для створення достовірних візуальних

підробок. При класифікації текстових даних застосовуються три основні підходи [3, 4]:

– імовірнісні моделі (зокрема наївний баєсівський класифікатор);
– нейронні мережі (рекурентні, згорткові, трансформери);
– поліноміальні моделі з ваговими коефіцієнтами.

Попередні дослідження бінарної класифікації даних показали, що гібридна мережа, яка поєднує рекурентні та згорткові можливості (RCNN), є однією з найефективніших [5]. Проте дезінформація різниться за впливом – від безпечного гумору до контенту, що загрожує суспільній стабільності.

У рамках представленого дослідження розроблено класифікаційну структуру типів дезінформації, що слугує основою для класифікації даних, відфільтрованих через модель RCNN. Ця структура включає такі категорії:

– явний гумор з об'єктивно ідентифікованими ознаками;
– тонкий гумор з контекстуальними проявами;
– шкідливі новини, спрямовані на окремих осіб або малі групи;
– регіонально шкідливі новини;
– глобально шкідливі новини.

Для ідентифікації ознак дезінформації виокремлено основні лінгвістичні маркери, що включають щільність риторичних прийомів, маніпуляції лексичною валентністю, прагматичну невідповідність, аналіз займенникової щільності та граматично-стилістичні відхилення. Додатково визначено вторинні стилометричні індикатори, які доповнюють основний аналіз та включають метрики маніпуляції афектом, аналіз щільності цитування, оцінку наративної узгодженості, оцінку достовірності джерела та коливання лінгвістичного регістру. На основі встановлених класів розроблено три моделі групування даних для другого шару класифікації:

– рекурентно-згорткова нейронна мережа (RCNN) – реалізовує гібридний підхід, що поєднує здатність рекурентних мереж опрацьовувати послідовні дані з можливістю згорткових мереж виявляти просторові залежності. RCNN на другому рівні використовує вектор імовірностей належності до класу «дезінформація» від першого шару як додатковий вхідний параметр, що суттєво підвищує загальну точність класифікації. Архітектура другого шару RCNN включає розширений набір фільтрів для виявлення специфічних ознак категорій дезінформації та механізм м'якої уваги, що дозволяє моделі зосередитися на найбільш релевантних частинах тексту для кожного класу;

– наївний баєсівський класифікатор – використовує теорему Баєса для обчислення ймовірності належності тексту до певного класу. Ця модель базується на принципі умовної незалежності ознак, що дозволяє розкласти складну проблему класифікації на набір простіших обчислень. На другому рівні впроваджено удосконалений варіант, що використовує концепцію згладжування Лідстоуна для подолання проблеми нульових ймовірностей та метод зваженої комбінації ознак для балансування впливу різних лінгвістичних маркерів. Ключовою перевагою цього підходу є його обчислювальна ефективність та інтерпретовність результатів, що дозволяє не лише класифікувати текст, але й визначити, які саме лінгвістичні особливості вплинули на рішення моделі;

– поліноміальний алгоритм – реалізовує лінійну адитивну згортку з ваговими коефіцієнтами, визначеними експертним шляхом. Для кожного з ідентифікованих лінгвістичних маркерів встановлено такі вагові коефіцієнти: емоційна характеристика тексту – 0,4; щільність риторичних конструкцій – 0,1; частота негативних конструкцій – 0,1; контекстуальний емоційний індекс – 0,1; коефіцієнт підозрілості – 0,15; фактор впливу повідомлення – 0,1; вектор величини емоційного забарвлення – 0,1. Сума всіх коефіцієнтів дорівнює 1,0, що забезпечує нормалізацію результатів класифікації. Для кожної категорії дезінформації визначено порогові значення, що дозволяють віднести текст до відповідного класу: явний гумор – 0,25-0,4; тонкий гумор – 0,4-0,55; новини проти окремих осіб – 0,55-0,7; регіонально шкідливі новини – 0,7-0,85; глобально

шкідливі новини – 0,85-1,0. Поліноміальний алгоритм демонструє високу інтерпретовність результатів та обчислювальну ефективність, проте поступається точністю іншим підходам, особливо при аналізі текстів із нетиповими стилістичними характеристиками.

Для забезпечення ефективної обробки великих обсягів даних застосовано парадигму розподілених обчислень на основі MapReduce. Ця методологія дозволяє розподілити операції аналізу тексту та тренування моделей між кількома обчислювальними вузлами, що суттєво скорочує час обробки та підвищує масштабованість системи. Зокрема, для RCNN архітектури реалізовано паралельне обчислення згорткових шарів, де кожен вузол обробляє окрему частину вхідного тексту з подальшим агрегуванням результатів для рекурентних компонентів.

Особливу увагу приділено механізмам протидії навмисним спробам обходу системи виявлення дезінформації. Розроблено адаптивні методи, що дозволяють ідентифікувати нові техніки маскування дезінформації під достовірний контент, включаючи використання навмисних орфографічних помилок для уникнення ключових слів-тригерів та стилістичну імітацію авторитетних джерел.

Для оцінювання ефективності цих методологій проведено експеримент з оцінки точності, часової ефективності та зменшення обсягу даних. Для валідації використовувались два набори даних кожен з яких стосувався російсько-української війни [6, 7].

Для забезпечення репрезентативності результатів експерименту застосовано техніку крос-валідації з 10-ма фолдами, що дозволило мінімізувати вплив випадкових флуктуацій у розподілі даних. Додатково проведено аналіз чутливості моделей до параметрів налаштування, включаючи розмір прихованого шару LSTM, кількість фільтрів у згорткових шарах та коефіцієнт регуляризації для запобігання перенавчанню.

Важливим аспектом дослідження стало порівняння ефективності моделей для різних мовних груп, що дозволило оцінити універсальність розроблених методів та їхню застосовність у багатомовному середовищі. Експерименти показали високу стійкість моделей до мовних особливостей при збереженні загальної точності класифікації, що є критичним для глобальних інформаційних систем.

Основні параметри оцінювання включали:

– точність класифікації (зважена F1-оцінка);
– ефективність опрацювання (час аналізу набору даних);
– вимоги до обсягу даних (зменшення розміру навчального набору).

Зважена F1-оцінка була обрана як основна метрика ефективності через її здатність балансувати між точністю та повнотою, що особливо важливо в контексті виявлення дезінформації, де як хибнопозитивні, так і хибнонегативні результати мають значні наслідки.

Результати експерименту продемонстрували, що кожен підхід із використанням дворівневої моделі показав у середньому 20% підвищення ефективності порівняно з прямим застосуванням методу RCNN. Зокрема:

– комбінація наївного баєсівського класифікатора та RCNN продемонструвала найвищу точність та швидкість роботи з коефіцієнтом ефективності 0,945;

– однорівнева реалізація RCNN досягла коефіцієнта ефективності 0,62;

– дворівнева архітектура RCNN продемонструвала значне покращення з коефіцієнтом 0,942;

– реалізація з використанням RCNN як первинного шару в поєднанні з поліноміальним підходом дала коефіцієнт ефективності 0,816.

Гібридна конфігурація RCNN-наївний Баєс продемонструвала оптимальне співвідношення між точністю класифікації та обчислювальною ефективністю. При порівнянні з однорівневою моделлю виявлено зниження швидкості обробки на незначні

5%, водночас точність класифікації підвищилася на 46%. Особливо важливим є той факт, що дана конфігурація потребує лише десятої частини початкового набору даних для підтримки рівня точності вище 80%.

Проведений аналіз матриці невідповідностей виявив, що ця гібридна модель найефективніше функціонує при ідентифікації тонкого гумору та новин із регіонально шкідливим впливом – категорій, що традиційно викликають найбільші труднощі при автоматизованій класифікації через їхню контекстуальну залежність. Додатково модель продемонструвала високу резистентність до шумів у вхідних даних та здатність швидко адаптуватися до нових стратегій дезінформації без повного перенавчання.

Експериментальні результати чітко демонструють значні відмінності в ефективності між різними архітектурними підходами. Суттєве підвищення точності порівняно з базовою однорівневою моделлю підтверджує доцільність застосування ієрархічних підходів для вирішення складних завдань класифікації, особливо в контексті комбінування методологічно різних, але взаємодоповнювальних алгоритмічних фреймворків.

Список використаних джерел

1. The impact of fake news on social media and its influence on health during the COVID-19 pandemic: a systematic review / Y.M. Rocha et al. Journal of Public Health. 2023. Vol. 31. P. 1007–1016.
2. Internet platforms as alternative sources of information during the Russian-Ukrainian war / K. Horska et al. Amazonia Investiga. 2023. Vol. 12, no. 62. P. 353–360.
3. Kumar P., Vardhan M. Plutchik Wheel of Emotion and Machine Learning-Based Hybrid Sentiment Analysis for the Hindi Language with Minimum Dependency on High Computation Resources. SN Computer Science. 2023. Vol. 26. no. 1. P. 28–63.
4. Khovrat A., Kobziev V. Using RCNN to Indentify the Fake Audio Information. IEEE 7th International Conference on Actual Problems of Unmanned Aerial Vehicles Development: Conference Proceedings, Kyiv, 22–24 October 2024. 2024. P. 205–208.
5. Yakovlev S., Khovrat A., Kobziev V. Using Parallelized Neural Networks to Detect Falsified Audio Information in Socially Oriented Systems. X International Scientific Conference «Information Technology and Implementation» (IT&I-2023): Conference Proceedings, Kyiv, 20–21 November 2023. 2024. P. 220–238.
6. DS-Pr1nce. War in Ukraine: Russian social network discussions. Kaggle. URL: https://www.kaggle.com/datasets/ustyk5/war-in-ukraine-russian-social-network-discussions (date of access: 20.03.2025).
7. Zepopo. Ukrainian news. Kaggle. URL: https://www.kaggle.com/datasets/zepopo/ukrainian-fake-and-true-news (date of access: 20.03.2025).

Хомяк К.М., Ларіонов В.В.

3D ОКУЛЯРИ – СУЧАСНІ ТЕХНІЧНІ ЗАСОБИ НАВЧАННЯ

Розвиток сучасних технологій не залишив сферу навчання осторонь. Розвиток та трансформація навчального процесу показала необхідність гнучкого підходу до вирішення проблематики навчання. А виклики сьогодення лише яскраво підтвердили той факт що процес навчання, як і будь-яка інша сфера діяльності потребує трансформації та все інтенсивнішого використання сучасних інформаційних технологій в процесі навчальної діяльності.

Яскравим прикладом однієї із таких технологій є використання концепції віртуальної реальності (VR). Відліком початку існування VR вважається 1965 рік, коли було вперше створено машину Sensorama, яка, по суті, відтворювала зображення на

стереоскопічному дисплеї за рахунок інтегрованих кінопроекторів. Пізніше у 1968 році було створено першу VR- гарнітуру яка мала назву «Дамоклів меч», та надавала змогу користувачу змінювати перспективу зображення у відповідності до повороту голови оператора. В подальшому процес мінімізації розмірів складових елекронних обчислювальних пристроїв відобразився і на складових технічних засобів VR. Зменшуються габаритні розміри, збільшується продуктивність засобів, з'являється змога записувати певні обсяги даних на самі засоби, вони стають більш мобільними.

Зі збільшенням продуктивності значно зростає і сфера використання, тут передові позиції утримують фахівці силових структур та військових організацій, це і медична сфера та навчальний процес в цілому.

Переваги використання таких технічних очевидні, це і економія матеріально-технічних засобів, значне зменшення ризиків для тих хто навчається, велика пропускна спроможність в обмеженому просторі, ініціація вироблення психологічної стійкості при утворенні стресової ситуації, вироблення алгоритму дій та порядку свого поводження на місцевості. Проте дані пристрої мають і ряд своїх особливих недоліків, а саме: втрата часу, небезпека для очей, навантаження на центральну нервову систему, висока ціна, необхідність додаткового обладнання, вплив на здоров'я, залежність.

Прикладів використання таких технічних засобів досить багато, проти ми хочемо зосередити увагу на лише одному із таких шляхів реалізації що вже має практичну апробацію у військовому середовищі. Мова піде про використання концепції віртуальної реальності при проведенні занять в період базової загальновійськової підготовки, а саме про навчальний - фільм «Перший бій». Проблематика створення такого фільму покликана питаннями психологічної неготовності до виконання, чи відмова від виконання завдань на полі бою у переважної більшості військовослужбовців, що прибули для проходження військової служби. Даний продукт дає змогу військовослужбовцю, вже на протязі перших днів підготовки в навчальному центрі зануритись в середовище першого бойового епізоду без реальної загрози його життю та здоров'ю. Саме такий продукт дає змогу підвищити стресостійкість, проводить імерсивне тренування, формує необхідні нейронні зв'язки для подальшої адаптації військовослужбовця до виконання подальших бойових завдань, збільшить його ефективність на полі бою, зменшить ймовірність виникнення «ступору» у військовослужбовця.

Побутує думка про неможливість використання даних засобів через їх високу собівартість, проте це довгострокове фінансове вкладення, адже засоби VR це не одноразові пристрої, а засоби багаторазового використання, через які є змога прогнати сотні чоловік особового складу. Інший аспект це змога створення, по суті, будь-якої обстановки, місця проведення тренування чи заняття, пристрою з яким необхідно працювати. Це доволі об'ємна та тривала робота, але результат однозначно перевершить всі сподівання та очікування.

Циганков П.М., Чаган Ю.А., Федоров О.Ю., Мокоївець В.І.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ

Застосування інформаційних технологій у підготовці та діяльності правоохоронних органів надає значну кількість переваг, які підвищують ефективність їхньої роботи, покращують охорону правопорядку, безпеку в суспільстві та сприяють справедливому правосуддю. Ось деякі з переваг.

Підготовка кадрів. Симуляційні тренінги. Використання віртуальної реальності (VR) та доповненої реальності (AR) для створення реалістичних сценаріїв, таких як

затримання злочинців, реагування на надзвичайні ситуації або ведення переговорів. Це дозволяє правоохоронцям тренуватися в безпечному середовищу, відпрацьовувати навички прийняття рішень та реагування на різні ситуації. Онлайн-навчання та дистанційні курси. Доступ до навчальних матеріалів, лекцій та тестів через онлайн-платформи. Це забезпечує гнучкість у навчанні, дозволяє правоохоронцям навчатися у зручний час та в зручному місці. Аналіз даних та оцінка ефективності. Використання програмного забезпечення для аналізу даних про результати тренінгів, виявлення слабких місць та покращення навчальних програм. Автоматизація рутинних процесів, інформаційні технології дозволяють автоматизувати багато адміністративних завдань, таких як ведення службової планувальної, інформаційної та звітної документації, складання звітів, облік речових доказів, що звільняє час співробітників для виконання більш важливих завдань.

Оперативна діяльність. Система відео спостереження та аналіз відеоданих. Використання камер відеоспостереження для підвищення рівня ситуаційної обізнаності, моніторингу громадського порядку, виявлення і фіксації злочинів та збору фактичних доказів. Застосування програмного забезпечення для аналізу відеоданих, розпізнавання облич, номерних знаків автомобілів та інших об’єктів. Бази даних та інформаційні системи. Доступ до баз даних про злочин, підозрюваних, транспортні засоби та іншу інформацію. Система ситуаційної обізнаності використовується для збору, обробки та відображення інформацій про поточну ситуацію, що дозволяє командирам швидко оцінювати обстановку та приймати обґрунтовані рішення. Використання інформаційних систем для обміну інформацією між різними правоохоронними органами. Геоінформаційні системи (ГІС). Використання ГІС для аналізу географічних даних , визначення зон підвищеної злочинності, планування патрулювання та реагування на надзвичайні ситуації. Кібербезпека. Захист інформаційних систем правоохоронних органів від кібератак. Розслідування кіберзлочинів. Використання дронів. Моніторинг великих територій, пошук зниклих осіб. Огляд місця злочину. Інформаційні технології використовуються для забезпечення надійного та безпечного зв'язку між особовим складом, включаючи використання захищених мереж, спутнікового зв’язку та мобільних технологій. Оптимізація розподілу ресурсів, таких як аналіз даних про злочинність та завантаженість підрозділів дозволяє більш ефективно розподіляти особовий склад та технічні засоби.

Взаємодія з громадськістю. Онлайн-платформи та соціальні мережі. Використання соціальних мереж для оповіщення та інформування громадськості, отримання інформації про події та злочини, реагування на звернення громадян. Мобільні додатки. Мобільні додатки для взаємного оповіщення, повідомлення про події і злочин, отримання інформації про правопорушення та взаємодії з правоохоронними органами. Інформаційні технології використовуються для аналізу великих обсягів даних з різних джерел, що дозволяє виявляти закономірності, прогнозувати події та оцінювати ризики.

Переваги застосування інформаційних технологій, це суттєве підвищення ефективності роботи правоохоронних органів, покращення якості фахової підготовки кадрів, загальне зниження рівня злочинності, гарантоване підвищення довіри суспільства та громадськості до правоохоронних органів. Незважаючи на численні переваги, важливо також враховувати потенційні ризики, пов’язані з використанням інформаційних технологій, наприклад, такі як питання конфіденційності даних, кібербезпека та можливе зловживання технологіями. Тому впровадження інформаційних технологій в правоохоронних органах повинно здійснюватися на основі чинного законодавства з урахуванням етичних та правових норм.

Слід зазначити, що застосування інформаційних технологій не є сталим і продовжує розвиватися, а новітні технології, такі як квантові обчислення та блокчейн, можуть мати значний вплив на службову діяльність правоохоронних органів у майбутньому.

Тому службові особи органів управління та особовий склад підрозділів сил охорони правопорядку правоохоронні органи повинні адаптуватися до нових технологій, щоб ефективно виконувати свої функції.

УДК: 621. 396

Чепкій В.В., Єфимчиков О.М., Цуканов В.Н., Єльчанінов О.Д.

ПЕРЕШКОДОЗАХИЩЕНІСТЬ КАНАЛІВ УПРАВЛІННЯ МОБІЛЬНИМИ БАГАТОЦІЛЬОВИМИ ПЛАТФОРМАМИ БЕЗПІЛОТНОЇ НАЗЕМНОЇ СИСТЕМИ В СЦЕНАРНИХ УМОВАХ РАДІОЕЛЕКТРОННОГО КОНФЛІКТА

Утилітарно-прагматичне сприйняття сценарної методології сталого дистанційного управління (ДУ) мобільними багатоцільовими роботизованими платформами (БРП) безпілотної наземної системи (БпНС) в транспортно-логістичних операціях (ТрЛО) позиціонується з аспектами резистентних властивостей виділеного (суміщеного) або розподіленого радіоканалів R_{sch} інформаційно-керуючої системи (ІКС), ступенем компетентності Q_{op} операторів управління мобільними БРП, завадостійкістю апаратно-програмного обладнання каналів командно-телеметричної інформації C_{cti} та корисного навантаження C_{tpi}, а також сценарними умовами S_{sc} їх активізації та взаємодії [1-4].

Сценарні умови S_{sc} представлено сукупністю екзогенно заданих та узгоджених на інтервалі оцінювання показників невразливості (інформаційної безпеки) радіоканалів ІКС, які обмежені рядом лабільних факторів: деструктивним впливом організованих перешкод $\eta(t)=\{\eta_i(t)\}\in W_\eta$ радіоелектронного придушення (РЕП), вибором стратегій та способів функціонування $\omega_0=\{\omega_к\}\in\Omega$, індикативними орієнтирами $w_\eta(\omega_к)$ об'єктивного контролю за виконанням цільових завдань $g_0=\{g_{0j}(t)\}\in G$, рівнем захищеності ліній радіозв'язку між наземним пунктом управління (НПУ) та віддаленими бортами БРП. Лабільні чинники ініціюють основні сценарії поведінки S_b та управління S_m [1, 2, 4]:

– синергічні сценарії S_{sm} моделюють поведінкові аспекти радіоканалу «НПУ-БРП» в умовах організованих перешкод $\eta(t)$ та описують способи отримання оптимальних оцінок показників завадостійкості і прихованості каналів ІКС за рахунок емердженості;

– сценарії прямого управління S_{dm} моделюють спектр характеристик скритності та завадостійкості каналів радіозв'язку з протоколом псевдовипадкової перебудови робочої частоти (ППРЧ) в динамічних умовах радіоелектронного середовища;

– атрактивні сценарії S_{am} моделюють суб'єктивно бажані, «інтелектуальні» процеси взаємодії та самоорганізації (параметричної адаптації) радіоканалу ІКС і засобів РЕП.

Сценарії управління S_m ергатичних конфігурацій БпНС синтезуються як інструмент формального аналізу альтернативних рішень, що приймаються предметно модельних варіантів перешкодозахищеності радіоканалу ІКС при заданих цільових установках.

Теза перешкодозахищеності радіоканалу ІКС досліджується, як мейнстрім сценарної методології поєднання стратегії, організаційних заходів, способів та технічних засобів, що спрямовані на забезпечення штатних режимів функціонування ІКС в умовах РЕП.

Оцінювання перешкодозахищеності радіоканалів ІКС здійснюється за категоріями:

– завадостійкості – здатності радіоканалу протистояти впливам активних перешкод, кількісна міра якої афілійована з показниками середньої ймовірності помилки на біт інформації, відношення сигнал/перешкода та ймовірності помилки в кодовому слові;

– прихованість – здатності радіоканалу протистояти діям радіотехнічної розвідки (РтР): виявленню сигналів $s(t)=\{s_i(t)\}\in W_s$, вимірюванню параметрів, визначенню напряму приходу. В межах окреслених завдань РтР піддано аналізу ряд похідних: енергетичної, структурної, інформаційної, просторової та часової прихованості [3, 4].

Заявлено загальну формулу захисту радіоканалів «НПУ–БРП», як «максимально швидке уникнення енергетичного протиборства» з перешкодами $\eta(t)\in W_\eta$.. За такої домінанти визначено показники захищеності радіоканалів ІКС: фактичний час роботи на одній частоті, потужність сигналу управління P_s, вид перешкоди та її потужність P_η, структура приймального пристрою (ресиверу), запроваджені способи завадостійкості.

Процес функціонування радіоканалу ІКС в середовищі активної дії перешкод за фізичною іманентністю асоціюється з гіпотезою радіоелектронного конфлікту (РЕК). Експлікація гіпотетичного судження відображена блок-схемою, яка містить трансівери радіоканалу передачі пакетної інформації, засоби РтР, станції радіоперешкод (СтРП) системи РЕП. Остання визначає послідовність етапів – технічна розвідка і протидія, які утворюють канали перехоплення пакетних даних та придушення сигналів $s(t)\in W_s$, [3].

Схемна інтерпретація передачі пакетної інформації представлена моделлю лінійного відгуку, як субодиниці наближення (моделі третього типу). Математичний оператор перетворення L_Ξ, між вхідним $x(t)=\{x_i(t)\}\in W_x$ та вихідним $y(t)=\{y_i(t)\}\in W_y$ векторами подається як лінійне відображення області визначення W_x в область значень W_y цільового результату. Додатком лінійного прообразу анонсовано локальну модель вхідного процесу $x(t)=\{x_i(t)\}\in W_x$. Моделюванню піддаються ситуації в таких версіях:

– типова версія, сигнал управління $\mathbf{s}(t)=\{s_i(t)\}$ передається по захищеному каналу за відсутності активних перешкод $\eta(t)\in W_\eta$. Ансамбль реалізацій випадкового процесу на вході ресивера описується вектором суміші $x(t)=\alpha(t)s(t)+\psi(t)$ корисного сигналу $s(t)$ та ненавмисних перешкод з мультиплікативною $\alpha(t)$ і адитивною $\psi(t)$) властивостями;

– не типова версія, предиктор РЕК подається, як організоване домінування навмисних перешкод $\eta(t)=\alpha(t)\xi(t)+\psi(t)$. Механізм формування «фальшивого» сигналу $\xi(t)$ векторної суміш пов’язаний з імітацією (ретрансляцією) інформаційних параметрів корисних сигналів $s(t)=\{s_i(t)\}$, отриманих засобами РтР і випромінених СтРП у вигляді. структурних перешкод $\xi_s(t)$. На входах ресивера радіоканалу спостерігається процес $x(t)=\alpha(t)s(t)+\alpha(t)\xi(t)+\psi(t)$, у векторній структурі якого присутні елементи дестабілізації.

Згідно концепції моделювання динаміка РЕК експонується сценарними умовами S_{ui} несанкціонованого втручання в роботу каналів радіозв’язку та управління мобільними БРП. Іманентність сценарних умов S_{ui} апріорі витікає із процесів перехоплення сигналу $s(t)=\{s_i(t)\}$ та підміни прийнятих пакетів даних. Субституцією служать різновиди структурних перешкод $\xi_s(t)$, наприклад, імітаційного походження. Розширеному аналізу піддаються імітаційні перешкоди або спуфінг-перешкоди $\xi_{ss}(t)$, як найбільш небезпечні для систем радіозв’язку. Оцінювання деструктивних впливів відбувається шляхом верифікації структурних властивостей сигналу $s(t)$ і спуфінг-перешкоди $\xi_{ss}(t)$, аналізу кореляційної функції R_{ss} з урахуванням розподілу їх енергій на частотно-часовій площині. Визначено простір параметричних ознак для амплітудної, поляризаційної, частотної, часової ідентифікації корисного $s(t)$ та фальшивого $\xi_s(t)$ сигналів [1, 3].

Предметно кінцевого результату прийняті альтернативні рішення стосовно розвідо- та перешкодозахищеності радіоканалів ІКС в умовах структурних перешкод $\xi_s(t)\in W_\xi$.

1. Рішення на основі синергічного сценарію S_{sm} передбачає перехід до проектування багатоканальних систем групового управління мобільними БРП в гетерогенній та/або гомогенній конфігураціях. Згідно теорії допустимо орієнтуватись на сетецентричний принцип побудови системи, а в прикладному додатку – на просторово-розподілену реалізацію каналів обміну інформацією та командних радіоліній зв’язку. Даний проект передбачає спільне використання прив’язних безпілотних літаючих апаратів (БПЛА) та БПЛА-ретранслятора, а також встановлення на опціональних БРП угрупування навісного обладнання з потужним обчислювальним ресурсом для обміну цільовою інформацією всередині групи. Такий обмін зорганізується за схемою багаторівневого ієрархічного управління [4]. Синергічний сценарій відображує організаційні аспекти розвідо- та перешкодозахищеності радіоканалів ІКС, що дозволяє [1, 2, 4. 5]:

– розширити робочу зону та збільшити дальності дії засобів передачі даних НПУ;
– підвищити поінформованість операторів БпНС щодо зовнішнього середовища;
– перерозподілити локальні цільові завдання всередині угрупування (резервування заміщенням) у разі виходу із експлуатації (враження) окремих опціональних БРП.

2. Ефективна реалізація сценарію прямого управління S_{dm} розподіленими каналами передачі командно-телеметричної інформації та корисного навантаження представлено схемою лінії радіозв'язку з псевдовипадковою перебудовою робочої частоти (ППРЧ). В режимі ППРЧ розширення спектру сигналу управління $s(t) \in W_s$ забезпечується шляхом стрибкоподібної зміни (переключення) однієї з несучих частот f_{0i} в межах виділеного діапазону ΔF, а саме, «сітки» частотних каналів. Число частот та порядок їх чергування корегуються псевдовипадковими кодами [3, 5]. Заявлено вимоги до застосування ППРЧ в динамічних умовах РЕК. Пропонується орієнтуватись на протокол ключових змінних в наступній редакції: визначення 40-канальної «сітку ППРЧ» в смузі частот 80 МГц; формування адресної групи частот з усієї доступної множини частот; дотримання тривалості одного сеансу передачі даних на одному каналі не більше 2 мс, а символьної швидкості передачі до 2000 кбод. Апаратно-програмне обладнання радіоканалів повинно забезпечувати двосторонню низькошвидкісну передачу командної інформації на борт БРП, телеметричної інформації з БРП на стаціонарний НПУ та односторонню високошвидкісну передачу інформації корисного навантаження з борта БРП на НПУ.

3. Практикам на базі атрактивних сценаріїв S_{am} властиві комплікації з процесами інтелектуального групового управління БРП та явищем самоорганізації, що виникають через втрату стійкого стану радіоканалів в силу динамічності умов РЕК. Комплікація породжена дилемою на процеси штучної самоорганізації в технічних системах, особливостями формування «організованої структури», стійкої в умовах РЕК. Питання самоорганізації щодо «вертикального» та «горизонтального» операційних принципів за певними правилами знаходяться на етапі наукової дискусії [3]. Заявлені ускладнення сценаріїв S_{am} потребують додаткового вивчення та окремого висвітлення результату.

Консеквенція видається очевидною, оскільки в умовах РЕК сигнали передачі інформації та прийомне обладнання радіоканалів ІКС є об'єктами впливу РтР та СтРП системи РЕП. Знання специфіки сценарних умов S_{sc}, сценаріїв управління S_m, стратегії перешкодозахищеності, формули та особливостей режимів (протоколів), сприяє вирішенню цільових завдань сталого управління віддаленими угрупуваннями БРП.

Список використаних джерел

1. Чепкій В.В., Єфимчиков О.М., Цуканов В.Н. Сценарні умови ефективного виконання транспортно-логістичних операцій безпілотною системою тактичного рівня управління. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану*: матеріали Міжнародної науково-практичної конференції (м. Одеса, 18 жовт. 2024 р.). Одеса, 2024. С. 294–295.
2. Кульба В.В., Кононов Д.А., Чернов И.В., Рощин П.Е., Шулигина О.А. Сценарное исследование сложных систем: анализ методов группового управления. *Управление большими системами.* 2010. №30-1. С. 154-186. URL: https://cyberleninka.ru/article/n/stsenarnoe-issledovanie-slozhnyh-sistem-analiz-metodov-gruppovogo-upravleniya (дата звернення: 07.03.2025).
3. Макаренко С.И., Иванов М.С., Попов С.А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: монография. Санкт-Петербург: Свое издательство, 2013. 166 с.
4. Чепкій В.В., Єфимчиков О.М., Цуканов В.Н., Ковалішин С.С., Дуйловській А.О. Утилітарна парадигма оцінювання ефективності безпілотної наземної системи в логістичних операціях тактичної ланки. *Збірник наукових праць Військової академії (м. Одеса).* Одеса, 2024. Вип. 2 (22). С. 101-115.

5. Васильев И.А., Половко С.А., Смирнова Е.Ю. Организация группового управления мобильными роботами для задач специальной робототехники. *Информатика, телекоммуникации и управление*. 2013. №1 (164). URL: https://cyberleninka.ru/article/n/organizatsiya-gruppovogo-upravleniya-mobilnymi-robotami-dlya-zadach-spetsialnoy-robototehniki (дата звернення: 02.03.2025).

Черних Ю.О.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ОЦІНЮВАННЯ РІВНЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Реформування системи вищої освіти в Україні є пріоритетною задачею держави, яка передбачає якісні зміни у системі підготовки фахівців для сфери оборони із застосуванням інформаційних технологій. Необхідність удосконалення організації освітнього процесу (ОП) у закладах вищої освіти (ЗВО) як складової системи освіти висуває невідкладні проблеми його комп'ютеризації, впровадження сучасних інформаційних технологій щодо оцінювання рівня якості освіти, формування на їх основі нових стратегій підготовки фахівців з вищою освітою.

Важливим елементом системи внутрішнього забезпечення якості вищої освіти є інформаційно-аналітична система оцінювання рівня якості освіти у ЗВО. Інформаційно-аналітичні системи (ІАС) оцінювання рівня якості освіти відноситься до класу інформаційних систем, призначених для аналітичної обробки інформації зі здійснення оцінювання рівня якості освіти у ЗВО з використанням баз знань і експертних систем. На цей час ринок програмного забезпечення пропонує певні рішення щодо управління ОП у ЗВО, зокрема:

– автоматизована система управління закладом вищої освіти АСК «ЗВО», розроблена Науково-дослідним інститутом Прикладних інформаційних технологій Кібернетичного центру Національної академії наук України;

– пакети комп'ютерних систем «Деканат», «Бібліограф», «Колоквіум», «ПС-персонал» приватного підприємства «Політек-софт»;

– ВНЗ АЛЬМА-МАТЕР» товариства з обмеженою відповідальністю «Direct IT».

Здійснимо стислий огляд програмного забезпечення із управління ОП у ЗВО.

АСК «ЗВО» складається з двох підсистем: «Приймальна комісія» та «Деканат». Основні функціональні можливості підсистеми «Деканат»: роздрукування заліково-екзаменаційної документації на період кожної сесії та перед початком навчального року; формування і роздрукування проектів наказів; формування заявки на виготовлення документів про освіту та студентських квитків. Підсистема «Приймальна комісія» дозволяє: організувати введення анкетних відомостей абітурієнта; перевірити інформацію атестата про середню освіту; здійснити друк екзаменаційних листів з фотографією абітурієнта; обробляти готові результати іспитів, що уведені оператором; проводити моніторинг вступних іспитів, прогнозування середнього та прохідного балу.

Серед усіх пакетів, які пропонує «Політек-Софт», найбільш функціональними, з точки зору автоматизації сфер діяльності ЗВО, є пакети «Деканат» і «Колоквіум». Пакет програм «Деканат» призначений для автоматизації планування та обліку ОП в закладах освіти (технікумах, коледжах, училищах, інститутах та університетах). Пакет дозволяє створити та підтримувати базу даних, в якій формується та реєструється така інформація: структура ОП закладу (спеціальності, освітні програми, групи, підгрупи, потоки, навчальні дисципліни (предмети), кількість годин з навчальних дисциплін (предметів) за різними видами занять, навчальні плани та, у разі необхідності, факультети, кафедри, циклові комісії); дані щодо всіх викладачів закладу та їхнього планового навчального навантаження; щоденні дані про фактичну роботу кожного

викладача з кожної навчальної дисципліни (предмету); великий обсяг даних щодо всіх студентів закладу та їхньої успішності за весь період навчання; дані про наявні корпуси та аудиторії навчального закладу, їхнього заповнення, розклад навчальних занять тощо. Пакет програм «Колоквіум» призначений для комп`ютерного тестування знань студентів ЗВО України. Пакет надає такі можливості: зручна оболонка для формування тестів; тестування студентів у різних режимах та на основі результатів тестування оцінювати знання; забезпечується доступ до бази даних з результатами тестування з метою всебічного аналізу; автоматична генерація та друк звітів за результатами тестування; інформаційна сумісність з пакетом програм «Деканат», призначеним для автоматизації документообігу в навчальній частині закладу. Головними особливостями пакету є: простота використання, мінімум необхідних дій при роботі з програмами; великий обсяг та повнота інформації, яка зберігається у базі даних; велика кількість режимів тестування і оцінювання, що дає можливість підібрати оптимальні параметри тестування для кожного конкретного випадку залежно від вимог викладача та важливості тесту; можливість використання в будь-яких навчальних закладах.

«Політек-софт» пропонує ще допоміжні пакети, такі як: «ПС-Персонал», «Бібліограф», «Деканат-Університет-Web», які використовуються для введення та збереження інформації тобто використовуються як банки даних. Головним недоліком пакетів, які представляє ПП »Політек-софт», є відсутність підтримки кредитно-модульної системи.

Програмний комплекс «ВНЗ АЛЬМА-МАТЕР» дозволяє автоматизувати діяльність співробітників, що пов'язана з одержанням, обробкою, зберіганням й аналізом даних, необхідних для функціонування ЗВО. До складу програмного комплексу входять наступні модулі: «Приймальна комісія», «Деканат/навчальна частина», «Навчально-методичний відділ» (з можливістю формування розкладу занять).

Головні переваги комплексу:

– модульність – можливість придбання програмного забезпечення частинами, а не цілим комплексом. Програмний комплекс допрацьовується під потреби кожного ЗВО індивідуально;

– програмний комплекс розроблено відповідно до вимог Болонського процесу.

Функціональні можливості модулів:

1. Приймальна комісія: тестування абітурієнтів, автоматичне зарахування тих, які пройшли вступні тести; автоматичне занесення результатів поточних електронних тестів (іспитів/заліків) до бази даних; облік усіх абітурієнтів і студентів в єдиній базі даних.

2. Деканат/навчальна частина: облік успішності, рубіжний контроль; надання вільного доступу до інформації про відвідуваність та успішність студентів; облік особистих карток усіх студентів в єдиній базі і швидкий їх пошук; автоматизація введення заліково-екзаменаційних відомостей; автоматичне формування наказів на відрахування, списків груп студентів, їх особистих карток, журналів та інших стандартних документів як внутрішнього, так і зовнішнього документообігу; полегшення створення документів про переміщення студентів із збереженням історії про зміни для подальшого аналізу; модуль обліку оплати за навчання, з можливістю встановлення індивідуальних розцінок для кожного студента і загальних по групах/потоках; формування друкованих форм «додатків» до дипломів/атестатів. Можливість зберігання бази даних виписаних дипломів/атестатів, їхні серії і номери; модуль розрахунку середньої успішності по групі/потоку/викладачеві/ навчальному закладу тощо.

3. Навчально-методичний відділ: облік викладацького складу; розрахунок погодинного навчального навантаження для викладачів; розрахунок фактично виконаного навантаження; можливість використання різних схем розрахунку, обліку і планування; формування навчальних і робочих планів; складання розкладу занять;

автоматизація створення звітів для аналітичного відділу. Формування звітів установленого зразка для служби статистики.

Дослідження, що проведені в сфері управління вищою освітою, показали недостатній рівень впровадження, використання і застосування можливостей існуючих ІАС оцінювання рівня якості освіти у ЗВО, які призначенні для удосконалення організації та проведення освітнього процесу. До основних недоліків можна віднести наступні: недостатньо ефективно використовується узагальнена інформація стосовно якості підготовки фахівців при виробленні управлінських рішень щодо здійснення коригування ОП; застосування лише адміністративних функцій; не в повній мірі задовольняються потреби оперативного аналізу даних; недостатній рівень проведення контролю результатів оцінювання рівня якості організації ОП у ЗВО; не враховується специфіка підготовки військових фахівців.

Головними вимогами щодо створення ІАС оцінювання рівня якості освіти у ЗВО є принцип неперервності, поетапності, послідовності та своєчасності забезпечення реагування системи на відхилення ОП від заданого рівня. Адекватність реагування ІАС оцінювання рівня якості освіти у ЗВО на відхилення від заданого рівня визначається кількістю показників, які характеризують стан рівня якості освіти у ЗВО.

При розробці ІАС оцінювання рівня якості освіти у ЗВО треба враховувати наступне:

1. Інформаційна технологія оцінювання якості освіти у ЗВО повинна передбачати відстеження показників трьох її основних складових: умов організації (управління, адміністративно-господарські процеси); освітнього процесу (відстеження навчальної, виховної, методичної, наукової, навчально-пізнавальної діяльності в її сукупності); та результатів навчання. Стосовно кінцевого результату, необхідним його показником повинен бути інтегральний показник «Інтегральна компетентність випускника ЗВО за спеціальністю». За цим показником перевіряється відповідність рівня теоретичної та практичної підготовленості фахівця на посаді первинного призначення вимогам замовника.

2. Напрямками формування оцінювання рівня якості освіти у ЗВО повинні бути: дослідження освітнього середовища; дослідження організації і результативності ОП; дослідження якості управління організацією і проведенням ОП у ЗВО.

3. Об'єктами, що впливають на рівень якості освіти у ЗВО повинні бути: індивідуальні досягнення тих, хто навчається (ключові компетенції, знання, уміння, навички, досягнутий рівень розвитку особи і соціалізації випускників); діяльність науково-педагогічних працівників (процес і результативність); державний стандарт (освітні програми); діяльність і досягнення ЗВО за напрямами діяльності, в тому числі й органів управління.

4. Суб'єктами системи оцінювання рівня якості освіти у ЗВО повинні бути: органи управління освітою; замовники; управління ЗВО (ректор та його апарат, відділи та служби); кафедри (завідуючий, науково-педагогічні працівники); ті, хто навчаються. При цьому, інтегральним показником оцінювання навчального досягнення студента є рівень засвоєння ними змістових модулів у визначений період часу. Причому, для порівняння важливості (складності) того чи іншого змістового модуля (наприклад, професійно-орієнтованого чи допоміжного) вводиться певна система їх вагових коефіцієнтів. Вага того чи іншого модуля визначається за допомогою методу А. Сааті.

Інформація про стан рівня якості освіти у ЗВО формується для: аналізу результатів поточного стану організації і проведення ОП у ЗВО (за показником навчальні досягнення) – компетенція викладачів кафедр, факультетів, навчального відділу; втручання керівника для коригування процесу організації і проведення ОП у ЗВО; оцінювання якості вихідної інформації з боку керівництва ЗВО (замовників, органів управління).

Створення ІАС оцінювання рівня якості освіти у ЗВО дозволить формалізувати та актуалізувати слабо структуровані і неструктуровані дані з оцінювання якості освіти у ЗВО, а також формувати бази знань, яка використовуються як інструмент для проведення аналізу відповідності рівня якості ОП вимогам нормативно-правових актів з питань організації і проведення ОП у ЗВО; сприяти вибору альтернатив особою, що приймає рішення з формування управлінських впливів на складові елементи ОП у ЗВО для його коригування для забезпечення якості освіти у ЗВО на рівні не нижче заданого.

УДК 004.942

Чесановський І.І.

МУЛЬТИАГЕНТНЕ УПРАВЛІННЯ РЕСУРСАМИ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Реалізація концепції інтегрованого управління кордонами [1], в умовах стрімкого розвитку інформаційних технологій, вимагає постійного пошуку та впровадження інноваційних рішень як на етапі проєктування систем так і на етапі їх експлуатації. Нові моделі, зокрема концептуальні, в інформаційно-технічній галузі з’являються і впроваджуються зі швидкістю, що практично унеможливлює повну планову розбудову складних інфраструктурних рішень без модернізації ще на початкових етапах. Однією з нових концепцій побудови складних інформаційно-технічних систем, є парадигма кіберфізичних систем (КФС) [2]. На сьогодні, в теорії КФС міститься потужна науково-методологічна база спрямована на впровадження ефективних підходів побудови складних, розподілених (мережевих) інформаційно-технічних рішень [3], з гнучкою багаторівневою архітектурою організації технічних, інформаційних та обчислювальних ресурсів. Концепція КФС може стати основою комплексного підходу побудови системи інформаційно-технічного забезпечення охорони кордону, яка дасть змогу інтегрувати елементи існуючої інформаційної і технічної інфраструктури в новій архітектурі без необхідності їх глибокої модернізації. Це вкрай актуальна проблема на сучасному етапі функціонування більшості інформаційно-технічних систем (ІТС), що характеризується відсутністю єдиного підходу інтеграції засобів та систем різних поколінь, різних моделей управління, стандартів та протоколів обміну інформацією, тощо. Крім того, інтенсивне використання широкого спектру смарт-технологій, яке спостерігається в останній час, створює міцний фундамент для запровадження високоефективних моделей розподілених обчислень, що є основою більшості сучасних інформаційних сервісів та моделей управління в ІТС з мережевою архітектурою [4]. Завдяки об'єднанню різних засобів спостереження, аналітики та оперативного реагування в єдину багаторівневу КФС, можливе підвищення ефективності моніторингу, оцінки ризиків та координації дій на державному кордоні.

Вагомою проблемою побудови КФС є інтеграція багаторівневих моделей управління на основі алгоритмів штучного інтелекту [1], що потребують значних обчислювальних ресурсів та концентрації інформаційних потоків в межах невеликої кількості обчислювальних вузлів. Альтернативою цьому підходу є мультиагентні системи (МАС) управління [5], що не потребують концентрації інформаційних і обчислювальних ресурсів а існують у вигляді окремих алгоритмічних сутностей в інформаційно-комунікаційному просторі ІТС.

У контексті управління складними розподіленими технічними системами, МАС представляють собою підхід, де кілька автономних агентів (програмно-алгоритмічні сутності, що містять моделі глибокого машинного навчання) взаємодіють між собою та з середовищем для досягнення певних цілей або вирішення складних завдань. Кожен

агент має свої власні цілі, знання та можливості, які визначаються складністю моделі та її початковою «навченістю». Колективна поведінка агентів призводить до їх взаємної адаптації спрямованої на забезпечення максимальної ефективності функціонування системи управління в цілому.

Ключовими особливостями мультиагентного підходу управління в системах зі складною, архітектурою є неявна цілеспрямованість системи управління на досягнення глобальної цілі. Це досягається за рахунок застосування децентралізованої моделі управління, яка утворюється з автономних, взаємопов'язаних елементів (агентів). Характерними рисами такої системи є [5]: автономність – кожен агент приймає рішення самостійно на основі свого сприйняття середовища та своїх внутрішніх правил або навченої поведінки; розподіленість – керування системою розподілене між окремими агентами, що підвищує стійкість та гнучкість; взаємодія – агенти обмінюються інформацією, координують свої дії або конкурують один з одним для досягнення своїх цілей або цілей системи; складність – розподілені системи є складними за своєю природою і мультиагентний підхід може допомогти розбити складну проблему на менші, керовані частини, де кожен агент відповідає за певну підзадачу; адаптивність - використання підкріплюючого навчання дає змогу агентам адаптувати свою поведінку до змін у середовищі та навчатися оптимальних стратегій взаємодії.

Здатність до навчання агентів надає важливу перевагу системі управління, яка полягає в стійкості до невизначених наперед станів. Кожен агент, як елемент системи управління, має певні базові навики і починає функціонувати спочатку в невідомих йому варіантах середовища. В процесі функціонування відбувається «донавчання» внутрішньої моделі і кожен агент стає більш компетентним у порівнянні з тим, що могли б дозволити тільки його початкові знання. Математичне формулювання поведінки агентів у таких системах може ґрунтуватись на принципах підкріплюючого навчання (Q-навчання). В цьому випадку визначення оптимальної дії в кожному стані визначається системою штрафів і винагород, що особливо ефективно себе проявляє в умовах кооперації агентів при колективному вирішенні завдань. Такий підхід не вимагає чіткого формулювання цілі управління і шляхів її досягнення, а зводиться лише до декількох формальних наборів дій агентів, можливих подій і їх наслідків для окремих агентів (розміри штрафів і винагород). В процесі функціонування, агенти, які не здатні вирішити деяку задачу самостійно, можуть «пропонувати» її вирішення іншим агентам, що складає основу процесу кооперації – використання колективу агентів для вирішення одного загального складного завдання. В більш потужних системах (ускладнення внутрішніх моделей машинного навчання агентів), агенти можуть вибудовувати плани дій, ґрунтуючись вже не тільки на своїх можливостях, але і «думати» про плани і наміри інших агентів. Сучасні МАС, побудовані навіть на основі найпростіших агентів, що переслідують тільки свої примітивні цілі, в загальному здатні вирішувати дуже складні завдання в динамічному оточуючому середовищі, що є недосяжним для інших типів систем автоматичного управління.

Список використаних джерел

1. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року. Офіційний вебпортал парламенту України : веб-сайт. URL : https://zakon.rada.gov.ua/go/687-2019-%D1%80 (дата звернення: 02.10.2024).
2. Lee E.A. Cyber Physical Systems: Design Challenges. 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC) : 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing. Orlando, FL, USA : IEEE, 2008. Cyber Physical Systems. С. 363–369. URL : http://ieeexplore.ieee.org/document/4519604/. (дата звернення : 31.10.2024).

3. The network platform cyber-physical systems application for smart buildings air pollution indicators monitoring. O. Duda, A. Mykytyshyn, M. Mytnyk, A. Stanko. 2023.
4. The development of methods for evaluating the state of complex technical systems using artificial intelligence theory : Information and control systems: modelling and optimizations. Kharkiv, Ukraine : Technology center PC, 2024. 32 с.
5. Konovalenko O., V. Brusentsev. Multi-agent management and decision support systems. Bulletin of the National Technical University «KhPI» Series: Engineering and CAD. 2019. Вип. 0. № 1. С. 18–27. 10.20998/2079-0775.2019.1.03.

УДК 621.396.962

Шаповал Л.О., Давиденко В.В., Дмитренко В.В.

ШЛЯХИ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЗАСОБІВ ДЛЯ ВІДНОВЛЕННЯ НЕСПРАВНОЇ (ПОШКОДЖЕНОЇ) ТЕХНІКИ

Сучасні бойові дії доводять, що ефективність військових підрозділів залежить не лише від потужності озброєння, а й від здатності швидко відновлювати пошкоджену техніку [1, 2]. Чим оперативніше повертається бойова техніка до виконання завдань, тим вищі рівень бойової готовності військових підрозділів і вище ефективність використання військової техніки [3, 4]. Тому на сьогодні зростає роль безпілотних засобів (БПЗ) наземного та повітряного використання, які можуть значно покращити процеси контрольного огляду діагностики, евакуації та ремонту зразків військової техніки при веденні бойових дій [5].

Застосування БПЗ у військових операціях за останнє десятиліття стало невід'ємною складовою ведення бойових дій [4, 6]. Вони використовуються для розвідки, коригування вогню, вогневого ураження, забезпечення логістики та, навіть, для медичної евакуації [3, 7]. Проте потенціал БПЗ у сфері ремонту та відновлення техніки ще недостатньо досліджений і реалізований.

Використання безпілотників (повітряного та наземного використання) може суттєво скоротити час ремонту та знизити ризики для персоналу, який працює в зоні бойових дій. Вони можуть виконувати огляд пошкоджень на полі бою, допомагати у транспортуванні інструментів і дрібних запчастин, а також безпосередньо брати участь у ремонтних роботах за допомогою спеціалізованих маніпуляторів або технічних модулів.

Військові конфлікти сучасності, у тому числі війна на території України, показали зростаючу роль автономних і дистанційно керованих технологій у всіх сферах бойових дій, зокрема в технічному обслуговуванні та ремонті військової техніки.

Наразі деякі країни, зокрема США, Ізраїль і Китай, активно впроваджують роботизовані системи і БПЗ у процеси технічного забезпечення військ. Деякі з цих систем використовуються для:

– огляду пошкодженої техніки і збору даних про її технічний стан;
– доставки запасних частин та інструментів без ризику для людей;
– евакуації легкої техніки або пошкоджених вузлів за допомогою вантажних апаратів;
– зварювальних і ремонтних робіт у важкодоступних місцях за допомогою маніпуляторів, які керуються через БПЗ;
– моніторингу ефективності відновлення техніки та координації ремонтних підрозділів.

Попри успішні експериментальні дослідження щодо використання БПЗ при відновленні військової техніки залишаються фрагментарними. Відсутня

стандартизована система інтеграції безпілотників у ремонтні підрозділи, а також немає чітких алгоритмів їх застосування. Це робить питання дослідження ефективності їх використання актуальним для військових досліджень.

Мета дослідження полягає у розробці шляхів використання підрозділів БПЗ у процесі відновлення пошкодженої (несправної) техніки під час бойових дій. При обґрунтуванні зазначених шляхів також оцінюється ефективність використання БЗП для відновлення зразків техніки, що полягає у визначені впливу БПЗ на зменшення часу ремонту та підвищення безпеки особового складу при проведенні ремонту та обслуговування військової техніки.

Для досягнення мети роботи необхідно вирішити такі завдання:

1. Провести аналіз існуючих підходів до використання БПЗ у військових умовах, зокрема у сфері ремонту та евакуації техніки.
2. Визначити типи БПЗ, які можуть бути ефективно задіяні в процесах технічного обслуговування та ремонту техніки.
3. Оцінити переваги і недоліки використання безпілотників для відновлення техніки в різних умовах бойових дій.
4. Розробити моделі інтеграції БПЗ в структуру ремонтних підрозділів.
5. Визначити потенційні загрози і обмеження щодо використання БПЗ для технічного забезпечення військ.
6. Обґрунтувати практичні рекомендації щодо оптимізації застосування БПЗ при ремонті військової техніки.

При цьому результати дослідження пропонується використовувати для:

– розробки нових тактик і стратегій застосування БПЗ у військових ремонтних підрозділах;

– підвищення оперативності ремонту техніки та зменшення часу простою військової техніки;

– зниження ризиків для особового складу ремонтних підрозділів при дії в умовах бойового зіткнення за рахунок автоматизації та дистанційного контролю за процесом ремонту та обслуговування;

– розвитку нових типів спеціалізованих військових безпілотників (повітряного та наземного використання) для ремонту та технічного обслуговування техніки;

– вдосконалення військової логістики за рахунок використання автономних систем доставки запчастин та інструментів.

Отримані висновки можуть бути корисними при проведенні наукових досліджень з питань удосконалення системи технічного забезпечення військових підрозділів.

Список використаних джерел

1. O. Daki, S. Herasimov and H. Zubrytskyi, **Digital Correlation Method For Power Measurement**, *Information Processing Systems*, № 4 (163), 2020, p.p. 15-26, https://doi.org/10.30748/soi.2020.163.02.
2. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.
3. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.
4. S. Herasimov, M. Pavlenko, E. Roshchupkin and etc. **Aircraft flight route search method with the use of cellular automata**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, is. 4, 2020, p.p. 5077-5082, https://doi.org/10.30534/ijatcse/2020/129942020
5. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of**

airspace radio engineering monitoring systems, *International scientific and practical conference «Application of information technologies in the preparation and operation of law enforcement forces»*, March 15, 2022, p.p. 31-32.

6. O. Brytov, D. Bieliaiev, S. Kukobko and etc. **Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects**, *Proceedings of the 3rd International Scientific and Practical Conference «Scientific Trends and Trends in The Context of Globalization»*, UMEÅ, SWEDEN, 21-22.12.2021, p.p. 431-434, https://doi.org/10.51582/interconf.21-22.12.2021.050.
7. V. Dzhus, Y. Roshchupkin, S. Kukobko and etc. **Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method**, *Information Processing Systems*, 2021, Issue 4 (167), p.p. 19-26, https://doi.org/10.30748/soi.2021.167.02.

УДК 623.765

Шило С.Г., Першин О.О., Яцун Д.А., Пахомова А.М.

СИТУАТИВНЕ УПРАВЛІННЯ ВІДОБРАЖЕННЯМ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ В АСУ

Дослідженню методів управління відображенням інформаційних моделей (ІМ) при організації інформаційної підтримки процесу рішення задач управління приділяється значна увага. Алгоритмічні методи створення й управління ІМ дозволяють сформувати моделі, що відбивають алгоритм діяльності оператора. Ці моделі використовуються для управління одним складним об'єктом, наприклад, енергоблоком, ядерним реактором, тощо[1-4].

По способу відтворення інформації й застосовуваному методу управління ІМ можна виділити образотворчий підхід до відображення інформації без урахування алгоритму діяльності оператора [4].

Недоліками цього підходу до створення ІМ є:

- відображення інформації, необхідної для рішення однієї - двох задач управління;
- відображувана інформація не відповідає логіці роботи оператора;
- аналіз моделі вимагає великих витрат часу.

Наступний метод управління ІМ, заснований на образотворчому підході до відображення інформації з обмеженим урахуванням алгоритму діяльності оператора [1].

Такий підхід дозволяє створювати більш досконалі ІМ у порівнянні з методом, розглянутим вище. Недоліками підходу є:

- обмежене число програм управління ІМ;
- відсутність реалізації підтримки розпізнавання оперативних ситуацій;
- відсутність можливості адаптивного управління параметрами відображення ІМ;
- підтримка діяльності оператора по обмеженому набору алгоритмів рішення задач управління.

Таким чином, питання, пов'язані зі створенням методу управління відображенням ІМ, які дозволили б управляти нею з урахуванням складної обстановки й відповідно до задач, розв'язуваними оператором при управлінні складними динамічними об'єктами, досліджені й представлені в літературі недостатньо й вимагають проведення подальших досліджень.

Розробка методу управління відображенням ІМ, з урахуванням зазначених вимог, можлива при використанні методів визначення важливості ситуацій, що склалися[2, 5].

Представляючи результати розробки методу управління відображенням інформаційних моделей для систем управління складними динамічними об'єктами, слід враховувати особливості предметної області, що розглядається.

Основним етапом при розробці ІМ є етап визначення множини завдань, рішення яких покладене на оператора. Рішення кожного завдання, як правило, пов'язане з особливостями складної обстановки (ситуаціями). Таким чином, для рішення кожного завдання може бути сформована відповідна безліч ІМ.

У складних динамічних системах управління через великий обсяг інформації, що використовується в ній, застосовується наступний принцип: оператор в один момент часу може вирішувати тільки одне завдання. Отже, зміст розробленої ІМ дозволяє в один момент часу вирішувати тільки одну із ситуацій, що склалися. Таким чином, при виникненні ситуації, коли виявлено не одиничну ситуацію, що склалася, виникає завдання - ІМ якої з ситуацій необхідно представити операторові в першу чергу.

Рішення даного завдання можливо двома способами:

– на вибір оператора;

– автоматично, коли відповідний алгоритм за заданими критеріями вибирає ІМ пріоритетною ситуації

Перший спосіб, є більше простим у порівнянні із другим і не вимагає застосування спеціальних методів. При цьому, основним недоліком такого підходу до вибору ІМ є те, що необхідно додаткові витрати часу на роботу оператора. У свою чергу, для підвищення обґрунтованості ухвалення рішення оператором при виборі ІМ, доцільно виконати ранжирування ситуацій, що склалися.

Таким чином, для вирішення задач управління відображенням ІМ ситуацій, що склалися на робочому місці оператора виникає необхідність рішення наступних часткових задач:

– визначення факторів, що впливають на пріоритетність ситуацій, що склалися;

– ранжирування ситуацій, що склалися.

Для рішення часткової задачі визначення факторів, що впливають на пріоритетність ситуацій, що склалися, і їхнє ранжирування найбільш доцільним є використання методу експертних оцінок, а для ранжирування факторів, доцільно використати метод парних порівнянь.

Список використаних джерел

1. Dmitriiev O., Shcherbak G., Borozenec I., Shylo S., Melnichuk M., Herashchenko M. Method of adaptive control of the information model's display parameters depending on the complexity of the air situation. Сучасні інформаційні системи. Харків, 2020. Вип. 3(3). С. 37–42.
2. Харченко В.П., Шмельова Т.Ф., Сікірда Ю.В. Прийняття рішень оператором аеронавігаційної системи: монографія / В.П. Харченко, Т.Ф. Шмельова, Ю.В. Сікірда. - Кіровоград: КЛА НАУ, 2012. - 292 с.
3. Borozenec I., Dmitriiev O., Melnichuk M., Pavlenko M., Shcherbak G., Shylo S. Method development of the information models' design and synthesis for infocommunication systems of air traffic control. Сучасні інформаційні системи. Харків, 2019. Вип. 3(3). С. 37–42. doi: https://doi.org/10.20998/2522-9052.2019.3.05.
4. Павленко М.А., Шило С.Г., Борозенець І.О., Дмітрієв О.М. Метод формалізації процесу формування інформаційних ознак ситуацій обстановки в автоматизованих системах управління повітряним рухом. Системи управління, навігації та зв'язку. Полтава, 2019. Вип. 2(54). С. 22–27. URL: http://nbuv.gov.ua/UJRN/suntz_2019_2_7.
5. Шило С.Г. Побудова інформаційних моделей обстановки для диспетчерів

управління повітряним рухом / С.Г. Шило, А.С. Кумпан // Проблеми інформатизації: Тези доповідей восьмої міжнародної науково- технічної конференції. – Черкаси: ДТУ; Харків: НТУ «ХПІ»; Баку: ВА ЗС Азербайджанської республіки; Бельсько – Бяла: Університет технології і гуманітарних наук; ДП «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості» // Черкаси : ДТУ, 2021. – С. 58.

Шинкар Є.В., Лаврут О.О.

ВИКОРИСТАННЯ ІТ В ОРГАНІЗАЦІЇ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ

Відповідно вимогам сьогодення, використання інформаційних технологій (ІТ) має бути одним з пріоритетних напрямів роботи з підвищення ефективності логістичного забезпечення матеріально-технічними засобами в ЗС України. Застосування сучасних методів надасть низку переваг: підвищення ефективності управління запасами, швидкістю і точністю їх обліку, зниження витрат на зберігання й обробку даних; здійснювати обрахунки за допомогою програмного забезпечення, що дозволить зменшити витрати та час на організацію перевезень МТЗ; забезпечить скорочення часу на одержання і всебічну оцінку відомостей про МТЗ на всіх етапах їх руху; покращити взаємодію між органами забезпечення та підпорядкованими підрозділами щодо економії виділених матеріальних ресурсів [1-3].

ІТ розглядаються як автоматизовані системи управління логістичними процесами, які в свою чергу складаються з апаратного забезпечення, спеціального програмного забезпечення, кодифікації матеріальних засобів та інтерфейсу користувача. Для належного функціонування необхідно використовувати захищену мережу передачі даних, є потреба в забезпеченні більш сучасними, потужними ПЕОМ, відповідним обладнанням і проведенні додаткової підготовки особового складу [1-3].

Питання використання інформаційних технологій для забезпечення належного функціонування системи логістичного забезпечення в ЗС України у науковому дискурсі висвітлене, але потребує додаткового огляду та дослідження.

Так, надходження під час війни міжнародної технічної допомоги для ЗС України надало можливість впровадження спеціалізованого програмного забезпечення «Системи функціональних областей логістики» (Logistics Functional Area Services (LOGFAS)) для обліку військового майна, отриманого як міжнародна технічна допомога, а також – постачання наземних військ, яке надходить від країн партнерів. LOGFAS пришвидшує врегулювання звітності про наявність цього майна у ЗС України. Однак, використовується, здебільшого, для обліку і не дозволяє вносити в програмний код зміни. Впроваджується і автоматизована система управління оборонними ресурсами на базі System Analysis Program Development (SAP). Система проходить тестування щодо обліку речового та автомобільного майна.

Створення нових і модернізація існуючих автоматизованих систем забезпечення (постачання) матеріально-технічними засобами на основі передових інформаційних технологій дозволить підвищити ефективність логістичного забезпечення підрозділів тактичного рівня.

Список використаних джерел

1. Іохов О.Ю., Лаврут О.О., Лаврут Т.В., Флорін О.П. Сучасні засоби зв’язку та інфокомунікаційні технології у Збройних Силах України та Національній гвардії України: сьогодення та перспективи застосування. Честь і закон. 2022. № 4/2022. С. 113-122. DOI: https://doi.org/10.33405/2078-7480/2022/4/83/272323.

2. Лаврут О.О. Вибір критерію оцінювання якості управління потоками інформації у телекомунікаційній мережі мобільного компоненту перспективної системи зв'язку ЗС України. Наука і техніка Повітряних сил Збройних Сил України. 2014. Вип. 3 (16). С. 113-115.
3. Лаврут О.О. Перспективні підходи та технології побудови систем управління силових структур. «Findings of modern engineering research and developments»: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2022. P. 233-264. DOI: https://doi.org/10.30525/978-9934-26-207-4-9.

УДК 004.056

Штонда Р.М., Білий В.О., Черниш Ю.О., Терещенко Т.П.

БЕЗПАРОЛЬНА АВТЕНТИФІКАЦІЯ: ПЕРЕВАГИ ТА РИЗИКИ

Традиційні методи автентифікації, що базуються переважно на логінах користувачів та паролях, на сьогоднішній день не дають належних гарантій щодо захисту критично-важливої інформації та інформаційно-комунікаційних систем (ІКС). Зазвичай працівники використовують неналежні логіни та слабкі паролі. Із-за цього організації та установи намагаються розв'язати цю проблему за допомогою двофакторної автентифікації (2FA), але і вона не гарантує повного захисту критично-важливої інформації та ІКС [1]. Кіберзловмисники все частіше обходять дані методи за допомогою фішингових атак та методів соціальної інженерії. Тому безпарольна автентифікація стає тим засобом, що забезпечить надійний захист критично-важливої інформації та ІКС.

Безпарольна автентифікація – це сучасний підхід, що спирається на технологію FIDO та дозволяє мінімізувати факт викрадення критично-важливої інформації, проникнення в ІКС, а також підвищує рівень кібербезпеки та зручність для користувачів.

Безпарольна автентифікація ґрунтується на наступних основних технологіях:

– біометрична автентифікація (розпізнавання обличчя, сітківки ока, відбитків пальців, голосу);

– апаратна автентифікація (смарт-карти, USB-ключі, токени);

– одноразові паролі (генератори паролів, коди отримані у вигляді SMS-повідомлень);

– push-сповіщення (миттєві повідомлення, що генеруються за допомогою мобільних додатків та підтверджують вхід);

– автентифікація на основі аналізу поведінки користувача (моніторинг звичок).

Переваги використання безпарольної автентифікації:

– забезпечення підвищеної безпеки, що дозволяє усунути ризики виникнення фішингових атак, перехоплення паролів та їх повторного використання кіберзловмисниками;

– зручність для користувача, що виключить можливість втрати логіна чи паролю;

– зменшення звернень до адміністраторів безпеки щодо відновлення логінів та паролів;

– відповідна сумісність із сучасними стандартами кібербезпеки.

На ряду із перевагами у використані безпарольної автентифікації є наступні ризики:

– компрометація біометричних даних – у випадку заволодіння кіберзлочинцями даних про відбитки пальців, обличчя, сітківки ока, голосу їх буде неможливо змінити;

– залежність від апаратних пристроїв – у разі втрати кінцевого пристрою, смарт-карти, USB-ключа чи іншого фізичного носія може суттєво ускладнити доступ користувачу до критично-важливої інформації або ІКС;

– вразливість до кібератак на довіреність – у разі перехоплення кіберзлочинцями SMS-повідомлень чи push-сповіщення виникне загроза їх втрати , що може призвести до витоку критично-важливої інформації або блокування ІКС.

– низька адаптація – велика кількість організацій та установ ще залежить від паролів та не прикладає зусиль для переходу до безпарольної автентифікації.

Безпарольна автентифікація здатна підвищити захист ІКС, не допустити втрати критично-важливої інформації та є на сьогоднішній день перспективним напрямком щодо розвитку кібербезпеки в організаціях та установах всіх форм власності.

Список використаних джерел

1. Дія.Бізнес. Дія.Бізнес Старт. URL: https://business.diia.gov.ua/history-of-success/bezparolna_avtentyfikatsiia (дата звернення: 27.02.2025).

УДК 004.738

Шульга В.В., Першин О.В., Нікора І.В., Дзюба І.В.

ІНТЕЛЕКТУАЛЬНА СИСТЕМА АНАЛІЗУ ВІДКРИТИХ ДЖЕРЕЛ

Зазвичай аналітики стикаються з величезним потоком інформації з відкритих джерел (OSINT), включаючи новини, соціальні мережі, супутникові знімки та звіти очевидців. У сучасних умовах гібридних конфліктів та інформаційних війн стає дедалі складніше оперативно відстежувати події, ідентифікувати загрози та аналізувати їхній вплив.

У 2025 року обсяг даних, які генеруються, зберігаються та споживаються, вже перевищує 180 зеттабайт, що значно ускладнює їхню обробку та використання. Для порівняння, у 2020 році цей показник становив 64,2 зеттабайта. При цьому частка інформації, придатної для аналітичної обробки, зросла з 22 % у 2012 році до 37 % у 2020 році. Джерела цих даних охоплюють різні сфери, зокрема соціальні платформи, системи моніторингу, розвідувальні звіти та інші джерела [1].

Зі зростанням обсягів OSINT-даних виникає потреба у розробці платформи, здатної автоматизувати процеси збору, фільтрації та аналізу інформації. Така система повинна:

– агрегувати дані з відкритих джерел у режимі реального часу;

– класифікувати інформацію за тематичними категоріями (наприклад, військова техніка, переміщення військ, кібератаки, політичні події);

– автоматично створювати короткі аналітичні звіти на основі зібраних матеріалів;

– генерувати релевантні теги для спрощеного пошуку та структуризації даних;

– здійснювати автоматизований переклад контенту з іноземних мов для розширення аналітичного охоплення.

Розробка подібної платформи значно підвищить швидкість та ефективність аналізу інформації, дозволяючи експертам оперативно реагувати на потенційні загрози та приймати обґрунтовані рішення.

Веб-платформа для збору, обробки та аналізу даних з відкритих джерел поєднує технології аналізу тексту із використанням локально розгорнутих великих мовних моделей (large language models, LLM) та інформаційні технології з метою автоматизації збору, аналізу та представлення актуальної інформації.

На діаграмі (рис. 1) зображено модель платформи. Вона включає кілька ключових компонентів і модулів, які взаємодіють між собою для забезпечення роботи системи.

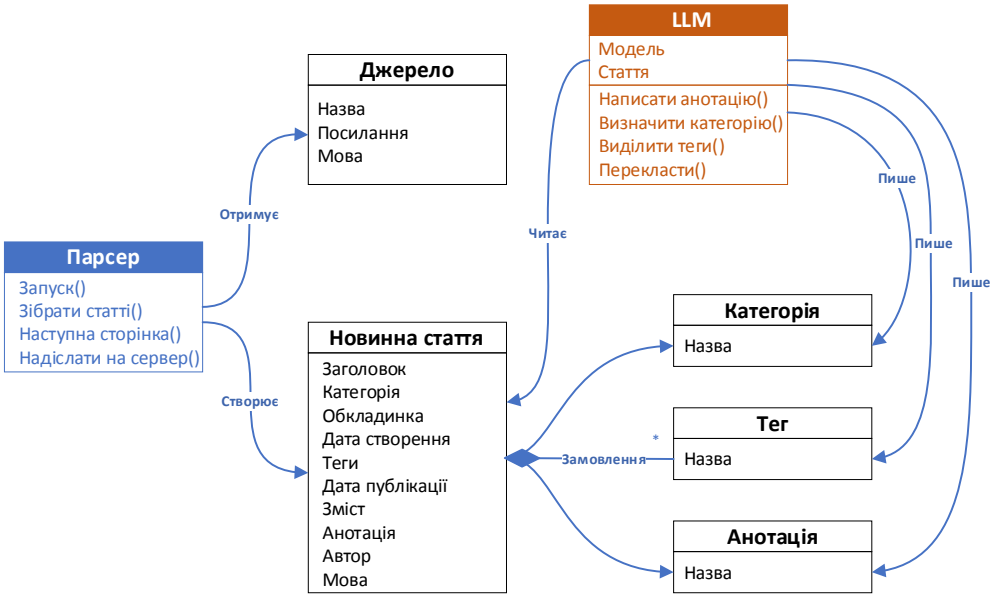


Рисунок 1 – Концептуальна діаграма веб-платформи

На діаграмі представлені такі ключові компоненти:

– **Парсер** – відповідає за вилучення інформації з джерел. Він збирає посилання на статті, переходячи по сторінках інформаційного ресурсу, після чого передає їх сервісу. Сервіс створює чергу посилань на статті для подальшого отримання їхнього контексту та надсилання на сервер бази даних;

– **Джерело** – надає інформацію, з якої парсер буде вилучати статті;

– **LLM** – обробляє статті, зібрані парсером, аналізує їхній вміст, створює анотації, визначає категорії, присвоює теги та виконує переклад;

– **Новинна стаття** – цей об'єкт містить інформацію про новинну статтю, включаючи заголовок, дату створення, посилання на джерело, обкладинку, зміст, категорію, теги, анотацію та мову;

– **Категорія** – містить категорію статті;

– **Тег** – містить теги, пов’язані зі змістом статті;

– **Анотація** – зберігає короткий опис змісту статті.

Основні компоненти системи для аналізу відкритих джерел, реалізовуються в контейнерах Docker. Кожен контейнер спеціалізується на виконанні своєї конкретної задачі. Для деяких груп контейнерів налаштовуються мережеві параметри для повної ізоляції одних груп від інших і вони повинні звертатися до цього контейнера через відповідні запити до API.

Веб-інтерфейс дозволяє користувачам взаємодіяти із системою через браузер і HTTP-запити. Клієнтські запити спрямовуються на фронтенд, розташований у відповідному контейнері. Nginx обробляє HTTP-запити, а додаток на Vue.js надає можливість перегляду статей користувачеві.

Використовуючи контейнеризацію, можна упакувати кожен сервіс зі всіма його залежностями в окреме ізольоване середовище для забезпечення єдності середовища як на етапі розробки, так і при розгортанні та підтримці платформи. Крім того, це дозволяє уникнути конфліктів між залежностями та різними версіями програмного забезпечення.

Серед найбільш поширених типів архітектури програмного забезпечення виділяють такі: монолітна, мікросервісна, багаторівнева, сервіс-орієнтована та клієнт-серверна [2].

Зважаючи на вимоги до OSINT-платформи, мікросервісна архітектура є найбільш

вдалим рішенням. Вона дозволяє розробляти, оновлювати та масштабувати окремі модулі без ризику для всієї системи. Контейнеризація (Docker) та оркестрація контейнерів (Docker Compose або Kubernetes) забезпечать ефективне управління ресурсами та високу стійкість до навантажень [3-4].

Цей підхід є оптимальним для аналізу відкритих джерел, де критично важливо швидко адаптуватися до змін інформаційного середовища, обробляти великі обсяги даних та своєчасно виявляти потенційні загрози.

Застосування мікросервісної архітектури здається досить обґрунтованим і перспективним рішенням, оскільки це дозволяє ефективно керувати різними компонентами системи, забезпечуючи їхню ізольованість і гнучкість. Кожен мікросервіс може бути створений, впроваджений і масштабований індивідуально, що спрощує процес розробки, оновлення та підтримки всієї платформи [5].

На основі аналізу популярних підходів до побудови програмного забезпечення можна зробити висновок про доцільність використання мікросервісної архітектури для розроблюваної платформи.

Подальший розвиток веб-платформи може включати оптимізацію продуктивності та масштабованості системи, паралельне виконання процесів парсингу й анотування даних, а також використання кешування для прискорення доступу до часто запитуваної інформації. Також є можливість розширення кількості джерел новинних статей шляхом додавання додаткових інформаційних ресурсів.

Список використаних джерел

1. Big data statistics: How much data is there in the world? *Rivery blog*: web site. URL: https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world (accessed 28.02.2025).
2. Основні типи архітектури програмного забезпечення. *Art of business analysis*: web site. URL: https://www.artofba.com/uk/post/main-types-of-software-architecture (accessed 28.02.2025).
3. Binani H. Kubernetes vs Docker Swarm – A Comprehensive Comparison HackerNoon. *HackerNoon - read, write and learn about any technology* web site. URL: https://hackernoon.com/kubernetes-vs-docker-swarm-a-comprehensive-comparison-73058543771e (accessed: 28.02.2025).
4. What is Docker? *Docker Documentation*: web site. URL: https://docs.docker.com/get-started/overview (accessed: 28.02.2025).
5. Microservices architecture design. *Learning for everyone, everywhere. Microsoft Learn:* web site. URL: https://learn.microsoft.com/en-us/azure/architecture/microservices (accessed 28.02.2025).

УДК 004.056.

Щадило П.Р., Площик А.С.

КІБЕРЗАХИСТ В УМОВАХ РЕАЛІЙ СУЧАСНОСТІ: ТЕХНОЛОГІЇ, МЕТОДИ ТА ПЕРСПЕКТИВИ

В умовах стрімкого розвитку інформаційного суспільства та зростання складності й витонченості кіберзагроз питання кібербезпеки набуває критичного значення. Сучасний світ усе більше залежить від цифрових технологій: фінансові операції, державне управління, охорона здоров'я, транспорт, освіта та багато інших сфер базуються на цифрових системах. Втрата або компрометація даних у таких галузях може мати катастрофічні наслідки, що впливає як на окремих користувачів, так і на

безпеку цілих держав. Захист цифрових систем та інформації вимагає впровадження сучасних методів і технологій, здатних протидіяти постійно еволюціонуючим загрозам.

За останні роки кількість атак на великі корпорації, урядові установи та об'єкти критичної інфраструктури значно зросла. Хакерські угруповання все частіше використовують передові методи, зокрема атаки із застосуванням штучного інтелекту, злом через уразливості ланцюгів постачання та складні багатоступеневі атаки (APT). Серед ключових викликів сучасної кібербезпеки – постійні хакерські атаки, несанкціонований доступ до конфіденційних даних, порушення їхньої цілісності та надійності.

Кібератаки можуть мати руйнівний вплив не лише на окремі організації, а й на суспільство загалом. Наприклад, атака вірусу-здирника WannaCry у 2017 році вразила сотні тисяч комп'ютерів по всьому світу, включаючи лікарні, державні установи та великі підприємства. Це призвело до збоїв у роботі медичних закладів, банківських установ та інших важливих сервісів.

Ефективне забезпечення кібербезпеки потребує комплексного підходу, що включає використання новітніх методів шифрування, багатофакторної аутентифікації, автоматизованого моніторингу мережної активності та систем швидкого реагування на інциденти. Впровадження цих технологій дозволяє мінімізувати ризики, підвищити рівень цифрової безпеки та захистити інформаційні ресурси. Такі заходи особливо актуальні для банківських установ, де витік даних може призвести до втрати мільйонів доларів, та для оборонної сфери, де злом систем може поставити під загрозу національну безпеку.

Однак кібербезпека – це динамічна сфера, що вимагає постійного оновлення та вдосконалення підходів до захисту. З кожним роком з'являються нові методи атак, які вимагають адаптивності та швидкого реагування. Традиційні методи, такі як антивіруси та міжмережеві екрани, вже не є достатніми для протидії сучасним загрозам, тому необхідно активно розвивати інноваційні стратегії. Серед таких стратегій – впровадження концепції Zero Trust, що передбачає постійну перевірку кожного доступу до системи, незалежно від того, чи є користувач внутрішнім чи зовнішнім.

Інвестиції в кібербезпеку стали не розкішшю, а необхідністю для будь-якої організації. Важливо не лише впроваджувати нові технології, а й навчати фахівців, підвищувати цифрову грамотність працівників та розробляти ефективні політики управління ризиками. Саме поєднання технологічних рішень, безперервного розвитку та підготовки кадрів є запорукою цифрової стійкості та ефективного захисту конфіденційної інформації в умовах нових кіберзагроз.

Тільки завдяки комплексному підходу та постійному вдосконаленню методів захисту можна забезпечити надійний кіберпростір, що стане основою безпечного функціонування цифрового суспільства.

УДК 004.738

Щербакова П.В., Новічков В.О.

ВИКОРИСТАННЯ ТЕЛЕМЕТРИЧНИХ СИСТЕМ У ВІЙСЬКОВІЙ СПРАВІ

У сучасній війні обчислювальні системи та інформаційні технології відіграють ключову роль в процесі управління військовими операціями, як оборонного так і наступального характеру. Вони допомагають військовим командирам різного рівня вчасно приймати обґрунтовані та ефективні рішення. Телеметрія це процес збору та передачі даних на відносно великих відстанях. Телеметрія є невід'ємною складовою

сучасних інформаційних систем, суттєво доповнює та розширяє їх функціонал. Телеметричні системи, як правило складаються з датчиків та системи передачі даних, що включає в себе канал зв'язку, передавальне та приймальне обладнання. Під час повномасштабного вторгнення росії на територію України телеметричні системи стали широко використовуватися в безпілотних летальних апаратах. Вони забезпечують ефективну передачу даних, необхідних для управління безпілотними літальними апаратами, артилерією, та логістикою, а також інформацію для розвідки. Додатково, телеметрія дозволяє проводити автоматичний аналіз параметрів боєздатності техніки та створення ефективних маршрутів для підрозділів, що виключає ризик зайвого пересування через небезпечні зони. Використання телеметричних систем забезпечують зменшити втрати серед військових, покращити точність ударів та оптимізувати бойові дії. Окрім цього, такі системи дозволяють створювати інтегровані мережі для обміну інформацією між різними військовими підрозділами, що значно підвищує оперативність дій.

Основні функції використання телеметричних систем: моніторинг техніки та особового складу, дистанційне керування безпілотними системами, аналіз та передача даних у реальному часі, удосконалення відпрацювання артилерійських ударів. Також телеметрія використовується для прогнозування логістичних потреб, таких як забезпечення боєприпасами, пальним і продовольством, що дозволяє забезпечити безперебійність у постачанні. Крім того, завдяки сучасним телеметричним системам можлива інтеграція з системами кіберзахисту, що мінімізує ризик перехоплення або втрати даних під час бойових дій. Перевагами використання телеметричних систем є можливість нанесення ударів з мінімальним ризиком для цивільних, отримання необхідних даних без затримок, дистанційний моніторинг, автоматизація процесів, захист техніки та ресурсів, яка попереджає про несправності та оптимізацію використання техніки, можливість швидкого перенаправлення ресурсів.

Телеметрія надає перевагу над ворогом підвищуючи ефективність військових операцій, покращуючи координацію підрозділів та мінімізуючи ризики. Нове покоління телеметричних систем також передбачає використання штучного інтелекту для аналізу великих обсягів даних, що дає змогу не лише швидко реагувати, а й передбачати наступні кроки ворога. Використання елементів машинного навчання в системах телеметрії дозволяє адаптуватися до змін у реальному часі, створюючи автоматизовані прогнози та допомагаючи командирам приймати оптимальні рішення. Сучасні технології активно впроваджують нові розробки телеметрії, що дозволяє швидше адаптуватися до змін у бойовій обстановці та отримувати перевагу над противником.

Яровий В.С., Гулій В.С., Денісова В.В., Мордвінов М.О.

ІНІЦІАТИВА ПРОЦЕСУ ВІДНОВЛЕННЯ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ АГРЕГАТНИМ МЕТОДОМ РЕМОНТУ

Війна в Україні поставила нові виклики перед технічним забезпеченням озброєння та військової техніки. Прийняття на озброєння підрозділів Збройних Сил України дуже великої кількісті нових зразків озброєння та військової техніки, враховуючи надходження техніки країн-партнерів зі всього світу, яка побудована на новій сучасній елементній базі привели до того, що ремонт озброєння та військової техніки на рівні окремих елементів вузлів та агрегатів важко реалізувати не тільки силами розрахунків але й ремонтно-відновлювальним органом військової частини.

Враховуючи ці обставини, під час виконання підрозділами завдань за призначенням доцільно застосовувати агрегатний метод ремонту озброєння та військової техніки при

якому відновлення відбувається за рахунок заміни агрегатів на нові або заздалегідь відремонтовані.

Для вирішення цих завдань пропонується ініціатива, що містить опис принципів побудови та функціонування системи ремонту. В загальному вигляді структуру елементів, які входять до складу ремонтно-відновлювальних органів військових частин всіх рівнів ієрархії можна представити у вигляді таких елементів:

– канали ремонту озброєння та військової техніки, які включають в себе спеціалістів з ремонту озброєння та військової техніки, комплекс необхідної технічної документації;

– діагностичне обладнання та спеціальне обладнання;

– запасні частини, інструменти, приладдя, експлуатаційні та витратні матеріали необхідні для проведення ремонту;

– накопичувач на виході каналу ремонту.

Озброєння та військова техніка, що потребує ремонту надходить до ремонтно-відновлювального органу військової частини всіх рівнів ієрархії на вході яких знаходиться канал дефектації. Відповідно до технічного стану озброєння та військова техніка поділяється на:

– працездатну;

– непрацездатну;

– ремонт якої є неможливим або економічно не доцільним.

Після дефектації зразки озброєння та військової техніки, які потребують проведення поточного, середнього та капітального ремонту надходять до накопичувача і при досягненні певної кількості, або у визначений час, партією направляються в ремонтний орган військової частини або органи вищого рівня ієрархії системи відновлення або ремонтні підприємства. Озброєння та військова техніка, ремонт яких є технічно неможливим або економічно не обґрунтованим списується з обліку військової частини встановленим порядком. Відновлене озброєння та військова техніка може направлятися на бази зберігання або до ремонтно-відновлювальних органів відповідних рівнів ієрархії.

Процес відновлення озброєння та військової техніки військової частини постійно знаходиться під керівництвом підсистеми управління, яка представлена органами різних рівнів ієрархії.

Таким чином представлена ініціатива відображає можливі варіанти побудови системи ремонту озброєння та військової техніки військової частини, враховує зв’язки окремих елементів, фактори, які впливають на озброєння та військову техніку та процес їх відновлення, технологічні процеси та може слугувати основою для:

– постановки задачі математичного моделювання процесу відновлення озброєння та військової техніки військової частини і розроблення математичної моделі;

– виявлення та визначення переліку показників системи, формування системи показників ефективності для оцінки якості її функціонування та визначення обмежень.

ЗМІСТ

Bordunova K. Problems of Using Frequency Hopping Spread Spectrum (FHSS) Signals in UAV Control Channels ……	5
Dyadun S. Information System for Modeling and Control of the Functioning of the City's Gas Supply Network ……..……	6
Iokhov O., Ishchuk O. Proposals for the Implementation of Artificial Intelligence into the JCATS Simulation System …….	7
Iokhov O., Liwång H., **Krahn U.** Modern Simulation Technologies for Tactical-Level Officer Training: the Case of Steel Beasts Usage ……..……	8
Kharchenko I., Lysechko V. Fixed Reallocation Method of Frequency Positions Among Channels in QOFDM ……...	9
Kubiavka M., Pyrogov K. Application of Reflexive Intelligent Systems for Processing Natural Language Information in Information Systems Education Quality Management …….	10
Shevchenko O., Perets K., Lysechko V. Expanding Approaches to the Evaluation of Signal Correlation Properties in Cognitive Networks ……..	11
Shubina H., Komar O., Lysechko V. Analysis of the Impact of Time Segmentation on the Efficiency of Telecommunication Systems ……..……	12
Sovhar O. Digital Tools for Defense: Leveraging Technology for Language Proficiency in Ukraine …….	12
Sporyshev K. Problematic Aspects of Information and Analytical Activities of Ukraine's Security Forces …….	14
Tupitsya I., Kryvonos V. Methodology for Restructuring Aircraft Intelligence Data for Unmanned Aircraft Info Communication Systems ……	15
Vasylyshyn V. Spectrum Monitoring Method for Communication Systems Based on Cognitive Radio …….……..	17
Vlasov K. The Role of IoM/BT Technologies in Ensuring Combat Effectiveness of Military Units …….…….	18
Yakovlev S., Uzlov D., Strukov V., Kobziev V. Handling Outliers in Data Processing and Swarm Algorithms ……..….….	20
Адаменко А.А., Антонов Д.В., Порохончук О.М. Імітаційно-тренажні та моделюючі системи для підготовки фахівців протиповітряної оборони ……..….	21
Бабенко О.І., Сізон Д.О., Калачова В.В. Проектування системи інформаційно-аналітичного забезпечення військової організаційної структури ……...	23
Балабуха О.С., Качуровський Г.М., Максимов М.О., Споришев К.О. Пропозиції щодо розробки автоматизованої системи підтримки прийняття рішення командира мобільного комплексу озброєння у складі підрозділу (частини) ракетних військ і артилерії сухопутних військ ……	24
Баранов Ю.М., Баранов А.М., Каршень А.М. Обґрунтування вимог до застосування роботизованих комплексів подолання інженерних загороджень …	26
Басараб О.К., Мішенюк Р.М. Щодо збільшення дальності польоту FPV-дронів	28
Безкоровайний В.В. Оптимізація топологічних структур мереж великомасштабного моніторингу ……..……..	29
Безкоровайний В.В., Драз О.М. Адаптація логістичних мереж в умовах надзвичайних ситуацій …….…..……	31
Бєрнік Є.В., Худов Г.В. Метод визначення координат розвідувальних БпЛА мережею двох SDR приймачів ……..	33
Биков О.М., Пришляк І.В., Дидюк В.Г. Розробка навчально-лабораторного стенду для дослідження систем управління двигунами зразків військової техніки	34

Бокачов С.В., Чаган Ю.А., Марцінко Н.М., Варванець Ю.В. Потреба розвитку системи управління логістичним забезпеченням військових формувань ЗСУ та правоохоронних органів під час виконання ними службово-бойових завдань в сучасних умовах ……..….	37
Бриженюк Ю.Д., Братченко Г.Д., Лукаш Р.В. Напрями підвищення живучості безпілотних наземних комплексів в умовах бойових дій ……..…..	39
Бричинський О.В., Малюк В.М., Контуров В.М. Застосування інформаційних технологій під час підготовки саперних груп ……..…..	42
Бурак А.В., Воловоденко Ю.М., Мосійчук М.В. Імітаційна модель діагностування технічного стану двигунів бронетанкової техніки ……..	44
Валько В.В., Бабарика А.О. Можливості тандемного застосування БПЛА та баражуючого боєприпасу для збільшення дальності ураження цілей ……..…	46
Винту А.О., Мільшин С.І. Ройові безпілотні системи – стратегічний потенціал для оборони України в умовах повномасштабної війни …….…….	47
Гетьман А.В., Плугова О.Б., Сайко В.Г., Комаров В.О. Аналіз методів та засобів радіоелектронної боротьби в умовах бойових дій …….…..……	48
Глущенко М.О. Охоронні комплекси на основі радіолокаційних засобів виявлення ……..…..	51
Горєлишев С.А., Залевський Г.С. Ітераційний метод розрахунку характеристик розсіювання деяких комбінованих об’єктів резонансних розмірів …….…..	52
Давіденко С.В., Заєць Я.Г., Рижов Є.В., Опалинський В.Б. Щодо інтегрування трекера в систему керування польотом безпілотного літального апарата …….....	54
Даник Ю.Г. Управління ризиками використання штучного інтелекту ……..…	55
Данило Н.Р., Данильчук Р.О., Площик А.С. Аналіз методик розпізнавання об'єктів з відеопотоку за допомогою нейронних мереж …….…….	59
Данилюк І.А., Радзівілов Г.Д., Куцаєв В.В. Інтеграція квантових технологій у військові спеціальності: необхідність, виклики та перспективи …….……	62
Дубовський Ю.В., Присяжний А.Є., Карлов В.Д. Аналіз можливостей дистанційного керування стрілецькою зброєю …….....	64
Дуболазов Ю.О., Коротій О.О. Оптимізація пошуку: векторні бази даних …...	65
Душкін В.Д. Сидоренко І.І. Дослідження використання інтернет-ресурсів здобувачами освіти при вивченні математичних дисциплін …….…..…	67
Жилінський І.В., Яровий В.С., Свідзінський Ю.О., Ющенко Ю.М. Варіант введення комплексної оцінки надійності базового шасі рухомого складу озброєння та військової техніки …….…….	68
Заєць Я.Г., Давіденко С.В. Щодо протидії виявленню роботи станцій супутникового зв’язку «Starlink» засобами радіотехнічної розвідки ……..……..	69
Зінченко М.О., Сайко В.Г., Комаров В.О. Аналіз застосування безпілотних літальних апаратів для рішення бойових і спеціальних завдань …….……..….	70
Зубков А.М., Годебський В.П., Каменцев С.Ю., Сірий Ю.І. Локаційний геомоніторинг прибережної водної поверхні в інтересах антидиверсійного захисту …….……..	73
Зубков А.М., Красник Я.В., Мартиненко С.А. Недопплерівський метод підвищення максимальної дальності радіолокаційного спостереження наземних цілей …….……..	75
Іванець М.Г., Горєлишев С.А., Іванець Г.В., Баулін Д.С., Хроль Л.О., Кириченко М.І. Системний підхід до розробки керуючого алгоритму оцінювання боєздатності військових підрозділів ……..……	76
Калачова В.В., Місюра О.М., Бабенко О.І., Гаврилов Д.С. Втілення досвіду застосування інформаційних технологій дистанційного навчання провідними закладами вищої освіти України в підготовку та діяльність силових структур в	78

умовах воєнного стану ……..	
Катеринчук І.С., Хоптинський Р.П. Використання п'єзорезонансних систем у кіберфізичних системах охорони державного кордону …….	81
Катунін А.М., Коломійцев О.В., Роянов О.М., Щолок А.В. Оцінювання нагріву навантажених алюмінієвих проводів із домішками титану у складі струмовідних жил ……..	83
Кисіль Г.А., Дядюн С.В. Розробка інформаційної системи інтерактивного перекладу текстів для мов, що використовують ієрогліфи …….…….	85
Кізло Л.М., Андреєва Л.М., Луньков А.В., Матала І.В. Особливості формування особистої і корпоративної обізнаності персоналу щодо захисту кіберпростору України в умовах воєнного стану …….…….	87
Кобзев Д.О., Суровицький С.В. Підходи до балансування продуктивності та захищеності у високонавантажених інформаційних системах …….	90
Козлов Ю.В., Новикова О.О. Вирішення завдань педагогічної кваліметрії методами нечіткої математики …….……	91
Коломійцев О.В., Комаров В.О., Пустоваров В.В., Іохов О.Ю. Метод проведення оптико-візуального контролю високорозташованих конструкцій планерів бойових літальних апаратів …….…….	93
Коломійцев О.В., Рудаков І.С., Бесова А.О., Бордунова К.І. Підвищення безпеки польотів групи однотипних безпілотних літальних апаратів під час моніторингу на основні технології машинного навчання …….……..	95
Коляденко Ю.Ю., Бабаєва М.О. Підвищення завадостійкості системи передачі інформації віддаленого відеоспостереження …….……	97
Коляденко Ю.Ю., Бадєєв В.О. Система контролю та управління інформаційною безпекою мережі 5G ……..	99
Коркін О.Ю., Ковалішин С.С., Коркіна Н.О., Симоненкова І.В. Забезпечення функціонування каналу управління наземного роботизованого комплексу в умовах радіоелектронної боротьби …….	101
Коробецький О.В. Боротьба з ударними безпілотними літальними апаратами разового застосування типу «Shahed-136» (Герань-2) та особливості їх локації над морем ……	104
Костиря О.О., Гризо А.А., Лук'янчиков А.А., Черевко А.Є. Розробка імітатора постановника активних шумових завад дециметрового діапазону хвиль для тренування обслуг радіолокаційних станцій …….……..	105
Кот В.В., Герасимов С.В. Імітаційна модель діагностування технічного стану електрообладнання бронетанкової техніки ……..……..	108
Котова М.А., Лабушняк В.В. Автоматизована методика калібрування цифрових мультиметрів закордонного виробництва ……..	110
Красинський С.В., Меркулов О.А., Мироненко О.В., Ніколенко В.В. Експертиза щодо виконання метрологічних вимог до виробів озброєння та військової техніки: актуальні питання організування та проведення …….	111
Лавренчук А.А., Пастушенко М.С., Стародубцев С.О. Сучасні методи біометричної автентифікації: інновації, загрози та захист……..……..	113
Лаврут О.О., Лаврут Т.В., Колесник В.О., Жук О.В. Покращення якості управління потоками інформації у сучасних телекомунікаційних мережах військового призначення:перспективи розвитку ……..…….	114
Лаврут О.О., Лаврут Т.В., Шармін В.В., Бойчук Б.М. Телекомунікаційні мережі військового призначення: перспективи розвитку ……..……	115
Лановий О.Ф. Класифікація звітів про дефекти методами ШІ ……..	116
Левківський Н.В., Бабарика А.О. Роль еквівалентів антен у підвищенні безпеки системи зв'язку …….……..	119

Лейба В.О., Любішин Б.В. Проблеми формування сигналів із заданим коефіцієнтом гармонік …….	120
Литвин А.В., Вакуленко Д.М. Напрямки модернізації широкосмугових мереж зв'язку типу MANET …….	121
Литвин А.В., Пеньковський О.Л. Застосування гібридних методів розширення спектру в сучасних засобах радіозв'язку ……	123
Лютий А.О. Інноваційне розгортання базових станцій на багатосмугових вулицях із підтримкою мультизв'язку між та всередині RAT, з використанням міліметрових і субміліметрових хвиль для підвищення ефективності мережі ..…	124
Майборода І.М. Перспективи застосування супутникових терміналів на основі RIS технології ……...….	127
Максюта Д.В., Книш Д.В., Порохончук О.М. Актуальні напрямки розвитку радіоелектронних систем для силових структур України …….……..	128
Малюк В.Г. Вплив параметрів моделі активного радіомаскування каналу зв'язку VHF/UHF діапазону на область розміщення генератора радіоперешкод ……..	130
Мартинюк І.М., Погребняк Т.Д., Шматов Є.М. Засоби імітаційного моделювання в освітньому процесі підготовки майбутніх військовослужбовців Збройних Сил України ……..	133
Матвєєв Г.А., Казмірчук Р.В. Досвід застосування технологій штучного інтелекту у військових цілях ……	134
Медовкін В.В., **Дядюн С.В.** Дослідження блокчейн-рішень для прозорого управління фінансами ……	137
Метешкін К.О., Шевченко В.А., Маслій Л.О. Моделювання даних і знань у концепції колективного розуму В.І. Вернадського …….……..	138
Мокоївець В.І., Бокачов С.В., Томчук О.А., Федоров О.Ю. Взаємодія засобів автоматизації пунктів управління сухопутних військ та інших складових сектору безпеки і оборони України ……..….	141
Мордвинцев М.В., **Хлєстков О.В.** Оптимізація оперативної діяльності правоохоронних органів України за допомогою систем відеоспостереження ..…	143
Нелінь Д.П., Максюта Д.В., Книш Д.В. Аналіз перспектив використання електронних комунікаційних мереж в службовій діяльності силових структур ..	144
Ненич Д.О. Розробка інтелектуального регулятора температури для дослідницьких та промислових застосувань …….……	147
Нещадін О.В. Досвід застосування інтерактивних технологій навчання щодо прийняття рішень спеціалістами інженерної підтримки …….…….	148
Нікора І.В., Богдановська К.Д. Моделі оцінки пропускної здатності інформаційно-комунікаційної мережі під впливом кібернетичних атак ……...	151
Олексенко О.О., Карлов В.Д., Ковальчук А.О. Пропозиції щодо створення та удосконалення систем дистанційного наведення засобів малокаліберної зенітної артилерії ……..	152
Оленченко В.Т. Застосування штучного інтелекту в освітньому процесі ……..…	153
Паламарчук Н.А., Процюк Ю.О., Мартинюк В.В., Кугот О.Л. Аналіз алгоритмів (методів) розпізнавання зображень, які базуються на комп'ютерному баченні для ідентифікації вибухонебезпечних предметів …….	154
Паламарчук С.А., Паламарчук Н.А., Чередниченко О.Ю., Побережець Т.В. Проблематика захисту інформації та кіберзахисту інформаційно-комунікаційних систем ……..……	157
Пастушенко М.О., Пастушенко М.С., Романюк В.А., Файзулаєв Т.А. Аналіз впливу нормалізації голосового сигналу системи автентифікації на якість формантних даних …….……	160

Пастушенко М.С., Романюк В.А., Файзулаєв Т.А. Аналіз впливу частоти дискретизації голосового сигналу системи автентифікації на якість формантних даних …….……..	161
Пащетник О.Д., Живчук В.Л., Петлюк І.В. Аналіз використання архітектурного підходу для проєктування інформаційних (автоматизованих) систем за стандартами НАТО ……	163
Першин О.В., Клабан І.Ю., Кулабухов О.М. Дослідження ефективності та продуктивності систем виявлення мережевих вторгнень …….	164
Поплавець С.І. Деякі погляди до формування інформаційних моделей радіаційної та хімічної обстановки …….….	164
Попов М.О. Визначення координат розвідувальних безпілотних літальних апаратів радіолокаційними станціями радіотехнічних військ та мережею SDR приймачів ……	166
Попова Н.О., Попов М.О., Нелінь Д.П. Аналіз застосування супутникового зв'язку у сучасній війні …….……	167
Поручник А.В. Технології захисту інформації та кібербезпека ……..……	168
Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Гетьман А.В. Аналіз впливу російських інформаційних операцій на Україну ……..……	170
Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Гетьман А.В. Аналіз інформаційно-аналітичної системи прогнозування вразливостей та загроз інформаційної безпеки …….……	172
Прохорський С.І., Бондаренко О.Є., Сергієнко А.В., Гетьман А.В. Оцінка якості системи прогнозування загроз інформаційної безпеки …….……	175
Радзіковський С.А., Павельчук В.Л. Практика використання інформаційних технологій в процесі навчання майбутніх офіцерів сухопутних військ ……..	178
Радченко М.М., Скляров О.В., Сайко В.Г. Волоконно-оптичні системи передачі для безпілотних систем ……..…...	181
Рєзніков Ю.В., Аркушенко П.Л., Андрушко М.В., Матющенко О.Г. Розробка методичного апарату випробувань акустичної помітності наземних роботизованих комплексів ……..…….	184
Сахарчишина А.І., Бабарика А.О. Можливості застосування патч-антен в радіосистемах УКХ діапазону …….	185
Січевська К.В., Шевчук І.В., Поліщук Є.Ю., Площик А.С. Актуальність розробки пристрою для аналізу узгодження антени та радіостанції на основі коефіцієнта стоячої хвилі ……..	186
Солодовник В.І., Пантась С.О., Пантась І.О. Особливості функціонування підрозділів бригади та застосування засобів зв'язку в умовах гібридної війни ...	187
Соломоненко Ю.С., Худов Г.В., Хижняк І.А., Грідасов І.Ю. Метод сегментування зображення в системі наведення FPV-дронів на основі перетворення Хафа ……	191
Старцев В.В., Леках А.А., Мусієнко О.П., Михальова Л.В. Застосування сучасних інформаційних технологій у процесах автоматизації руху та обліку матеріально-технічних засобів під час воєнного стану ……..…..….	192
Стратійчук І.О. Метод формування вимог до побудови системи захисту від радіокерованих боєприпасів на автомобілях та бронетехніці ……..……	195
Струкевич Д.І., Зелінська А.В., Алексєєва О.О., Площик А.С. Методи підвищення ефективності антен для супутникового зв'язку в польових умовах ..	196
Тарасенко А.В., Кобзєв В.Г. Використання засобів штучного інтелекту для збору інформації з інтернет-ресурсів ……..…	198
Терещенко І.О., Лученко Я.В., Каук В.І. Адаптивні освітні системи як інструмент підготовки кадрів з кібербезпеки в силових структурах ……..…	199

Ткаченко К.М., Лазарев В.Д. Використання програмного забезпечення Xmind у навчальному процесі ……..	201
Толстов О.С. Кореляційно-екстремальний метод виміру кута фазового зсуву ...	202
Удніков О.М., Шеховцова І.О., Климченко С.В. Особливості використання сучасного вимірювального обладнання при калібруванні вимірювачів потужності електромагнітних коливань надвисокої частоти ……	203
Ушаков В.А. Огляд можливого використання спеціалізованих моделей Chat GPT у навчальному процесі …….	204
Федоров О.Ю., Томчук О.А., Циганков П.М., Варванець Ю.В. Застосування інформаційних технологій підтримки прийняття рішень силами оборони України у ході відсічі широкомасштабної збройної агресії російської федерації проти України	206
Флорін О.П., Богачов С.О., Кот О.Б., Кузміч О.Є. Розвиток бездротових сенсорних мереж у комплексах технічного контролю ……..….	207
Фтемов Ю.О. Застосування STEM-підходу у процесі виконання курсової роботи курсантами військових закладів освіти ……	209
Фурман К.С., Бондар К.А., Демидас М.О. Дослідження джерел радіочастотних завад і методи їх зменшення ……..……	210
Хмелевський С.І., Скріпченко Є.Л. Проектування системи оперативної підтримки прийняття рішень особами бойової обслуги ……..…….	212
Хмелевський С.І., Хмелевська О.О. Інформаційні технології в управлінні …..	213
Ховрат А.В., Стрельченко А.В., Кобзєв В.Г. Дворівнева система класифікації дезінформації в соціально-орієнтованих системах з використанням штучного інтелекту ……..	215
Хомяк К.М., Ларіонов В.В. 3D окуляри – сучасні технічні засоби навчання …..	218
Циганков П.М., Чаган Ю.А., Федоров О.Ю., Мокоївець В.І. Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку	219
Чепкій В.В., Єфимчиков О.М., Цуканов В.Н., Єльчанінов О.Д. Перешкодозахищеність каналів управління мобільними багатоцільовими платформами безпілотної наземної системи в сценарних умовах радіоелектронного конфлікта ……	221
Черних Ю.О. Застосування інформаційно-аналітичних систем оцінювання рівня якості вищої освіти ……..……..	224
Чесановський І.І. Мультиагентне управління ресурсами в кіберфізичних системах.	227
Шаповал Л.О., Давиденко В.В., Дмитренко В.В. Шляхи використання безпілотних засобів для відновлення несправної (пошкодженої) техніки ……..…	229
Шило С.Г., Першин О.О., Яцун Д.А., Пахомова А.М. Ситуативне управління відображенням інформаційних моделей в АСУ ……..……	231
Шинкар Є.В., Лаврут О.О. Використання ІТ в організації логістичного забезпечення ……..……	233
Штонда Р.М., Білий В.О., Черниш Ю.О., Терещенко Т.П. Безпарольна автентифікація: переваги та ризики ……..	234
Шульга В.В., Першин О.В., Нікора І.В., Дзюба І.В. Інтелектуальна система аналізу відкритих джерел ……..….	235
Щадило П.Р., Площик А.С. Кіберзахист в умовах реалій сучасності: технології, методи та перспективи ……..……	237
Щербакова П.В., Новічков В.О. Використання телеметричних систем у військовій справі …….	238
Яровий В.С., Гулій В.С., Денісова В.В., Мордвінов М.О. Ініціатива процесу відновлення озброєння та військової техніки агрегатним методом ремонту ……..	239
Зміст …….	241
Абетковий покажчик авторів публікацій ……..……	247

АБЕТКОВИЙ ПОКАЖЧИК АВТОРІВ ПУБЛІКАЦІЙ

General Manager Terranis Systems Ltd, м. Одокра (Швеція)

Ulf Krahn		***8***

Lodz University of Technology, м. Лодзь (Польща)

Yakovlev S. ***(Яковлєв С.В.)***	- Doctor of Physical and Mathematical, professor of Institute of Information Technology, Lodz University of Technology (Lodz, Poland), Deputy Director of the Educational and Scientific Institute of Computer Sciences and Artificial Intelligence of V.N. Karazin Kharkiv National University. Corresponding Member of the National Academy of Sciences of Ukraine	***20***

Swedish Defence University (Швеція)

Hans Liwång	- Department Management, Department of Systems Science for Defence and Security, Ph.D. in Shipping and Marine Technology from Chalmers University of Technology	***8***

Військова академія, м. Одеса

Братченко Г.Д.	- доктор технічних наук, професор, провідний науковий співробітник науково-дослідного лабораторії наукового центру	***39***
Бриженюк Ю.Д.	- ад'юнкт	***39***
Єфимчиков О.М.	- кандидат технічних наук, доцент, провідний науковий співробітник наукового центру	***221***
Ковалішин С.С.	- начальник науково-дослідного відділу наукового центру	***101***
Коркін О.Ю.	- доктор філософії, провідний науковий співробітник науково-дослідного відділу наукового центру	***101***
Коркіна Н.О.	- старший помічник начальника відділу штабу	***101***
Лукаш Р.В.	- начальник науково-дослідної лабораторії наукового центру	***39***
Симоненкова І.В.	- науковий співробітник наукового центру	***101***
Цуканов В.Н.	- старший науковий співробітник наукового центру	***221***
Чепкій В.В.	- кандидат технічних наук, доцент, провідний науковий співробітник наукового центру	***221***

Військова частина А 0785, м. Харків

Дуболазов Ю.О.	- науковий співробітник	***65***
Климченко С.В.		***203***
Коротій О.О.	- старший науковий співробітник	***65***
Котова М.А.	- науковий співробітник науково-дослідного відділу	***110***
Красинський С.В.	- старший науковий співробітник	***111***
Лабушняк В.В.	- молодший науковий співробітник науково-дослідного відділу	***110***
Лейба В.О.	- старший науковий співробітник	***120***
Любішин Б.В.	- науковий співробітник	***120***
Меркулов О.А.	- старший науковий співробітник	***111***
Мироненко О.В.		***111***
Ніколенко В.В.	- заступник начальника науково-дослідного відділу військових еталонів	***111***
Толстов О.С.		***202***
Удніков О.М.	- провідний науковий співробітник	***203***
Шеховцова І.О.	- провідний науковий співробітник	***203***

Військовий інститут Київського національного університету імені Тараса Шевченка

Kubiavka M. ***(Кубявка М.Б.)***	- кандидат технічних наук, начальник науково-дослідного відділу - заступник начальника науково-дослідного управління військово-гуманітарних досліджень науково-дослідного центру	***10***
Pyrogov K.	- старший науковий співробітник науково-дослідного відділу -	***10***

(Пирогов К.О.)	заступник начальника науково-дослідного управління військово-гуманітарних досліджень науково-дослідного центру	
Черних Ю.О.	- кандидат технічних наук, доцент, провідний науковий співробітник	***224***

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут , м. Київ

Білий В.О.	- курсант	***234***
Бондаренко О.Є.	- начальник науково-дослідного відділу - заступник начальника науково-дослідного управління наукового центру	***170, 172, 175***
Гетьман А.В.	- старший науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру	***48, 170, 172, 175***
Гулій В.С.	- заступник начальника кафедри	***239***
Данилюк І.А.	- кандидат технічних наук, доцент, головний науковий співробітник	***62***
Денісова В.В.	- викладач кафедри	***239***
Жилінський І.В.	- доцент кафедри	***68***
Зінченко М.О.	- начальник науково-дослідного управління наукового центру	***70***
Комаров В.О.	- кандидат технічних наук, старший дослідник, провідний науковий співробітник науково-дослідної лабораторої наукового центру	***48, 70***
Кугот О.Л.	- викладач кафедри	***154***
Куцаєв В.В.	- молодший науковий співробітник	***62***
Мартинюк В.В.	- провідний науковий співробітник науково-дослідної лабораторії	***154***
Мордвінов М.О.	- старший викладач кафедри	***239***
Паламарчук Н.А.	- начальник науково-дослідної лабораторії	***154, 157***
Паламарчук С.А.	- головний науковий співробітник	***157***
Пантась С.О.	- старший викладач кафедри	***187***
Пантась І.О.	- викладач кафедри	***187***
Плугова О.Б.	- старший науковий співробітник наукового центру	***48***
Побережець Т.В.	- науковий співробітник	***157***
Прохорський С.І.	- науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру	***170, 172, 175***
Процюк Ю.О.	- провідний науковий співробітник науково-дослідної лабораторії	***154***
Радзівілов Г.Д.	- кандидат технічних наук, професор, заступник начальника інституту з наукової роботи	***62***
Радченко М.М.	- науковий співробітник науково-дослідної лабораторії	***181***
Сайко В.Г.	- доктор технічних наук, професор, професор кафедри	***48, 70, 181***
Свідзінський Ю.О.	- старший викладач кафедри	***68***
Сергієнко А.В.	- провідний науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру	***170, 172, 175***
Скляров О.В.	- провідний науковий співробітник науково-дослідної лабораторії	***181***
Солодовник В.І.	- доктор філософії, доцент кафедри	***187***
Терещенко Т.П.	- старший науковий співробітник науково-дослідного відділу наукового центру	***234***
Чередниченко О.Ю.	- старший науковий співробітник науково-дослідного відділу наукового центру	***157***
Черниш Ю.О.	- старший науковий співробітник науково-дослідного відділу наукового центру	***234***
Штонда Р.В.	- начальник науково-дослідного відділу	***234***
Ющенко Ю.М.	- старший викладач кафедри	***68***
Яровий В.С.	- доктор філософії, професор кафедри	***68, 239***

Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, м. Черкаси

Андрушко М.В.	- провідний науковий співробітник науково-дослідного відділу	***184***
Аркушенко П.Л.	- кандидат технічних наук, старший дослідник, начальник науково-дослідного відділу	***184***

Богачов С.О.	- науковий співробітник	***207***
Іванець М.Г.	- кандидат технічних наук, старший дослідник, провідний науковий співробітник – провідний інженер-випробувач науково-дослідного відділу	***76***
Кот О.Б.		***207***
Кузміч О.Є.	- начальник науково-дослідної лабораторії	***207***
Матющенко О.Г.	- доктор філософії, старший науковий співробітник-старший інженер випробувач науково-дослідного відділу	***184***
Пустоваров В.В.	- кандидат технічних наук, провідний науковий співробітник	***93***
Рєзніков Ю.В.	- кандидат технічних наук, с.н.с., провідний науковий співробітник науково-дослідного відділу	***184***

Державне некомерційне підприємство «Державний університет авіаційного інституту Київ», м.Київ

Komar O. ***(Комар О.М.)***	- кандидат технічних наук, доцент кафедри	***12***

Командування Повітряних Сил збройних Сил України (м. Вінниця)

Олексенко О.О.	- доктор філософії, начальник воєнно-наукового відділу	***152***

Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький

Алексєєва О.О.		***196***
Бабарика А.О.	- доктор філософії, доцент кафедри	***46, 119, 185***
Басараб О.К.	- кандидат технічних наук, доцент, доцент кафедри	***28***
Бондар К.А.	- курсант	***210***
Валько В.В.	- курсант	***46***
Винту А.О.	- викладач кафедри	***47***
Данило Н.Р.	- курсант	***59***
Данильчук Р.О.	- курсант	***59***
Демидас М.О.	- командир відділення	***210***
Зелінська А.В.		***196***
Катеринчук І.С.	- доктор технічних наук, професор, професор кафедри	***81***
Левківський Л.В.	- курсант	***119***
Мільшин С.І.	- старший викладач кафедри	***47***
Мішенюк Р.М.	- кандидат педагогічних наук, доцент, начальник кафедри	***28***
Площик А.С.	- старший викладач кафедри	***59, 186, 196, 237***
Поліщук Є.Ю.	- командир відділення	***186***
Сахарчишина А.І.	- курсант	***185***
Січевська К.В.	- курсант	***186***
Струкевич Д.І.	- курсант	***196***
Фурман К.С.	- курсант	***210***
Хоптинський Р.П.	- кандидат технічних наук, доцент кафедри	***81***
Чесановський І.І.	- кандидат технічних наук, доцент, докторант	***227***
Шевчук І.В.	- курсант	***186***
Щадило П.Р.	- курсант	***237***

Національна академія Національної гвардії України, м. Харків

Баулін Д.С.	- кандидат технічних наук, с.н.с., провідний науковий співробітник науково-дослідного центру	***76***
Bordunova K. ***(Бордунова К.І.)***	- науковий співробітник відділу Центру імітаційного моделювання	***5, 95***
Vlasov K. (***Власов К.В.)***	- старший викладач кафедри	***18***
Горєлишев С.А.	- кандидат технічних наук, доцент, доцент кафедри	***52, 76***
Глущенко М.О.	- старший викладач кафедри	***51***
Душкін В.Д.	- кандидат фізико-математичних наук, доцент, доцент кафедри	***67***
Єльчанінов О.Д.	- кандидат технічних наук, доцент, професор кафедри	***221***

Iokhov O. ***(Іохов О.Ю.)***	- доктор технічних наук, професор, начальник Центру імітаційного моделювання	***7, 8, 93***
Ishchuk O. ***(Іщук О.Р.)***	- старший інженер-програміст відділу Центру імітаційного моделювання	***7***
Лазарев В.Д.	- старший викладач кафедри	***201***
Майборода І.М.	- кандидат військових наук, доцент, доцент кафедри	***127***
Малюк В.Г.	- кандидат технічних наук, доцент, доцент кафедри	***130***
Новикова О.О.	- кандидат технічних наук, доцент, професор кафедри	***91***
Оленченко В.Т.	- кандидат технічних наук, доцент, начальник кафедри	***153***
Романюк В.А.	- кандидат технічних наук, доцент, доцент кафедри	***160, 161***
Сидоренко І.І.	- кандидат педагогічних наук, доцент, доцент кафедри	***67***
Sporyshev K. ***(Споришев К.О.)***	- доктор технічних наук, доцент, заступник начальника Центру імітаційного моделювання	***14, 24***
Стародубцев С.О.	- кандидат військових наук, доцент, доцент кафедри	***113***
Стратійчук І.О.	- ад'юнкт	***195***
Ткаченко К.М.	- доктор філософії, заступник начальника кафедри	***201***
Ушаков В.А.	- старший викладач	***204***
Флорін О.П.	- кандидат технічних наук, доцент, доцент кафедри	***207***
Щолок А.В.		***83***

Національна академія Сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів

Андреєва Л.М.	- викладач кафедри	***87***
Баранов А.М.		***26***
Баранов Ю.М.	- кандидат технічних наук, доцент, заступник начальника кафедри	***26***
Бойчук Б.М.	- старший викладач кафедри	***115***
Бокачов С.В.	- провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***37, 141***
Бричинський О.В.	- старший викладач кафедри	***42***
Варванець Ю.В.	- науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***37, 206***
Годебський В.П.	- науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***73***
Давіденко С.В.	- кандидат технічних наук, доцент, провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***54, 69***
Живчук В.Л.	- кандидат технічних наук, начальник науково-длслідної лабораторії науково-дослідного відділу Наукового центру Сухопутних військ	***163***
Жук О.В.	- викладач кафедри	***114***
Заєць Я.Г.	- кандидат технічних наук, старший дослідник,старший науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***54, 69***
Зубков А.М.	- доктор технічних наук, с.н.с., провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***73, 75***
Казмірчук Р.В.		***134***
Каменцев С.Ю.	- провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***73***
Каршень А.М.	- начальник кафедри	***26***
Кізло Л.М.	- науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***87***
Колесник В.О.	- старший науковий співробітник Наукового центру Сухопутних військ	***114***
Контуров В.М.		***42***
Красник Я.В.	- старший науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***75***
Лаврут О.О.	- доктор технічних наук, професор, заступник начальника кафедри	***114, 115, 233***
Лаврут Т.В.	- кандидат географічних наук, доцент, старший науковий співробітник науково-дослідного відділу Наукового центру	***114, 115***

	Сухопутних військ	
Ларіонов В.В.		***218***
Луньков А.В.	- старший науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***87***
Матала І.В.	- науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***87***
Матвєєв Г.А.	- старший викладач кафедри	***134***
Малюк В.М.		***42***
Мартиненко С.А.	- начальник науково-дослідного відділу Наукового центру Сухопутних військ	***75***
Мартинюк І.М.	- кандидат біологічних наук, начальник науково-дослідної лабораторії	***133***
Марцінко Н.М.	- кандидат історичних наук, науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***37***
Мокоївець В.І.	- провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***141, 219***
Нещадін О.В.	- старший викладач кафедри	***148***
Опалинський В.Б.	- викладач кафедри	***54***
Павельчук В.Л.	- начальник науково-дослідного відділу Наукового центру Сухопутних військ	***178***
Пащетник О.Д.	- кандидат технічних наук, с.н.с., начальник науково-дослідної лабораторії науково-дослідного відділу Наукового центру Сухопутних військ	***163***
Петлюк І.В.	- кандидат технічних наук, старший дослідник, провідний науковий співробітник науково-дослідної лабораторії науково-дослідного відділу Наукового центру Сухопутних військ	***163***
Погребняк Т.Д.		***133***
Поручник А.В.	- викладач кафедри	***168***
Радзіковський С.В.	- науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***178***
Рижов Є.В.	- кандидат технічних наук, старший дослідник, начальник науково-дослідного відділу Наукового центру Сухопутних військ	***54***
Сірий Ю.І.	- науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***73***
Sovhar O. ***(Совгар О.М.)***	- кандидат педагогічних наук, доцент, професор кафедри	***12***
Томчук О.А.	- начальник науково-дослідного відділу Наукового центру Сухопутних військ	***141, 206***
Федоров О.Ю.	- провідний науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***141, 206 219***
Фтемов Ю.О.	- кандидат технічних наук, с.н.с., професор кафедри	***209***
Хомяк К.М.	- старший викладач кафедри	***218***
Циганков П.М.	- старший науковий співробітник науково-дослідного відділу Наукового центру Сухопутних військ	***206, 219***
Чаган Ю.А.	- кандидат технічних наук, старший дослідник, заступник начальника науково-дослідного відділу Наукового центру Сухопутних військ	***37, 219***
Шармін В.В.		***115***
Шинкар Є.В.	- ад'юнкт	***233***
Шматов Є.М.		***133***

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Даник Ю.Г.	- доктор технічних наук, професор, професор кафедри	***55***
Пастушенко М.О.	- студент	***160***

Національний технічний університет «ХПІ», м. Харків

Балабуха О.С.		***24***
Бесова А.О.		***95***

Биков О.М.	- кандидат технічних наук, доцент кафедри	***34***
Бурак А.В.	- викладач кафедри	***44***
Воловоденко Ю.М.	- старший викладач кафедри	***44***
Герасимов С.В.	- доктор технічних наук, професор, професор кафедри	***108***
Давиденко В.В.	- старший викладач кафедри	***229***
Дидюк В.Г.	- старший викладач кафедри	***34***
Дмитренко В.В.	- викладач кафедри	***229***
Качуровський Г.М.		***24***
Кобзев Д.О.	- студент	***90***
Коломійцев О.В.	- доктор технічних наук, професор, професор кафедри	***83, 93, 95***
Комаров В.О.		***93***
Кот В.В.	- заступник начальника кафедри	***108***
Максимов М.О.		***24***
Мосійчук М.В.	- заступник начальника факультету з навчальної та наукової роботи	***44***
Пришляк І.В.	- старший викладач кафедри	***34***
Роянов О.М.		***83***
Рудаков І.С.	- аспірант	***95***
Суровицький С.В.	- молодший науковий співробітник	***90***
Шаповал Л.О.	- магістрант	***229***

Національний університет цивільного захисту України, м. Харків

Катунін А.М.	- кандидат технічних наук, старший науковий співробітник	***83***

ТОВ «ТАФ-87», м. Харків

Файзулаєв Т.А.	- директор	***160, 161***

Український державний університет залізничного транспорту, м. Харків

Perets K..		***11***
(Перець К.Г.)		
Kharchenko I.		***9***
(Харченко І.В.)		

Харківський національний університет імені В. Н. Каразіна

Dyadun S.	- кандидат технічних наук, доцент, доцент кафедри	***6, 85, 137***
(Дядюн С.В.)		
Кисіль Г.А.	- студент	***85***
Медовкін В.В.	- студент	***137***
Ненич Д.О.	- студент	***147***
Strukov V.	- кандидат технічних наук, доцент, в.о. завідувача кафедри	***20***
(Струков В.)	математичного моделювання та аналізу даних	
Uzlov D.	- кандидат технічних наук, доцент, директор навчально-	***20***
(Узлов Д.)	наукового інституту комп'ютерних наук і штучного інтелекту	

Харківський національний університет міського господарства ім. О.М. Бекетова

Маслій Л.О.		***138***
Метешкін К.О.	- доктор технічнихнаук, професор, професор кафедри	***138***
Шевченко В.О.		***138***

Харківський національний університет внутрішніх справ

Мордвинцев М.О.	- кандидат технічних наук, доцент, провідний науковий співробітник науково-дослідної навчально-наукового інституту № 4	***143***
Хлєстков О.В.	- старший науковий співробітник науково-дослідної лабораторії навчально-наукового інституту № 4	***143***

Харківський національний університет Повітряних Сил імені Івана Кожедуба

Адаменко А.А.	- кандидат технічних наук, с.н.с., провідний науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру Повітряних Сил	***21***
Антонов Д.В.	- начальник центру імітаційного моделювання	***21***
Бабенко О.І.	- кандидат військових наук, доцент, провідний науковий співробітник наукового центру Повітряних Сил	***23, 78***
Бєрнік Є.В.	- ад'юнкт	***33***
Богдановська К.Д.	- курсантка	***151***
Вакуленко Д.М.	- курсант	***121***
Vasylyshyn V. (Василишин В.І.)	- доктор технічних наук, професор, начальник кафедри	***17***
Гаврилов Д.С.	- молодший науковий співробітник наукового центру Повітряних Сил	***78***
Гризо А.А.	- кандидат технічних наук, доцент, начальник науково-дослідної лабораторії	***105***
Грідасов І.Ю.	- провідний науковий співробітник науково-методичного відділу забезпечення якості освітньої діяльності та вищої освіти університету	***191***
Дзюба І.В.	- старший науковий співробітник	***235***
Дубовський Ю.В.	- курсант	***64***
Залевський Г.С.	- доктор технічних наук, професор, начальник кафедри	***52***
Іванець Г.В.	- кандидат технічних наук, доцент, старший науковий співробітник науково-дослідної лабораторії факультету	***76***
Калачова В.В.	- кандидат технічних наук, с.н.с., доцент, провідний науковий співробітник наукового центру Повітряних Сил	***23, 78***
Карлов В.Д.	- доктор технічних наук, професор, завідувач кафедри	***64, 152***
Кириченко М.І.	- молодший науковий співробітник науково-дослідної лабораторії факультету	***76***
Клабан І.Ю.	- курсант	***164***
Ковальчук А.О.	- кандидат технічних наук, доцент, професор кафедри	***152***
Коробецький О.В.	- старший науковий співробітник наукового центру Повітряних Сил	***104***
Костиря О.О.	- доктор технічних наук, с.н.с., провідний науковий співробітник науково-дослідної лабораторії	***105***
Книш Д.В.	- начальник науково-дослідного відділу науково-дослідного управління наукового центру Повітряних Сил	***128, 144***
Kryvonos V. (Кривонос В.М.)	- кандидат технічних наук, начальний кафедри	***15***
Кулабухов О.М.	- викладач кафедри	***164***
Леках А.А.	- кандидат технічних наук, начальник науково-дослідної лабораторії	***192***
Литвин А.В.	- старший викладач кафедри	***121, 123***
Lysechko V. (Лисечко В.П.)	- доктор технічних наук, професор, провідний науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру Повітряних Сил	***9, 11, 12***
Лук'янчиков А.А.	- сстарший науковий співробітник науково-дослідної лабораторії	***105***
Максюта Д.В.	- кандидат технічних наук, молодший науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру Повітряних Сил	***128, 144***
Михальова Л.В.	- молодший науковий співробітник	***192***
Місюра О.М.	- кандидат технічних наук, с.н.с., начальник наукового центру Повітряних Сил	***78***
Мусієнко О.П.	- кандидат технічних наук, провідний науковий співробітник	***192***
Нелінь Д.П.	- провідний науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру Повітряних Сил	***144, 167***
Нікора І.В.	- викладач кафедри	***151, 235***
Новічков В.О.	- викладач кафедри	***238***
Пахомова А.М.		***231***

Пеньковський О.Л.	- курсант	***123***
Першин О.В.	- старший викладач кафедри	***164, 235***
Першин О.О.		***231***
Поплавець С.І.	- доктор філософії, професор кафедри	***164***
Попов М.О.	- науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру Повітряних Сил	***166, 167***
Попова Н.О.	- молодший науковий співробітник науково-дослідної лабораторії факультету	***167***
Порохончук О.М.	- старший науковий співробітник науково-дослідного відділу науково-дослідного управління наукового центру Повітряних Сил	***21, 128***
Присяжний А.Є.	- кандидат технічних наук, доцент кафедри	***64***
Сізон Д.О.	- начальник науково-дослідного відділу наукового центру	***23***
Скріпченко Є.Л.	- курсантка	***212***
Соломоненко Ю.С.	- кандидат технічних наук, заступник начальника факультету з навчальної та наукової роботи – начальник навчальної частини	***191***
Старцев В.В.	- науковий співробітник	***192***
Tupitsya I. (Тупиця І.М.)	- старший викладач кафедри, доктор філософії	***15***
Хижняк І.А.	- кандидат технічних наук, начальник науково-методичного відділу забезпечення якості освітньої діяльності та вищої освіти університету	***191***
Хмелевська О.О.	- провідний науковий співробітник, кандидат технічних наук, с.н.с.	***213***
Хмелевський С.І.	- кандидат технічних наук, доцент, начальник кафедри	***212, 213***
Хроль Л.О.	- науковий співробітник науково-дослідної лабораторії факультету	***76***
Худов Г.В.	- доктор технічних наук, професор, начальник кафедри	***33_ 191***
Черевко А.Є.	- курсант	***105***
Shevchenko O. (Шевченко О.О.)		***11***
Шило С.Г.	- кандидат технічних наук, доцент, доцент кафедри	***231***
Shubina H. (Шубіна Г.В.)		***12***
Шульга В.В.	- старший викладач кафедри	***235***
Щербакова П.В.	- курсантка	***238***
Яцун Д.А.		***231***

Харківський національний університет радіоелектроніки

Бабаєва М.О.	- студентка	***97***
Бадеєв В.О.	- аспірант	***99***
Безкоровайний В.В.	- доктор технічних наук, професор, професор кафедри	***29, 31***
Драз О.М.	- асистент кафедри	***31***
Каук В.І.	- кандидат технічних наук, с.н.с., доцент кафедри	***199***
Kobziev V. (Кобзєв В.Г.)	- кандидат технічних наук, с.н.с., доцент кафедри	***20, 198, 215***
Козлов Ю.В.	- кандидат технічних наук, доцент, доцент кафедри	***91***
Коляденко Ю.Ю.	- доктор технічних наук, професор, професор кафедри	***97, 99***
Лавренчук А.А.	- магістрант	***113***
Лановий О.Ф.	- кандидат технічних наук, доцент, доцент кафедри	***116***
Лученко Я.В.		***199***
Лютий А.О.	- студент	***124***
Пастушенко М.С.	- кандидат технічних наук, професор, професор кафедри	***113, 160, 161***
Стрельченко А.В.		***215***
Тарасенко А.В.	- магістрант	***198***
Терещенко І.О.		***199***
Ховрат А.В.	- аспірант	***215***

Наукове видання

Міжнародна науково-практична конференція

«ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ»

Збірник тез доповідей

Відповідальний за випуск *О. Ю. Іохов*

В авторській редакції.
Упорядник: *О. О. Новикова*
Комп'ютерна верстка: *О. О. Новикова*

Формат 60х84/16. Ум. друк. арк. 23,25. Тираж 30 пр. Зам. № 39.

Видавець і виготовлювач Національна академія Національної гвардії України
Майдан Захисників України, 3, м. Харків, 61001.
Свідоцтво суб'єкта видавничої справи ДК № 4794 від. 24.11.2014 р.